

RODO - GDPR

OCHRONA

DANYCH MEDYCZNYCH

Jakub Rzymowski (red.)

Dominik Spalek

RODO – GDPR

OCHRONA

DANYCH MEDYCZNYCH

Jakub Rzymowski (red.)

Dominik Spalek

Wydawnictwo Uniwersytetu Medycznego w Łodzi

Copyright by © Jakub Rzymowski and Dominik Spalek

Autorstwo podrozdziałów i wzorów dokumentów
wskazane w spisie treści lub/i w stopkach stron ^(R/S)

Numer ORCID J. Rzymowskiego: 0000-0003-0538-8895

Recenzja naukowa:
Profesor doktor habilitowany
Rafał Kubiak

J. Rzymowski jest adiunktem w Katedrze Europejskiego Prawa
Gospodarczego Wydziału Prawa i Administracji
Uniwersytetu Łódzkiego.

Projekt okładki: Magdalena Rzymowska

ISBN 978-83-67198-18-9

Wydawca:
Uniwersytet Medyczny w Łodzi
Wydawnictwo Uniwersytetu Medycznego w Łodzi.
Wydanie I, Łódź 2022

Spis treści

Wstęp ^R	13
Dlaczego chroni się dane osobowe ^R	14
RODO - obowiązywanie ^R	17
Przygotowanie dokumentów ^R	18
Dokumentacja jako obowiązek ^R	19
Pojęcia istotne	
dla ochrony danych medycznych ^R	23
Dane osobowe ^R	23
Dane spseudonimizowane ^R	25
Dane dotyczące dzieci urodzonych żywo	
i nie urodzonych żywo ^R	26
Dane genetyczne ^R	26
„Dane genetyczne prenatalne ^R	27
Szczególne kategorie danych, dane wrażliwe, nazewnictwo ^R ...	30
Przetwarzanie danych osobowych ^R	30
Podmiot przetwarzający ^R	31
Przykładowe podmioty przetwarzające ^R	32
Przykładowe podmioty nie będące podmiotami	
przetwarzającymi ^R	33
Podmioty, które zależnie od sytuacji	
są podmiotami przetwarzającymi lub nie ^R	38
Umowy powierzenia w praktyce NIK ^{RiS}	38
Działania do podjęcia przez podmiot ^{RiS}	45
Zgoda osoby, której dane dotyczą ^R	48
Jednoczesne stosowanie art. 9 RODO i art. 6 RODO ^R	53
Odpowiedzialność na gruncie RODO ^R	63
Odpowiedzialność administracyjna ^R	63
Kto może ponieść odpowiedzialność administracyjną ^R	64
„Polityka ochrony jako narzędzie, odwrócenia ciężaru dowodu ^R	67
Odpowiedzialność cywilna ^R	68
Istota odpowiedzialności cywilnej ^R	68
Kto może ponieść odpowiedzialność cywilną	
w realiach medycznych ^R	69
Jak administrator lub podmiot przetwarzający mogą zwolnić się	
z odpowiedzialności cywilnej ^R	69

Przykładowe naruszenia,	
mogące skutkować odpowiedzialnością cywilną ^R	70
„Odpowiedzialność cywilna spowodowana brakiem dokumentacji” ^R	72
Wdrożenie RODO w podmiocie Krok po kroku ^R	77
Kolejność przygotowywania dokumentów ^R	77
Pierwszy etap wdrożenia ^R	78
Audyt przestrzegania RODO ^R	78
Rejestr czynności przetwarzania RiS	83
Konstrukcja RCPD ^S	85
Forma dokumentu ^R	112
Możliwe błędy w RCPD ^R	113
Realizacja artykułu 13 RODO ^S	115
Źródło obowiązku ^S	115
Treść dokumentu ^S	115
„Dokumentowanie realizacji art. 13 RODO,	
realizacja zasady rozliczalności” ^S	129
Uwaga. Ostrożnościowa realizacja art. 13 RODO ^{RiS}	140
Uwaga. Informacje o odbiorcach ^{RiS}	140
„Możliwe błędy” ^R	141
Realizacja artykułu 14 RODO ^R	143
Źródło obowiązku ^R	143
Treść dokumentu ^R	143
Zwolnienia ze stosowania art. 14 RODO w realiach medycznych ^R	149
Zwolnienie z art. 14 ust. 5 lit. a RODO ^R	149
Zwolnienie z art. 14 ust. 5 lit. b RODO ^R	149
Zwolnienie z art. 14 ust. 5 lit. c RODO ^R	149
Zwolnienie z art. 14 ust. 5 lit. d RODO ^R	150
„Możliwe błędy” ^R	151
Realizacja artykułów 15 - 22 RODO ^S	153
Prawo dostępu do danych / uzyskania informacji /	
uzyskania kopii danych – art. 15 RODO ^S	157
Konieczność weryfikacji tożsamości wnioskodawcy ^S	159
„Dokumentowanie realizacji art. 15 RODO	
– realizacja zasady rozliczalności” ^S	159
Zastosowanie formularzy ^S	160
Prawo do sprostowania danych – art. 16 RODO ^S	167

Prawo do usunięcia danych – prawo do bycia zapomnianym – art. 17 RODO ^S	175
Prawo do ograniczenia przetwarzania ^S	185
Prawo do przenoszenia danych – art. 20 RODO ^S	197
Możliwe błędy ^{RiS}	202
Udostępnianie danych osobowych	
poprzez udostępnianie dokumentacji medycznej	
oraz informacji o stanie zdrowia	
i udzielonych świadczeniach zdrowotnych ^S	207
Prawo do dokumentacji medycznej ^S	207
Definicja dokumentacji medycznej ^S	208
Forma prowadzenia dokumentacji medycznej ^S	208
Dokumentacja medyczna w postaci papierowej ^S	209
Dokumentacja medyczna w postaci elektronicznej ^S	210
EDM – Elektroniczna Dokumentacja Medyczna ^S	210
Szczególne wymogi ^S	212
System teleinformatyczny do prowadzenia	
dokumentacji medycznej w postaci elektronicznej ^S	213
Podmioty uprawnione	
do dokumentacji medycznej i informacji ^S	214
Definicje kategorii osób uprawnionych ^S	214
Pacjent ^S	214
Przedstawiciel ustawowy pacjenta ^S	215
Osoba upoważniona ^S	216
Inne uprawnione podmioty ^S	218
Wykaz udostępnionej dokumentacji medycznej ^S	218
Imię (imiona) i nazwisko pacjenta,	
którego dotyczy dokumentacja medyczna ^S	219
Sposób udostępnienia dokumentacji medycznej ^S	220
Do wglądu ^S	220
W postaci wyciągu, odpisu, kopii, wydruku ^S	220
Wydanie oryginału za potwierdzeniem odbioru ^S	221
Za pośrednictwem środków komunikacji elektronicznej	
Na informatycznym nośniku danych ^S	222
Zakres udostępnionej dokumentacji medycznej ^S	224
Imię (imiona) i nazwisko osoby innej niż pacjent ^S	224
Imię (imiona) i nazwisko oraz podpis, osoby	
która udostępniła dokumentację medyczną ^S	225

Data udostępnienia dokumentacji medycznej ^S	226
Praktyczne porady dotyczące	
wykazu udostępnionej dokumentacji medycznej ^S	226
Po raz pierwszy czy po raz kolejny udostępniono ^S	226
Skrupulatnie odnotowany zakres udostępnionej dokumentacji ^S	227
Ewidencja wniosków o udostępnienie dokumentacji medycznej ^S	227
Osobiście odebrana dokumentacja medyczna ^S	227
Kopia danych osobowych ^S	228
Oплата za udostępnienie dokumentacji medycznej ^S	228
Wysokość odpłatności, sposób określenia	
oraz podania do informacji w podmiocie ^S	228
Obowiązek informowania o wysokości stawek opłat ^S	230
Wniosek o udostępnienie dokumentacji medycznej ^S	232
Forma wniosku o udostępnienie dokumentacji medycznej ^S	232
Dane zawarte we wniosku ^S	233
Ustalenie tożsamości jako warunek bezwzględny	
dla udostępnienia dokumentacji medycznej ^S	234
Termin na udostępnienie dokumentacji medycznej ^S	235
Odmowa udostępnienia dokumentacji medycznej ^S	236
Upoważnienie	
do przetwarzania danych osobowych ^R	255
Forma upoważnień ^R	259
Podsumowując ^R	261
Upoważnienie i polecenie, administrator danych	
i podmiot przetwarzający ^R	262
Treść dokumentu ^R	263
Proces zarządzania uprawnieniami do systemów	
wymaga przemyślenia i dokładnego rozplanowania ^S	279
Nadanie uprawnień do nadawania upoważnień	
do przetwarzania danych osobowych	281
Osoba nadająca upoważnienia ^R	282
Nadawanie upoważnień do przetwarzania danych osobowych	
przez inspektora ochrony danych ^R	282
Uchylanie/ustanie upoważnienia	
do przetwarzania danych osobowych, dokument:	
uchylenia, odebrania, wycofania, stwierdzenia nieważności	
upoważnienia do przetwarzania danych osobowych ^R	285

Uprawnienie do uchylania upoważnień	
do przetwarzania danych osobowych ^R	285
Możliwe błędy ^R	286
Polecenie przetwarzania danych osobowych ^R	289
Źródło obowiązku ^R	289
Wskazanie osób uprawnionych	
do odwrócenia pseudonimizacji ^R	290
Źródło obowiązku ^R	290
Polityka ochrony ^R	295
Źródło obowiązku ^R	295
Polityka ochrony jako narzędzie rozliczalności ^R	295
Polityka ochrony	
jako narzędzie odwrócenia ciężaru dowodu ^R	296
Dodatkowe narzędzia rozliczalności ^R	298

Wstęp

Wstęp

Lekarze i inni pracownicy podmiotów wykonujących działalność leczniczą mają zazwyczaj świadomość obowiązków spoczywających na nich w związku z wykonywanymi zawodami. Lekarze wiedzą o tajemnicy zawodu lekarza, pielęgniarki i położne wiedzą zwykle również o swoich tajemnicach zawodowych, aczkolwiek zaobserwowaliśmy, że zakres tych tajemnic zawodowych rozumiany jest zwykle zbyt wąsko przez osoby, na których tajemnice owe spoczywają.

Zagadnienia dotyczące tajemnic zawodowych zawodów medycznych nie są przedmiotem szczegółowych rozważań w niniejszej książce, zwracamy jednak na nie uwagę, bowiem naruszając swoje tajemnice zawodowe lekarze i pielęgniarki i położne łamią prawo i narażają się na odpowiedzialność.

Naruszenia prawa wynikające z obowiązku zachowywania tajemnic zawodowych są często trudne do wykrycia. Przeciwnie, nie-zwykle łatwe do wykrycia, zwłaszcza w przypadku kontroli z biura Prezesa Urzędu Ochrony Danych Osobowych, są naruszenia prawa polegające na umożliwieniu dostępu do danych osobowych pacjentów osobom, którym danych tych udostępniać się nie powinno. Równie łatwo wykryć brak dokumentacji przetwarzania danych osobowych, do posiadania której zobowiązuje RODO.¹

Podkreślenia wymaga, że wymieniona tu dokumentacja przetwarzania danych osobowych nie może być mylona z dokumentacją medyczną.

Obowiązek prowadzenia dokumentacji medycznej w podmiotach wykonujących działalność leczniczą wynika z ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta (Dalej: UoPPiRPP).²

¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) Dziennik Urzędowy Unii Europejskiej L 119/1, 4.5.2016, p. 1–88. [dalej: RODO].

² Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta Dz. U. 2009 r. Nr 52, poz. 417 ze zm. t.j. Dz. U. 2019 poz. 1127 ze zm. [dalej: UoPPiRP]

Dlaczego chroni się dane osobowe

Dla zrozumienia systemu ochrony danych osobowych należy postawić pytanie o to dlaczego dane osobowe, a zwłaszcza dane dotyczące stanu zdrowia, podlegają ochronie. Dane dotyczące stanu zdrowia chronione są z różnych przyczyn. Prawo do ochrony danych dotyczących stanu zdrowia jest częścią prawa do ochrony danych osobowych mającego swoje źródło w Konstytucji.³ Kiedy kartoteka zawierająca dane dotyczące stanu zdrowia konkretnych osób znajdzie się na śmietniku i ktoś nieuprawniony zapozna się z tymi danymi, to niewątpliwie nastąpi naruszenie prywatności osób, których dane dotyczą. Prawdziwych zagrożeń dopatrywałbym się jednak gdzie indziej.

Dane dotyczące stanu zdrowia chronione są, by chronić osoby, których dane owe dotyczą, przed dyskryminacją.

Ochrona przed dyskryminacją ma znaczenie zwłaszcza w stosunkach zatrudnienia. Przy dzisiejszym rozwoju medycyny z niejaką pewnością, zwłaszcza w przypadku niektórych chorób, wnioskować możemy o przyszłym stanie zdrowia osoby, której aktualny stan zdrowia szczegółowo znamy. Pracodawca, mający pełen dostęp do danych o stanie zdrowia pracownika, mógłby po prostu nie przyjąć do pracy osoby, która nie jest absolutnie zdrowa. Osoba, której obecny, czy też domniemany przyszły stan zdrowia, cechy charakterologiczne, czy wręcz kod DNA, odbiegałyby od idealnego, pożądanego przez pracodawcę wzorca, pracownikiem nie zostałaby nigdy i u nikogo. Podobne problemy osoba taka miałaby w stosunkach ubezpieczeniowych, bowiem ubezpieczyciele najchętniej ubezpieczaliby jedynie osoby absolutnie zdrowe. Można tu wyprowadzić pewną zależność. Choroba to pewna odmienność. odmienność w dodatku niekorzystna z punktu widzenia pracodawcy, odmienność ta grozi dyskryminacją, dyskryminacja grozi wykluczeniem społecznym i może do niego prowadzić, w związku z czym informacje o tym, że ktoś jest chory muszą być chronione.

Dane te powinny również podlegać ochronie ze względu na

³ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997. Dz. U. 1997 Nr 78 poz. 483 ze zm.

żywotne interesy samej placówki medycznej oraz zatrudnionego personelu. Chęć uzyskania rekompensaty finansowej od jednostki, zamiar złożenia wniosku o przeprowadzenie kontroli jej funkcjonowania, a także często potrzeba rozładowania własnych niechęci na przykład niechęci do personelu zatrudnionego w podmiocie, czy wręcz do treści wydanego orzeczenia o stanie zdrowia, stają się motywami działania, jakimi kierują się ludzie starając się w sposób nieuprawniony pozyskać informacje o stanie zdrowia, czy też dokumentację medyczną. Brak dostatecznej ochrony danych osobowych w jednostce otwiera takim ludziom drogę do działania, wręcz zachęca do tego.

Oprócz obowiązku ochrony danych RODO nakłada na administratora wiele innych obowiązków. Prawdę mówiąc, ochronie danych poświęcone jest (zależnie od przyjętej metody liczenia) od 3 % do 5 % tekstu RODO. Reszta RODO to (zaskakujące czasem) obowiązki administratora, równie zaskakujące uprawnienia osób, których dane dotyczą a nade wszystko potencjalnie drakońskie kary za brak realizacji owych uprawnień i obowiązków.

Realizacja uprawnień osób, których dane dotyczą jest kluczowa, z uwagi na bezpieczeństwo prawne administratora.

Wiele uprawnień nie może być zrealizowanych zgodnie z życzeniem osób, których dane dotyczą. Jeżeli na przykład pacjent żąda usunięcia jego danych, to podmiot udzielający świadczeń zdrowotnych⁴ nie może ich usunąć ma bowiem obowiązek przechowywać te

⁴ Podmiot udzielający świadczeń zdrowotnych to podmiot, o którym mowa w art. 2 ust. 1 pkt 5 Ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej, czyli podmiot wykonujący działalność leczniczą (PVDL), za który uznajemy podmiot leczniczy, o którym mowa w art. 4 ww. Ustawy, oraz lekarza, pielęgniarkę lub fizjoterapeutę wykonujących zawód w ramach działalności leczniczej, jako praktykę zawodową, o której mowa w art. 5 ww. Ustawy.

Zgodnie z art. 4 ww. Ustawy podmiotami leczniczymi są niżej wymienione podmioty – w zakresie, w jakim wykonują działalność leczniczą:

- 1) przedsiębiorcy w rozumieniu przepisów ustawy z dnia 6 marca 2018 r. - Prawo przedsiębiorców (Dz. U. z 2021 r. poz. 162) we wszelkich formach przewidzianych dla wykonywania działalności gospodarczej, jeżeli ustawa nie stanowi inaczej,
- 2) samodzielne publiczne zakłady opieki zdrowotnej,
- 3) jednostki budżetowe, w tym państwowe jednostki budżetowe tworzone i nadzorowane przez Ministra Obrony Narodowej, ministra właściwego do spraw wewnętrznych, Ministra Sprawiedliwości lub Szefa Agencji Bezpieczeństwa Wewnętrznego,

dane, zawarte w dokumentacji, przez dziesiątki lat. Co zatem zrobić? Nie pozostaje nic innego niż udać, że realizuje się uprawnienie, zasympulować to. PWDL powinien przyjąć żądanie pacjenta. Rozpatrzyć je, po czym poinformować go, że przez najbliższe na przykład 20 lat nie może ono być zrealizowane. PWDL powinien jednocześnie zachować dowody (np. wydruki, notatki, kopie pism), z których wynika, że w taki właśnie ułomny i dziwaczny sposób zrealizował żądanie.

Przypominamy, że pacjent ma prawo do dostępu do dokumentacji medycznej dotyczącej jego stanu zdrowia oraz udzielonych mu świadczeń zdrowotnych a dane zawarte w dokumentacji medycznej podlegają ochronie. W celu realizacji tego prawa pacjenta podmiot udzielający świadczeń zdrowotnych jest obowiązany prowadzić, przechowywać i udostępniać dokumentację medyczną w sposób określony w Ustawie z dnia 6 listopada 2008r., o prawach Pacjenta i Rzeczniku Praw Pacjenta oraz w ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, a także zapewnić ochronę danych zawartych w tej dokumentacji.

posiadające w strukturze organizacyjnej ambulatorium, ambulatorium z izbą chorych lub lekarza podstawowej opieki zdrowotnej, pielęgniarkę podstawowej opieki zdrowotnej lub położną podstawowej opieki zdrowotnej w rozumieniu przepisów ustawy z dnia 27 października 2017 r. o podstawowej opiece zdrowotnej (Dz. U. z 2020 r. poz. 172 i 1493),

- 4) instytuty badawcze, o których mowa w art. 3 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. 2020 r. poz. 1383),
- 5) fundacje i stowarzyszenia, których celem statutowym jest wykonywanie zadań w zakresie ochrony zdrowia i których statut dopuszcza prowadzenie działalności leczniczej,
- 6) posiadające osobowość prawną jednostki organizacyjne stowarzyszeń, o których mowa w pkt 5,
- 7) osoby prawne i jednostki organizacyjne działające na podstawie przepisów o stosunku Państwa do Kościoła Katolickiego w Rzeczypospolitej Polskiej, o stosunku Państwa do innych kościołów i związków wyznaniowych oraz o gwarancjach wolności sumienia i wyznania,
- 8) jednostki wojskowe.

RODO - obowiązywanie

Akt prawny znany jako RODO jest to „Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG)”. RODO zostało wydane dnia 4 maja 2016 roku. Zgodnie z art. 99 ust. 1 RODO, RODO weszło w życie 25 maja 2016 roku. Zgodnie z art. 99 ust. 2 RODO, RODO „ma zastosowanie” od 25 maja 2018 roku. RODO poprzedzone było Dyrektywą 95/46/WE⁵. Dyrektywa wdrożona była do polskiego porządku prawnego za pomocą ustawy o ochronie danych osobowych⁶ (Dalej: UODO97) i za pomocą innych ustaw jak np. ustawa o zakładach opieki zdrowotnej, czy później ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta. RODO obowiązuje w polskim porządku prawnym wprost.

Zwracam uwagę na fakt, że nieuzasadnione są uwagi, że „RODO kogoś nie obowiązuje, bo to nie jest polska ustawa”. RODO to Rozporządzenie Parlamentu Europejskiego i Rady i nie dość, że obowiązuje ono w Polsce, to w przypadku niezgodności RODO z polskimi aktami krajowymi należy stosować RODO. Nie wskazujemy tu konkretnych źródeł, zdarzyło nam się jednak napotkać takie stanowisko, czy to podczas naszej pracy praktycznej, czy to w fejsbukowych grupach dyskusyjnych poświęconych RODO.

Należy jednocześnie pamiętać, że RODO nie jest jedynym aktem prawnym regulującym sprawy ochrony informacji o pacjencie, postępowanie z dokumentacją medyczną ochronę i udostępnianie dokumentacji. Przede wszystkim należy tu pamiętać o UOPPiRP oraz o Rozporządzeniu Ministra Zdrowia z dnia 6 kwietnia 2020r. w spra-

⁵ Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. OJ L 281, 23.11.1995, p. 31–50.

⁶ Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. 1997 nr 133 poz. 883. ze zm. t.j. Dz.U. 2016 poz. 922. ze zm.

wie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania⁷.

Trzeba też pamiętać o pozostałych rozporządzeniach dotyczących prowadzenia dokumentacji medycznej. Są to: Rozporządzenie Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2020r. w sprawie rodzajów, zakresu i wzorów oraz sposobu przetwarzania dokumentacji medycznej w podmiotach leczniczych utworzonych przez ministra właściwego do spraw wewnętrznych⁸ i Rozporządzenie Ministra Obrony Narodowej z dnia 6 sierpnia 2021 r. w sprawie rodzajów, zakresu i wzorów oraz sposobu przetwarzania dokumentacji medycznej w podmiotach leczniczych utworzonych przez Ministra Obrony Narodowej.⁹ Wskazane rozporządzenia regulują prowadzenie dokumentacji medycznej w podmiotach leczniczych podlegających pod resorty siłowe. Ze względu na to, kontrola PUODO w takich podmiotach wydaje się mało prawdopodobna, jest jednak możliwa.

Przygotowanie dokumentów

Obowiązków dokumentacyjnych, które wynikają z RODO nie powinien zaniedbywać żaden administrator (danych osobowych) – przychodnia, szpital, lekarz prowadzący praktykę itd..., ponieważ każdy administrator powinien liczyć się z tym, że zostanie skontrolowany. Kontrola przetwarzania danych osobowych uregulowana jest w RODO. Praca niniejsza nie dotyczy kontroli, a ochrony danych, dlatego też o kontroli nie piszemy wiele. Kontrola uregulowana w RODO dotyczyć może poszanowania każdego uprawnienia wynikającego z RODO i przestrzegania każdego obowiązku wynikającego z RODO.

Najłatwiej jest skontrolować dokumenty. Jeśli chodzi o kontrolę dokumentów, to przede wszystkim można skontrolować, czy podmiot kontrolowany konkretne dokumenty posiada, o ile zachodzi obowiązek posiadania konkretnych dokumentów.

Poza tym można skontrolować treść dokumentów pod kątem zgodności tej treści z RODO. Można również próbować kontrolować

⁷ Dz.U. 2020 poz. 666 ze zm.

⁸ Dz.U. 2020 poz. 788 ze zm.

⁹ Dz.U. 2021 poz. 1825.

formę dokumentów, nie jest to jednak takie łatwe, bowiem w przypadku zjawisk dokumentacyjnych, które wynikają z RODO, trudno jest o wskazanie jedynej właściwej, przewidzianej prawem formy. Kiedy prawo formy nie przewiduje, to kontroler nie powinien wymagać żadnej konkretnej formy.

Łatwość kontrolowania dokumentów nie jest jednak jedynym powodem, dla którego należy te dokumenty stworzyć. Należy je stworzyć, ponieważ obowiązek taki wynika z RODO. Dokładniej opisujemy to poniżej w podrozdziale: „Dokumentacja jako obowiązek”.

Dokumentacja jako obowiązek

Administrator danych powinien stworzyć dokumenty dotyczące przetwarzania danych osobowych, ponieważ takie obowiązki nakłada na niego RODO. Zdanie to jest oczywiste, jednak twórcy RODO mieli chyba świadomość, że jeżeli nałożą na administratorów (danych) obowiązki i w żaden sposób nie będą karać za nierealizowanie tychże, to jedni administratorzy obowiązki zrealizują, zaś inni nie.

Kilkunastoletnia praca z przepisami o ochronie danych osobowych pozwoliła mi wyrobić sobie własne zdanie na temat obowiązków dokumentacyjnych, związanych z przetwarzaniem danych osobowych. Zdanie to jest dalekie od entuzjazmu. Dokumenty nie chronią danych. To prawda, jednak trzeba te dokumenty mieć. Jeśli administrator nie ma dokumentów, to naraża się na odpowiedzialność. RODO wprowadza, od około 20, do około 40 rozmaitych zjawisk dokumentacyjnych. Piszę „około”, ponieważ użycie tu konkretnej liczby zależy od tego jak dokumenty liczymy i czy każdy obowiązek, który trzeba wykazać, wykazujemy osobnym dokumentem, czy łączymy obowiązki po kilka, w celu ich wykazania jednym dokumentem, miast kilkoma. Dokumenty te, niektóre w wersji skończonej, inne jako półprodukty do uzupełnienia prezentujemy dalej w książce. Dokumenty prezentowane są wynikiem wspólnej, ale niezależnej pracy autorów książki. Jeden z autorów (J. Rz.) pierwsze wersje wzorów opracował, upowszechniał i wdrażał już około roku 2017, zaś po ich klaryfikacji umieścił je w książce dokumentacji poświęconej. Drugi z autorów (D.S.) swoje wzory opracował niezależnie od pierwszego i równie niezależnie się nimi posługiwał. Do niniejszej publi-

kacji wybraliśmy te, które wspólnie uznaliśmy za najlepsze, z różnych, głównie merytorycznych, względów.

RODO nakazuje prowadzić bogatą dokumentację przetwarzania danych osobowych.

Jeżeli administrator nie wytworzy konkretnych, przewidzianych w RODO dokumentów, to administrator ponieść może odpowiedzialność za samo tylko nieposiadanie dokumentów. Wynika to z art. 5 ust. 2 RODO w zw. z art. 83 ust. 5 lit. a RODO.

Jednym z elementów dostosowania się do RODO jest sporządzenie i wdrożenie dokumentacji, obowiązek prowadzenia której wynika z RODO. Dokumentacji tej, między innymi, poświęcona jest niniejsza praca. Praca poświęcona jest również zasadom przetwarzania danych osobowych i realizacji tych zasad z pomocą dokumentacji o której mowa. Za pomocą samej tylko dokumentacji, nie da się w pełni i wyczerpująco zrealizować zasad przetwarzania danych osobowych, mimo tego obowiązków dokumentacyjnych, które wynikają z RODO, nie należy zaniedbywać, bowiem bez dokumentacji zasad zrealizować się nie da.

Pojęcia istotne dla ochrony danych medycznych¹⁰

¹⁰ Rozważania definicyjne prowadzone w niniejszym rozdziale zostały zaczerpnięte z publikacji powstającej równocześnie z niniejszą książką (i wydanej już w momencie ukazania się książki niniejszej), a mianowicie z: J. Rzymowski. *RODO – GDPR. Zasady dotyczące przetwarzania danych osobowych. Zgodność przetwarzania danych osobowych z prawem*. Łódź. 2020.

Pojęcia istotne

dla ochrony danych medycznych

Dane osobowe

Definicja danych osobowych zawarta jest w art. 4 pkt 1 RODO. Wynika z niej jak opisano poniżej.

Dane osobowe to wszelkie informacje o:
osobie fizycznej zidentyfikowanej,
lub o
osobie fizycznej możliwej do zidentyfikowania.
Innymi słowy:

Dane osobowe to informacje o osobie fizycznej, którą można wskazać lub o osobie fizycznej, którą można odróżnić od innych osób fizycznych lub o osobie wskazanej lub o osobie odróżnionej od innych osób fizycznych

W realiach medycznych dane osobowe to wszystkie informacje o pacjentach, które znajdują się w dokumentacji medycznej, wszelkie informacje zbierane o pacjencie np. wyniki badań i wszelkie informacje udostępniane, zwłaszcza jako informacje o stanie zdrowia.

Danymi osobowymi są również informacje o rodzinach pacjentów, zawarte w dokumentacji medycznej, o pracownikach medycznych, zawarte w dokumentacji medycznej.

Zwracam uwagę na **kilka szczegółów dotyczących definicji**. Każda informacja może być daną osobową, o ile tylko wiemy lub możemy ustalić kogo ta informacja dotyczy.

Dane osobowe chronione na gruncie RODO to informacje dotyczące żywych ludzi.¹¹ Motyw 27 Preambuły RODO stanowi:

¹¹ P. Litwiński, P. Barta, M. Kawecki. w: P. Litwiński (red.) P. Barta, M. Kawecki. *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz.* Warszawa 2018. s. 175.

„Niniejsze rozporządzenie nie ma zastosowania do danych osobowych osób zmarłych. Państwa członkowskie mogą przyjąć przepisy o przetwarzaniu danych osobowych osób zmarłych”. W Polsce takimi przepisami są np. przepisy dotyczące ochrony informacji o pacjencie po śmierci pacjenta, przepisy dotyczące tajemnic medycznych itp.¹² Fakt, że RODO nie dotyczy danych osobowych osób zmarłych nie ma dużego znaczenia w realiach medycznych. Codzienne zarządzanie dokumentacją nie jest uzależnione od tego, czy pacjent, którego dokumentacja dotyczy żyje czy nie. Fakt, że RODO nie dotyczy danych osobowych osób zmarłych może mieć znaczenie jeżeli dane ulegną nieuprawnionemu zniszczeniu czy ujawnieniu. Możliwa jest wtedy odpowiedzialność cywilna (np. za naruszenie dóbr osobistych), karna (np. za ujawnienie tajemnic) ale odpowiedzialność na gruncie RODO za ujawnienie czy zniszczenie danych osobowych dotyczących osób zmarłych jest niemożliwa.

RODO nie chroni danych osobowych osób zmarłych, należy jednak chronić te dane z uwagi na krajowe przepisy dotyczące tajemnic i udostępniania informacji o pacjencie.

Dane osobowe to informacje o osobie zidentyfikowanej lub możliwej do zidentyfikowania **nie zaś jedynie** informacje umożliwiające identyfikację osoby. Informacje umożliwiające identyfikację osoby **są**, z samej ich istoty, danymi osobowymi. Jeżeli informacja umożliwia identyfikację osoby, to oczywiście jest że jest informacją o konkretnej osobie i tym samym daną osobową¹³. W realiach medycznych dane osobowe to wszystkie informacje o pacjencie jakie posiada podmiot. Zwłaszcza informacje znajdujące się w dokumentacji medycznej, w tym informacje o imieniu, nazwisku, miejscu zamieszkania. Podkreślenia wymaga, że jeżeli podmiot nie zna imienia i nazwiska

¹² Podobnie: D. Lubasz w: *RODO Ogólne rozporządzenie o ochronie danych. Komentarz*. Red. n. E. Bielak-Jomaa, D. Lubasz. E. Bielak-Jomaa, W. Chomiczewski, M. Czerniawski, P. Drobek, U. Góral, M. Kuba, D. Lubasz, J. Łuczak, P. Makowski, K. Witkowska-Nowakowska, N. Zawadzka. Warszawa 2018. s. 168.

¹³ Rzeczownik „dane”, wbrew powszechnemu pogładowi, posiada w języku polskim liczbę pojedynczą i wygodnie jest jej używać, co czasem czynię. Podobnie jest w języku angielskim: „a piece of data”.

pacjenta (tzw. pacjent NN) to i tak wszystkie informacje o tym pacjencie posiadane przez podmiot są danymi osobowymi.

Danymi osobowymi są też informacje powtarzalne takie jak np. wzrost czy waga pacjenta. Wielu pacjentów ma taki sam wzrost, ale informacja, że ten pacjent ma taki a taki wzrost to dane tego pacjenta. Podkreślamy to szczególnie, zdarzyło nam się bowiem spotkać ze stanowiskiem, że skoro na podstawie na przykład wzrostu, nikogo nie da się zidentyfikować, to informacja o wzroście nie należy do danych osobowych. Prawdą jest, że na podstawie danych powtarzalnych nie da się nikogo zidentyfikować, ale jak napisałem wyżej, dane osobowe to informacje dotyczące osoby zidentyfikowanej lub możliwej do zidentyfikowania a nie tylko informacje umożliwiające identyfikację. Prościej pisząc – dane osobowe to wszystkie posiadane w podmiocie i zbierane oraz udostępniane przez podmiot informacje o pacjencie, członkach jego rodziny, lekarzach, innych pracownikach, kontrahentach – o ile ci są osobami fizycznymi.

Dane spseudonimizowane

Paweł Litwiński pisze: „Ponieważ pseudonimizacja jest czynnością odwracalną, spseudonimizowane dane osobowe należy traktować jak dane osobowe”¹⁴. Pogląd P. Litwińskiego jest zbieżny z wnioskiem, który wypływa z motywu 26 Preambuły RODO, czyli że dane spseudonimizowane to dane osobowe.

Należy zwrócić tu uwagę na pewien niuans. Należy pamiętać, że art. 4 pkt 1 RODO nie ogranicza danych osobowych do informacji, które dotyczą osoby fizycznej identyfikowalnej dla tego czy innego podmiotu czy administratora. Jeśli informacja spełnia warunki z art. 4 pkt 1 RODO, to należy do danych osobowych. To wynika z definicji danych osobowych. Takie podejście ogromnie rozszerza zakres informacji, które są danymi osobowymi.

Należy tu zwrócić uwagę na teleradiologię – jeżeli radiolog opisuje zdjęcia pacjentów oznaczonych pseudonimami, to należy przyjąć że i tak przetwarza on dane osobowe, mimo że podczas opisywania nie wie dokładnie czyje wyniki opisuje.

¹⁴ P. Litwiński, P. Barta, M. Kawecki. *Op. cit.* s. 174.

Dane dotyczące dzieci urodzonych żywo i nie urodzonych żywo

Informacje dotyczące dzieci są danymi osobowymi. Jeśli dziecko urodzi się żywe to informacje go dotyczące, jednak z okresu życia przed urodzeniem, są danymi osobowymi tego dziecka, jeżeli urodzenie żywe nie zajdzie to informacje te są danymi osobowymi jego matki lub/i ojca¹⁵. Dane dziecka nienarodzonego, informacje związane z poronieniem, informacje dotyczące dziecka martwo urodzonego, mogą być (zależnie od sytuacji) danymi ojca, matki, matki biologicznej - surogatki, dawcy nasienia, matki genetycznej - dawczyni komórki jajowej. Kiedy dziecię urodzi się żywe to z kolei dane dotyczące wymienionych osób, są w pewnym zakresie danymi osobowymi dziecięcia.

Należy pamiętać przy tym o prenatalnych danych genetycznych – również są to dane osobowe, odpowiednio dziecięcia lub jego przodków.

Dane genetyczne

Definicja danych genetycznych, będących danymi osobowymi, zawarta jest w art. 4 pkt 13 RODO.

Przepis traktuje zarówno o danych genetycznych uzyskanych po urodzeniu się osoby fizycznej jak i o danych uzyskanych przed urodzeniem się osoby fizycznej, czy o tzw. danych prenatalnych. Dane genetyczne są danymi osobowymi.

Dane genetyczne to dane dotyczące cech genetycznych osoby fizycznej. Cechy genetyczne, o których mowa w przepisie mogą być odziedziczone lub nabyte.

Dane genetyczne dotyczą cech genetycznych ujawniających informacje o fizjologii lub zdrowiu osoby, zarówno informacje, z których wynika, że ktoś jest chory jak i informacje o tym, że ktoś jest zdrowy. Ujawniane informacje o fizjologii lub zdrowiu są niepowtarzalne. Dane genetyczne (osobowe) to dane, które mogą wynikać z analizy próbki biologicznej pochodzącej od osoby fizycznej lub z innych źródeł.

¹⁵ P. Litwiński, P. Barta, M. Kawecki. *Op. cit.* s. 176.

„Dane genetyczne prenatalne

Artykuł 4 pkt 13 RODO dotyczy danych genetycznych. Dane genetyczne, co wiemy z przepisu, to dane osobowe. Dane osobowe to dane dotyczące osoby fizycznej. Dane genetyczne to zatem dane dotyczące osoby fizycznej, czyli żywego człowieka. Zastanowiwszy się nad danymi prenatalnymi należy poczynić kilka uwag.

Jeżeli człowiek żyje, ponieważ się urodził to dotyczące go dane genetyczne uzyskane po jego urodzeniu są danymi osobowymi, które go dotyczą.

Jeżeli człowiek nie żyje, ponieważ się urodził, jednak później zmarł, to dotyczące go dane genetyczne uzyskane po jego urodzeniu są danymi osobowymi, które go dotyczą, jednak RODO nie chroni tych danych.

Jeżeli człowiek żyje, ponieważ się urodził, to dotyczące go dane genetyczne uzyskane przed jego urodzeniem są danymi osobowymi, które go dotyczą.

Jeżeli człowiek nie żyje, ponieważ się urodził, jednak później zmarł, to dotyczące go dane genetyczne uzyskane przed jego urodzeniem są danymi osobowymi, które go dotyczą, jednak RODO nie chroni tych danych.

Jeżeli człowiek jeszcze się nie urodził, ma jednak szansę się urodzić, to dotyczące go dane genetyczne uzyskane przed jego urodzeniem są danymi osobowymi, które go dotyczą, wydaje się jednak, że RODO dotyczy tych danych warunkowo, a mianowicie pod warunkiem, że człowiek ten urodzi się żywy. Dane należy zatem chronić jeszcze przed urodzeniem się człowieka, jeżeli bowiem urodzi się on żywy, to dane uzyskane przed jego urodzeniem są danymi osobowymi.

Jeżeli dane uzyskane przed urodzeniem zostaną jeszcze przed urodzeniem ujawnione, to uważam, że administrator nie powinien ponieść odpowiedzialności administracyjnej, ponieważ chroni go wynikająca z art. 7a KPA¹⁶ zasada tłumaczenia wątpliwości na korzyść uczestnika postępowania a skoro człowiek się jeszcze nie urodził i nie wiadomo czy się urodzi żywy, to nie wiadomo czy RODO chroni informacje, które go dotyczą a zebrane i ujawnione jeszcze przed jego urodzeniem. Niestety administrator danych nie jest tu w pełni bez-

¹⁶ Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego. Dz.U. 1960 nr 30 poz. 168 ze zm. t.j. Dz. U. 2021 poz. 735 ze zm.

pieczny, ponieważ informacje dotyczące tego człowieka są również informacjami dotyczącymi jego rodziców i to niezależnie od tego czy urodzi się żywy.

Jeżeli człowiek jeszcze się nie urodził, i się nie urodzi bo zmarł przed urodzeniem, to dotyczące go dane genetyczne uzyskane przed jego urodzeniem nie są, jak się wydaje, danymi osobowymi, które go dotyczą, ponieważ byt ten, nazwany na początku zdania człowiekiem, nigdy się nie urodził, zatem nie stał się osobą fizyczną. Dane bytu, który nie urodził się żywy należy chronić, ponieważ są to dane jego rodziców, również (odpowiednio) dawczyni komórki jajowej, dawcy nasienia, surogatki.”¹⁷

Przez **dane medyczne** należy rozumieć dane osobowe, które dotyczą medycyny, czyli diagnozowania i leczenia.

Medyczny to: „dotyczący medycyny, związany z medycyną”.¹⁸

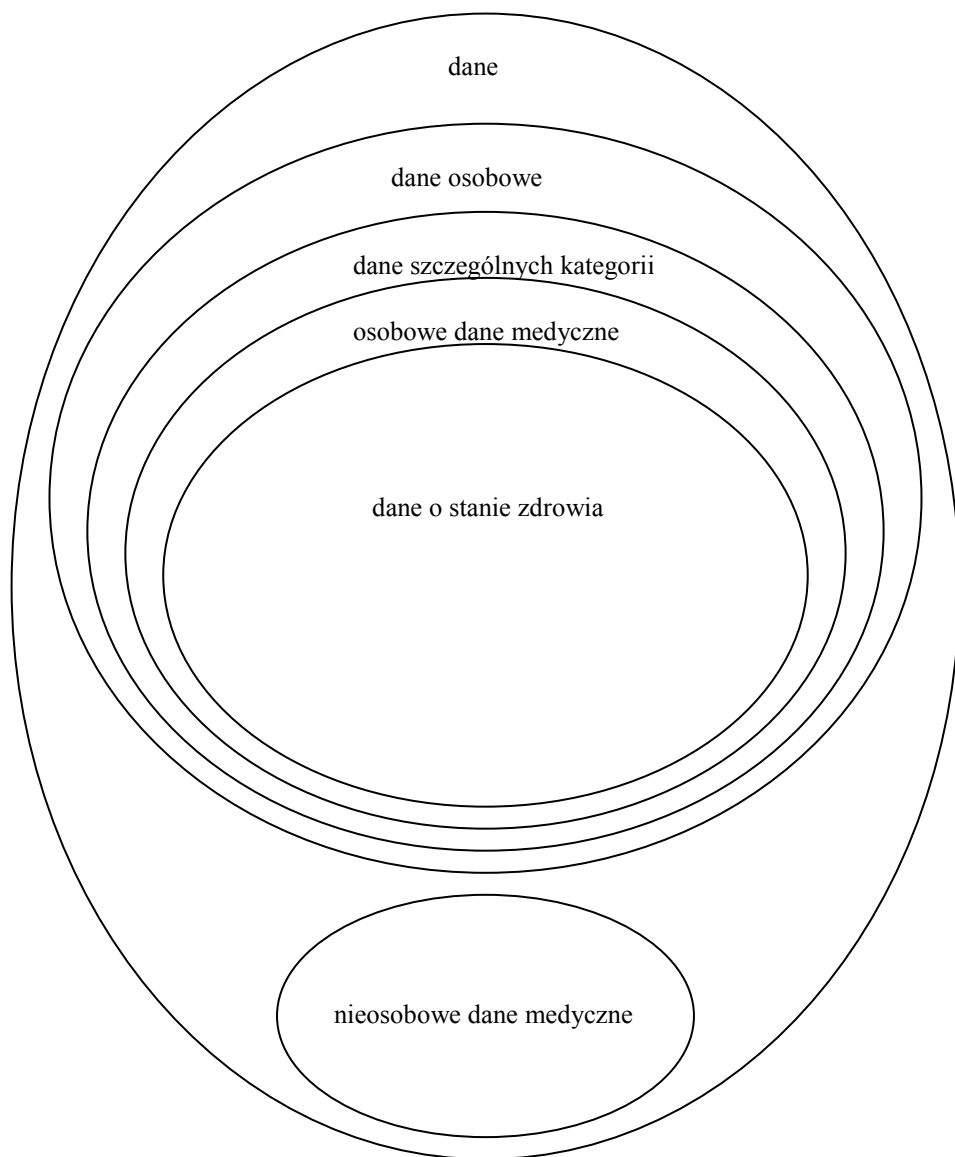
Medycyna to: „nauka obejmująca całość wiadomości o człowieku zdrowym i chorym, mająca za zadanie utrzymywanie zdrowia, leczenie chorych i zapobieganie chorobom; sztuka leczenia”.¹⁹

Dane medyczne, by były chronione jak dane osobowe, muszą jednocześnie być właśnie danymi osobowymi. Z tego względu jestem zwolennikiem używania nazwy „osobowe dane medyczne”.

¹⁷ Cytat lub prawie dokładny cytat z: J. Rzymowski. *RODO – GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje*. Łódź. 2020.s. 551-552.

¹⁸ Słownik języka polskiego. Pod red. W. Doroszewskiego. Warszawa 1963. T. IV

¹⁹ *Loc. cit.*



Ryc. 1: Zależności poszczególnych grup danych.

Źródło: J. Rzymowski, opracowanie własne.

Szczególne kategorie danych, dane wrażliwe, nazewnictwo

Dane nazywane tradycyjnie danymi wrażliwymi zostały w tytule art. 9 RODO nazwane: „szczególnymi kategoriami danych osobowych”. Twórcy RODO utożsamiają nazwę „szczególne kategorie danych osobowych” z nazwą: „dane wrażliwe”.²⁰

W realiach medycznych najczęściej występują następujące kategorie danych szczególnych kategorii:

- dane genetyczne,
- dane biometryczne używane w celu jednoznacznego zidentyfikowania osoby fizycznej,
- dane dotyczące zdrowia,
- dane dotyczące seksualności,
- dane dotyczące orientacji seksualnej.

Pozostałe dane szczególnych kategorii, które rzadko jednak znajdują się np. w dokumentacji medycznej to: dane ujawniające pochodzenie rasowe, dane ujawniające pochodzenie etniczne, dane ujawniające poglądy polityczne, dane ujawniające przekonania religijne, dane ujawniające przekonania światopoglądowe, dane ujawniające przynależność do związków zawodowych.

Przetwarzanie danych osobowych

Definicja przetwarzania (danych osobowych) zawarta jest w art. 4 pkt 2 RODO. Wynika z niej jak opisano poniżej.

Przez przetwarzanie należy rozumieć każdą czynność wykonywaną na danych osobowych od ich zebrania do ich zniszczenia łącznie z ich zbieraniem i z ich niszczeniem.

Prawodawca pozornie definiuje jedynie „przetwarzanie”, jednak z treści definicji wynika, że w istocie definiowane jest „przetwarzanie danych osobowych.

²⁰ Motyw 10 Preambuły RODO zawiera między innymi słowa: „Niniejsze rozporządzenie umożliwia też państwom członkowskim doprecyzowanie jego przepisów, w tym w odniesieniu do przetwarzania szczególnych kategorii danych osobowych (zwanych dalej „danymi wrażliwymi”).”

Przetwarzaniem danych osobowych, w realiach PWDL, jest każda czynność podejmowana w związku z informacjami o pacjencie. Zbieranie danych pacjenta na przykład podczas wywiadu, zbieranie danych w celu założenia historii choroby, przechowywanie dokumentacji, niszczenie dokumentacji, udostępnianie dokumentacji, udostępnianie informacji o stanie zdrowia.

Przetwarzanie to operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych. Inaczej - przetwarzanie to czynność wykonywana na danych osobowych. Już jedna czynność jest przetwarzaniem danych osobowych. Skoro więc już jedna czynność jest przetwarzaniem, to nie ma znaczenia czy rozumiane jako zestaw dwie czynności stanowią jedną czynność, ponieważ stanowią zestaw, czy stanowią dwie, zestawione, jednak osobne, czynności.

Jeżeli czynność nie jest wykonywana na danych osobowych ani na zestawach danych osobowych to nie jest przetwarzaniem (danych osobowych).

W zakresie definicji mieszczą się czynności zautomatyzowane i nieautomatyzowane, czyli wszystkie

W przepisie wymienione są przykładowe czynności przetwarzania danych osobowych.²¹ Przykładowe ale nie wszystkie. Jeżeli zatem jakaś czynność jest wykonywana na danych osobowych ale nie jest wymieniona w przepisie, to też jest czynnością przetwarzania danych osobowych – po prostu przetwarzaniem.

Podmiot przetwarzający

Podmiot przetwarzający zdefiniowany jest w art. 4 pkt 8 RODO. W przepisie zdefiniowano podmiot przetwarzający, jednak w żaden sposób nie powiązano definicji z art. 28 RODO, zatytułowanym: „Podmiot przetwarzający”. Oczywiście „podmiot przetwarzający” o którym mowa w komentowanym przepisie i „podmiot przetwarzający”, o którym mowa w art. 28 RODO, to ten sam podmiot, ten sam podmiot przetwarzający, co wynika z dyrektywy języka prawnego²².

²¹ Podobnie: P. Litwiński, P. Barta, M. Kawecki. *Op. cit.* s. 197.

²² L. Morawski. *Zasady wykładni prawa*. Toruń 2006 s. 93–95, M. Zirk–Sadowski w: *System Prawa Administracyjnego* Red: R. Hauser, Z. Niewiadomski, A. Wróbel. *Tom IV. Wykładnia w prawie administracyjnym*. L. Leszczyński, B. Wojciechowski, M. Zirk–Sadowski. Warszawa 2012. s. 199.

W art. 28 RODO zawarto przepisy doprecyzowujące definicję podmiotu przetwarzającego, a przede wszystkim przepisy ustanawiające obowiązki podmiotu przetwarzającego, mimo tego, jeżeli podmiot spełnia warunki wynikające z art. 4 pkt 8 RODO to jest podmiotem przetwarzającym, niezależnie od tego, czy podmiot ten spełnia również warunki z art. 28 RODO.

Podmiotem przetwarzającym, może być każdy podmiot lub osoba.²³

Podmiotem przetwarzającym może być osoba fizyczna.

Podmiotem przetwarzającym może być osoba prawna.

Podmiotem przetwarzającym może być organ publiczny.

Podmiotem przetwarzającym może być jednostka.

Podmiotem przetwarzającym może być inny podmiot.

Warunkiem by podmiot lub osoba był podmiotem przetwarzającym jest, by ten podmiot lub osoba przetwarzał dane osobowe w imieniu administratora.

Przykładowe podmioty przetwarzające

Poniżej wymieniamy podmioty, które są podmiotami przetwarzającymi, zatem **należy** podpisywać z nimi umowy powierzenia przetwarzania (jest to obowiązek).

Biuro rachunkowe

Podmiot przetwarzający.

Trafny jest pogląd, że biuro rachunkowe powinno podpisywać ze swoimi klientami umowy powierzenia przetwarzania danych osobowych.

Dostawcy usługi serwera na WWW na prowadzenie www i bip²⁴

Wykonują czynności na danych osobowych, są więc podmiotami przetwarzającymi.

Dostawcy oprogramowania

do zdalnego w chmurze prowadzenia dok. medycznej²⁵

Zachodzi co najmniej przechowywanie danych osobowych – są oni zatem podmiotami przetwarzającymi.

²³ Podobnie: P. Litwiński, P. Barta, M. Kawecki. *Op. cit.* s. 225-226.

²⁴ Problem - D.S. omówienie – J.Rz.

²⁵ Problem - D.S. omówienie – J.Rz.

Przykładowe podmioty nie będące podmiotami przetwarzającymi

Poniżej wymieniamy podmioty, które nie są podmiotami przetwarzającymi, zatem **nie wolno** podpisywać z nimi umowy powierzenia przetwarzania. Zwracamy uwagę, że podpisanie umowy z tymi podmiotami jest błędem! Nie wolno tego lekceważyć.

„Należy podkreślić że umowa powierzenia przetwarzania nie ustanawia między stronami umowy relacji administrator/podmiot przetwarzający w sytuacji, kiedy przetwarzanie danych przez jeden podmiot (podmiot przetwarzający) w imieniu drugiego podmiotu (administrator danych) nie zachodzi. Podmiot przetwarzający zdefiniowany jest w artykule 4 pkt 8 RODO i definicja tego podmiotu w żaden sposób nie jest związana z umową powierzenia przetwarzania. Jeżeli zatem administrator udostępni dane innemu podmiotowi, który staje się nowym administratorem i jednocześnie podpisze z tym podmiotem umowę powierzenia przetwarzania to taki podmiot – (nowy) administrator nie staje się w wyniku podpisania tej umowy podmiotem przetwarzającym, jeżeli przetwarzanie danych osobowych w imieniu administratora danych nie zachodzi. Podmiot taki – (nowy) administrator może jednak uważać, że skoro podpisano z nim umowę powierzenia przetwarzania to w wyniku podpisania tej umowy stał się podmiotem przetwarzającym, w związku z czym nie spoczywają na nim obowiązki które spoczywają na administratorze danych. Pierwszym obowiązkiem którego nowy administrator uważający że jest podmiotem przetwarzającym nie realizuje jest obowiązek informacyjny wynikający z artykułu 14 RODO. Opisany tu problem może skutkować odpowiedzialnością administracyjną i cywilną po stronie (nowego) administratora który uważa, że jest podmiotem przetwarzającym.”²⁶

Podmiot świadczący usługę medycyny pracy

Odbiorca, administrator, nie podmiot przetwarzający.

Usługa medycyny pracy nie jest czynnością na danych osobowych. Poza tym podmiot świadczący te usługi, świadczy ja w swoim imieniu, fabryka np. młotków nie może świadczyć sama sobie czynności z zakresu medycyny pracy, zatem jeśli są one dla niej świadczone, to w imieniu zleceniobiorcy, nie w imieniu fabryki.

²⁶ J. Rzymowski. *RODO – GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje*. Łódź. 2020. s. 358-359.

Ponadto podmiot świadczący usługę medycyny pracy wykonuje ją w sposób opisany w przepisach.

Adwokat

Odbiorca, administrator, nie podmiot przetwarzający.

Usługa adwokacka nie jest czynnością na danych osobowych. Usługa adwokacka to (upraszczając) doradztwo i reprezentowanie, nie są to czynności na danych osobowych. Zlecenie usługi adwokackiej nie jest zleceniem czynności na danych osobowych.

Ponadto adwokat wykonuje usługę w sposób opisany w przepisach.

Kancelaria prawna²⁷

Odbiorca, administrator, nie podmiot przetwarzający.

Adwokat, radca prawny, doradca podatkowy są administratorami.

Wymienieni przetwarzają dane osobowe w swoim imieniu, w sposób wynikający z przepisów zawodowych.

Zlecenie usługi wymienionych nie jest zleceniem czynności na danych.

Należy tu odróżnić świadczenie usługi adwokackiej czy radcowskiej, od sytuacji kiedy człowiek, który jest adwokatem lub radcą prawnym, wykonuje inną funkcję i jej wykonywanie odbywa się w warunkach powierzenia. Uważam, że sytuacja ta **nie** zachodzi kiedy adwokat lub radca prawny wykonuje czynności doradcze np. przy procedurze związanej z udzieleniem zamówienia publicznego.

Adwokat/radca powinni być tu traktowani jak pracownicy, zjawisko przetwarzania danych osobowych w takiej sytuacji nie zachodzi, choć przyznam, że spotkałem się też²⁸ z poglądem przeciwnym, który jednak uważam za mylny, z przyczyn opisanych wyżej.

Doradca podatkowy²⁹

Odbiorca, administrator, nie podmiot przetwarzający.

Usługa doradztwa podatkowego nie jest czynnością na danych osobowych. Usługa doradztwa podatkowego to (upraszczając) doradztwo i reprezentowanie, nie są to czynności na danych osobowych. Zlecenie usługi doradztwa podatkowego nie jest zleceniem czynności na danych osobowych.

Ponadto doradca podatkowy wykonuje usługę w sposób opisany w przepisach.

²⁷ Pytanie internauty o nicku FB - Tomuś Thomas

²⁸ Pogląd internauty o nicku FB - Tomuś Thomas

²⁹ Problem: (doradca podatkowy jako administrator), (biuro rachunkowe jako?), (biegły rewident jako?) został postawiony przez internautę, Bogdana Gibulę.

Pracodawca wobec danych studenta na praktykach zawodowych³⁰

Pracodawca jest administratorem, z tej prostej przyczyny, że praktyki zawodowe nie są czynnością na danych. Niezależnie od istoty relacji między uczelnią a pracodawcą (odpłatna, bezpłatna, umowa, porozumienie), to w relacji tej nie zachodzi powierzenie, ponieważ przedmiotem umowy nie jest czynność na danych.

Przedsiębiorstwo szkoleniowe³¹

Jest administratorem, usługa szkoleniowa nie jest usługą na danych.

Jest administratorem ponieważ zlecenie usługi szkoleniowej nie jest zleceniem czynności na danych osobowych.

W związku ze świadczeniem usługi szkoleniowej mają miejsce czynności na danych, np. wystawienie zaświadczeń, odnotowanie obecności słuchaczy. Uważam, że są to czynności, które zleceniobiorca wykonuje we własnym imieniu w celu wykonania umowy szkoleniowej.

Można próbować wywodzić, że umowie szkoleniowej (bez umowy powierzenia) towarzyszy czasem umowa powierzenia związana właśnie np. z weryfikacją obecności pracowników. Uważam, że jest to niepotrzebne komplikowanie relacji, uważam, że dopuszczalne jest by uznać, że sprawdzenie obecności jest elementem usługi szkoleniowej.

Firma szkoląca z zakresu BHP³²

Jest tu analogicznie jak z firmą szkolącą z jakiegokolwiek innego zakresu.

Jest administratorem, usługa szkoleniowa BHP nie jest usługą na danych.

Jest administratorem ponieważ zlecenie usługi szkoleniowej BHP nie jest zleceniem czynności na danych osobowych.

W związku ze świadczeniem usługi szkoleniowej BHP mają miejsce czynności na danych, np. wystawienie zaświadczeń, sporządzenie listy obecności, przeprowadzenie egzaminów. Uważam, że są czynności, które zleceniobiorca wykonuje we własnym imieniu w celu wykonania umowy szkoleniowej BHP.

Można próbować wywodzić, że umowie szkoleniowej BHP (bez umowy powierzenia) towarzyszy czasem umowa powierzenia związana właśnie np. z weryfikacją obecności pracowników. Nie jestem w stanie podać źródła, ale jest to pogląd zasłyszany. Uważam, że jest to niepotrzebne komplikowanie relacji, uważam, że dopuszczalne jest by uznać, że sprawdzenie obecności jest elementem usługi szkoleniowej BHP.

³⁰ Problem postawiony przez internautkę Elżbietę Dąbrowicz w grupie FB.

³¹ Problem postawiła internautka Basia Matczyńska w grupie FB.

³² Problem postawiła internautka Basia Matczyńska w grupie FB.

Nie sposób zgodzić się tu z poglądem wyrażonym przez Ministerstwo Cyfryzacji w poradniku „RODO dla administracji”. Poradnik ten ma postać pytań i odpowiedzi. Pytanie brzmi: „Czy z firmą prowadzącą szkolenia BHP należy zawrzeć umowę powierzenia?”. Cytuję dalej słowa, są bowiem dowodem na brak zrozumienia zjawiska powierzenia przetwarzania danych przez anonimowych niestety autorów poradnika.³³ „W sytuacji, gdy zadania służby BHP powierzono specjalistom spoza zakładu pracy np. firmie zewnętrznej, administrator zobligowany jest do zawarcia umowy powierzenia danych osobowych. Umowa taka nakłada na podmiot, któremu dane powierzono do przetwarzania, obowiązek odpowiedniego zabezpieczenia danych, zgodnie z wytycznymi, zawartymi w RODO.”. Prawdą jest, że specjalista BHP powinien chronić dane zgodnie z RODO, to jest oczywiste, jednak czynności specjalisty BHP nie są czynnościami na danych osobowych. Pracodawca powierza czynności z zakresu BHP zewnętrznemu wobec pracodawcy podmiotowi. Podmiot wykonuje te czynności na pewno dla pracodawcy, na pewno na zlecenie pracodawcy, być może nawet w imieniu pracodawcy, ale nie są to czynności na danych. Są to głównie czynności szkoleniowe, którym czynności na danych jedynie towarzyszą.

Podmiot medyczny

sprawujący opiekę nad pracownikiem w „pakiecie medycznym”

Jest administratorem.

Zlecenie opieki medycznej nad pracownikami nie jest zleceniem czynności na danych.

Poza tym podmiot leczniczy ma własne cele wynikające z aktów prawnych.

Przedsiębiorstwo ubezpieczeniowe,

na przykład przy ubezpieczeniach grupowych pracowników administratora

Jest administratorem.

Ma własne cele wynikające z ustawy.

Umowa, na mocy której pracodawca ubezpiecza pracowników nie jest umową zlecenia czynności na danych.

³³ *RODO dla administracji*. Ministerstwo Cyfryzacji Styczeń 2019. Projekt: Wydział Komunikacji, Ministerstwo Cyfryzacji. Poradnik dostępny ze strony: <https://www.gov.pl/web/cyfryzacja/przewodnik-po-rodo> (dostęp: 27.02.2022 godz. 16:52)

Podmioty medyczne, do których inny podmiot kieruje z wykorzystaniem skierowania,³⁴ w tym podmioty świadczące usługi z zakresu diagnostyki laboratoryjnej.

Podmioty te mają własne cele wynikające z przepisów.

Umowa między podmiotem a podmiotem nie jest umową zlecenia czynności na danych.

Można przyjąć, że każdy podmiot wykonujący działalność leczniczą jest osobnym administratorem. Tak samo relacja ze skierowaniem z podmiotu do podmiotu jest relacją ADO-ADO, czyli administrator-administrator.

Tu odrobinę inaczej jest w badaniach klinicznych, tam bowiem nakładają się role. Sponsor jest administratorem. Ośrodek badawczy jest podmiotem przetwarzającym i administratorem (np. z uwagi na własny obowiązek przechowywania dokumentacji).

Związek zawodowy

Administrator, nie podmiot przetwarzający.

Posiada własne cele wynikające z przepisów.

Kurierzy dla listów i kurierzy dla materiału biologicznego³⁵

Odbiorca, administrator, nie podmiot przetwarzający.

Usługa kurierska nie jest czynnością na danych osobowych.

Transport sanitarny³⁶

Odbiorca, administrator, nie podmiot przetwarzający.

Usługa transportu sanitarnego nie jest czynnością na danych osobowych.

³⁴ Problem postawił internauta Romuald Maria Walewski w grupie FB.

³⁵ Problem - D.S. omówienie – J.Rz.

³⁶ Problem - D.S. omówienie – J.Rz.

Podmioty, które zależnie od sytuacji są podmiotami przetwarzającymi lub nie³⁷

Podmioty świadczące usługę IT – zdalnie lub stacjonarnie.

Zależy to od rodzaju usługi, jeżeli podmiot na przykład zajmuje się odtwarzaniem i sprawdzaniem kopii to jest podmiotem przetwarzającym, jeżeli zajmuje się np. aktualizacją oprogramowania – nie jest podmiotem przetwarzającym.

Osoby administrujące stroną www z firm zewnętrznych dodających zlecone treści na www.

Jeśli treści zawierają dane osobowe, to osoby takie są podmiotami przetwarzającymi.

Serwisanci sprzętu medycznego

Zależy to od rodzaju serwisu.

Serwisant wirówki czy lodówki jest stroną trzecią.

Serwisant sprzętu zawierającego bazę danych osobowych jest:

Podmiot przetwarzający – jeżeli na zlecenie administratora dokonuje np. odzysku danych

Administrator danych – jeżeli zlecono mu np. aktualizację oprogramowania i po dokonaniu tejże, musi dokonać typowych czynności na żywej bazie.

Umowy powierzenia w praktyce NIK

Niestety prawo sobie a organy je stosujące sobie. Wyżej piszemy kiedy należy zawierać umowy powierzenia przetwarzania a kiedy, w żadnym razie czynić tego nie należy. Niestety dzieje się jak opisujemy poniżej.

Najwyższa Izba Kontroli, podczas kontroli przeprowadzanych w podmiotach medycznych zwraca również uwagę na sprawy związane z ochroną danych osobowych. Nie byłoby w tym nic złego, gdyby kontrolerzy kontrolowali i wykazywali spostrzeżone nieprawidłowości. Tymczasem dzieje się rzecz straszna. Otóż kontrolerzy NIK kontrolują przetwarzanie danych osobowych w podmiotach medycznych i w zakresie zawierania umów powierzenia przetwarzania, wykazują nieprawidłowości tam gdzie ich nie ma. Posuwamy się do takiej retoryki, ponieważ szkody, jakie przynosi taka działalność NIK, długo bę-

³⁷ Problem - D.S. Omówienie – J.Rz.

dą trudne do usunięcia. Wystąpienia pokontrolne są jawne. Czytają je nie tylko podmioty kontrolowane ale i inne podmioty medyczne. Czytają i, co gorsza, mogą dostosować swoją praktykę do fantasmagorycznych oczekiwań NIK. NIK stwierdza brak umów powierzenia przetwarzania w sytuacjach, w których umów tych, pod żadnym pozorem, zawierać nie należy.

Niżej odnosimy się do dwóch wystąpień pokontrolnych NIK, w zakresie dotyczącym obowiązku zawierania umów powierzenia przetwarzania danych osobowych. Wystąpienia te wybraliśmy, są bowiem reprezentatywne dla błędów popełnianych przez NIK. Cytujemy fragmenty wystąpień i odnosimy się do nich.

Cytujemy: „Ustalono, że umowy dotyczące powierzenia przetwarzania danych zawierano z podmiotami (wykonawcami) realizującymi na rzecz Szpitala zadania związane m.in. ze: świadczeniem usług informatycznych oraz serwisu oprogramowania, badaniami z zakresu diagnostyki obrazowej, usługami laboratoryjnymi, współpracy i konsultacji medycznych.”³⁸

- **Świadczenie usług informatycznych.** Nie zabieramy tu głosu, ponieważ powierzenie może tu zachodzić lub nie, zależnie od rodzaju usługi.
- **Serwis oprogramowania.** Kwestia czy zachodzi tu powierzenie czy nie powinna być rozpatrzona zależnie od szczegółów zlecenia jednak ... Jednak jeżeli zlecenie dotyczyło usunięcia usterek oprogramowania a dostęp serwisantów do danych osobowych zachodził niejako przy okazji, to zwracamy uwagę, że zlecniodawca nie zlecał czynności na danych osobowych. Zlecniodawca zleca czynność na oprogramowaniu, na systemie informatycznym itd. Czynności na danych osobowych towarzyszą czynności zleconej. Czynności na danych są czasem konieczne, na przykład do przetestowania oprogramowania przed i po serwisie, nie są one jednak istotą zlecenia. W takiej sytuacji przedsiębiorstwo serwisujące jest odbiorcą danych czyli nowym administratorem. Podstawę prawną do przetwarzania danych osobowych przez przedsiębiorstwo serwisujące stanowi art. 6 ust 1 lit f RODO (prawnie uzasadniony interes

³⁸ Wystąpienie pokontrolne. LZG. 410.002.04.2019. s. 12.

administratora wynika z obowiązku realizacji umowy zawartej ze szpitalem, umowy serwisowej, nie umowy powierzenia przetwarzania ponieważ takowa nie powinna tu mieć miejsca (!) w zw. z art. 9 ust. 2 lit. h RODO (zapewnienie zarządzania systemami opieki zdrowotnej). Dla uczynienia zadość wymogowi wynikającemu z art. 9 ust. 3 RODO czyli przetwarzania danych przez pracownika, na którym spoczywa obowiązek zachowania tajemnicy zawodowej, pracodawca, czyli firma serwisowa powinna zobowiązać go do zachowania w tajemnicy informacji, z którymi zapozna się przy serwisowaniu, w tym danych osobowych pacjentów. Dla uczynienia zadość obowiązkom wynikającym z art. 6 ust. 1 lit. f RODO należy przeprowadzić test równowagi i postąpić zgodnie z jego wynikiem. Można jednak, dla potrzeb niniejszego rozważania, przyjąć, że wynik testu pozwoli na udostępnienie danych w sytuacji kiedy jest to niezbędne do serwisu.

- **Badania z zakresu diagnostyki obrazowej. Badania laboratoryjne.** Nie należy zawierać umowy powierzenia przetwarzania ze wskazanymi poniżej względów.
- Podmiot świadczący usługę diagnostyki obrazowej, laboratorium przetwarzają dane osobowe we własnym imieniu. Dowodem na to jest fakt, że tworzą one własną dokumentację medyczną, ponoszą odpowiedzialność za źle wykonane badanie.
- Podmiot świadczący usługę diagnostyki obrazowej, laboratorium wykonują działalność uregulowaną prawem³⁹ w taki sposób, że działają w sposób, który nie dopuszcza przyjmowania wskazówek od zleceńodawcy. Rentgenodiagnosta (lub inny diagnosta), diagnosta laboratoryjny wykonuje swój zawód i w ramach skierowania wykonuje czynności, wykonuje badanie, jednak techniczne parametry ustala sam i ponosi za to odpowiedzialność. Przetwarza dane osobowe we własnym imieniu. Dowodem na to jest fakt, że tworzy on własną dokumentację medyczną, ponosi odpowiedzialność za źle wykonane badanie.
- Szpital nie może skutecznie żądać zwrócenia danych od podmiotu świadczącego usługę diagnostyki obrazowej ani od laborato-

³⁹ Ustawa z dnia 27 lipca 2001r. o diagnostyce laboratoryjnej. Dz.U. z 2001r., Nr 100, poz. 1083 ze zm. t.j. Dz.U. z 2019r., poz. 849.

rium, gdyż te tworzą własną dokumentację medyczną i mają obowiązek ją przechowywać.

-- Szpital nie zleca wykonania czynności na danych. Szpital zleca wykonanie badania, którego efektem są co prawda dane osobowe, jednak istotą zlecenia jest badanie.

- **Konsultacje medyczne.** Wystąpienie pokontrolne jest tu niekonkretne, jednak jeżeli lekarz opiniuje, diagnozuje, konsultuje, to lekarz działa we własnym imieniu, czyli nie w imieniu szpitala zlecającego „konsultację”, czyli powierzenie tu nie zachodzi. Nie zachodzi ono nawet gdyby umowę podpisano. Lekarz i tak jest administratorem.

- „W dziesięciu przypadkach Szpital zawarł i realizuje umowy główne w zakresie zlecenia lub realizacji świadczeń zdrowotnych na rzecz pacjentów (własnych lub kontrahenta) lub usług serwisowych programów informatycznych, w których przetwarzane są dane osobowe, a tylko sześć z nich ujęto w prowadzonym wykazie umów powierzenia przetwarzania danych.”⁴⁰. Umowy, o których tu mowa, to umowy, do których odnosimy się powyżej, zwracamy jednak uwagę, że nie ma obowiązku prowadzenia wykazu umów powierzenia przetwarzania danych. Nieuwzględnienie umów w takowym wykazie (abstrahując tu od obowiązku ich zawierania) nie jest naruszeniem jakiegokolwiek przepisu, obowiązek posiadania takiego wykazu jest niczym innym jak erupcją fantazji kontrolerów.

Śmieszny byłby wniosek pokontrolny zawarty w omawianym wystąpieniu. Byłby śmieszny, gdyby nie był straszny. Wniosek ten brzmi: „Podjęcie skutecznych działań w celu zawarcia z wszystkimi kontrahentami Szpitala umów powierzenia przetwarzania danych osobowych w sytuacji, kiedy występuje przetwarzanie tych danych przez Szpital lub kontrahenta Szpitala.”⁴¹. Trzeba napisać to otwarcie. Wskutek niekompetencji, NIK, przynajmniej częściowo, wnioskuje tu by podmiot łamał prawo. Oczywiście może się zdarzyć, że szpital po-

⁴⁰ Wystąpienie pokontrolne. LZG. 410.002.04.2019. s. 18.

⁴¹ Wystąpienie pokontrolne. LZG. 410.002.04.2019. s. 20.

wierza przetwarzanie danych (hosting BIP, przechowywanie backupów danych), może się zdarzyć, że szpital jest podmiotem przetwarzającym (teoretycznie, trudno tu o przykład) i wtedy wniosek NIK byłby na miejscu, jednak tak sformułowany wniosek to zachęta do łamania prawa. Zachęta niebezpieczna. Może się zdarzyć, że szpital podpisze umowę powierzenia z nowym administratorem, ten nie realizuje art. 13 RODO, co może skutkować monstrualną odpowiedzialnością administracyjną oraz odpowiedzialnością cywilną o nieustalonym jeszcze w drodze orzecznictwa zakresie finansowym.

Cytujemy: „Ustalono, że umowy dotyczące powierzenia przetwarzania danych zawierano z podmiotami (wykonawcami) realizującymi na rzecz Szpitala zadania związane m.in. z wykonywaniem badań laboratoryjnych i diagnostycznych, świadczeniem usług informatycznych oraz opieki serwisowej, obsługą prawną, świadczeniem usług hostingowych i brokerskich.”⁴² Częściowo odsyłamy wyżej, do omówienia elementów Wystąpienia pokontrolnego LZG. 410.002.04.2019.

- **Badania laboratoryjne i diagnostyczne.** Podmioty je wykonujące są administratorami danych.
- **Świadczenie usług informatycznych i opieka serwisowa.** Zależnie od szczegółów zlecenia, przypominamy jednak, że sam tylko dostęp do danych uzyskany przez zleceniobiorcę, nie skutkuje powierzeniem przetwarzania.
- **Obsługa prawna.** Adwokat, radca – działają we własnym imieniu, zgodnie z prawem i ze swoją wiedzą. Usługa adwokata lub radcy nie jest czynnością na danych wykonywaną w imieniu szpitala. Usługa ta ma szerszy zakres, przetwarzanie danych jest jej elementem.
- **Usługi hostingowe.** Powierzenie przetwarzania zachodzi.
- **Usługi brokerskie.** Prawdopodobnie chodzi o brokera ubezpieczeniowego. Broker ubezpieczeniowy jest odbiorcą, administratorem. „agent ubezpieczeniowy działa na rzecz zakładu ubezpieczeń. Broker ubezpieczeniowy działa na rzecz i w imieniu klienta, czyli osoby chcącej zawrzeć ubezpieczenie czyli szpitala. Broker jest administratorem, nie podmiotem przetwarzającym. Celem brokera

⁴² Wystąpienie pokontrolne. LZG. 410.002.03.2019. s. 10.

jest pośrednictwo ubezpieczeniowe, czyli (nieco upraszczając) zawarcie umowy ubezpieczenia, ale w imieniu klienta, podmiotu ubezpieczonego - szpitala. Odróżnia go to od agenta, którego celem jest zawarcie umowy w imieniu zakładu ubezpieczeń.”⁴³

Cytujemy: „Według stanu na 25 lutego 2019 r. usługi na rzecz Szpitala świadczyło na podstawie kontraktów 27 lekarzy (lekarze kontraktowi), przy czym każdy z nich posiadał odrębne imienne pisemne upoważnienie do przetwarzania danych osobowych – z ww. lekarzami nie zawierano umów (porozumień) dotyczących powierzenia przetwarzania danych osobowych.

IOD wyjaśniła, że *z lekarzami zatrudnionymi na kontrakcie nie są zawierane umowy powierzenia przetwarzania danych osobowych, ponieważ nie są oni zobowiązani do samodzielnego prowadzenia dokumentacji medycznej. Prowadzą oni tę dokumentację w imieniu Szpitala. Osoby takie podpisują oświadczenie poufności oraz uzyskują upoważnienie do przetwarzania danych osobowych nadane przez ADO. Osoby te są szkolone w zakresie ochrony danych osobowych. W zakresie przestrzegania ochrony danych osobowych traktowani są jak pracownicy Szpitala.*”⁴⁴ Nie mamy tu zastrzeżeń, powierzenie przetwarzania byłoby błędem. Nadawanie pisemnych, imiennych upoważnień, w sytuacji posiadania kontraktu też jest niepotrzebne, ale sprawy tej tu nie rozwijamy, szkoda jednak, że NIK nie zwrócił uwagi na fakt, że upoważnienia nadano niepotrzebnie.

Cytujemy: „W dwóch przypadkach (...) Szpital zawarł i realizuje umowy główne jako Administrator, a nie zostały zawarte umowy powierzenia przetwarzania danych osobowych (odmowa zawarcia takiej umowy przez podmioty przetwarzające), co stanowiło naruszenie przepisu art. 28 RODO.

⁴³ J. Rzymowski. *RODO – GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje*. Łódź. 2020. *Komentarz do art. 4 pkt. 8.* (3.11. Art. 4 pkt 8. Uwaga 11. Przykładowi odbiorcy, administratorzy danych, nie podmioty przetwarzające.) (W trakcie pisania niniejszej publikacji, cytowany Komentarz był jeszcze pisany, słowa cytowane mogły ulec zmianie. Cytat został przekształcony, pod kątem tematyki niniejszej książki.).

⁴⁴ Wystąpienie pokontrolne. LZG. 410.002.03.2019. s. 11.

Dyrektor Szpitala wyjaśniła, że „(...) w przypadku pierwszej firmy, pomimo zawarcia umowy, której przedmiotem były badania diagnostyczne w zakresie Tomografu Komputerowego i Rezonansu Magnetycznego Szpital nigdy nie korzystał z jej usług. Po wejściu w życie przepisów RODO Szpital zwrócił się do niej z prośbą o zawarcie umowy powierzenia. Spółka odmówiła zawarcia umowy na formularzu przygotowanym przez Szpital uzasadniając, iż jako duża korporacja przygotowuje własny wzór umowy, który zostanie przesłany do wszystkich kontrahentów. W związku z powyższym do chwili podpisania umowy powierzenia Szpital nie zleca badań Spółce. W przypadku drugiego podmiotu Szpital planuje podjęcie dalszych kroków w celu zawarcia umowy powierzenia.”.⁴⁵

Badanie tomograficzne nie stanowi przetwarzania danych w imieniu szpitala, więc podpisanie umowy powierzenia przetwarzania byłoby tu błędem. Podmiot wykonujący badanie tomograficzne prowadzi je w oparciu o przepisy prawa, prowadzi własną dokumentację, której oryginałów na pewno nie wyda szpitalowi, choćby ów tego żądał. Szpital nie zleca czynności na danych, szpital zleca wykonanie badania – użycie sprzętu, przygotowanie pacjenta do badania itp. – dane są wynikiem badania, z kolei dane przekazane w skierowaniu są konieczne do wykonania badania, zleceńbiorca przetwarza je w swoim imieniu bo do niego skierowano pacjenta. Odmowa spółki uchroniła szpital i spółkę świadczącą usługę przed zawarciem umowy, jednak uzasadnienie odmowy każe sądzić, że spółka ta umowy takie zawiera. Zawiera i występuje w roli podmiotu przetwarzającego, podczas gdy jest administratorem danych, co z kolei prowadzi do wniosku, że spółka prawdopodobnie nie realizuje art. 13 RODO, choćby za pośrednictwem zleceniodawcy czyli szpitala. Nie zawarcie umowy powierzenia przetwarzania z przedsiębiorstwem świadczącym usługę tomografu komputerowego i rezonansu magnetycznego jest właściwe i w żadnym razie, wbrew temu co pisze NIK, nie stanowi naruszenia art. 28 RODO. NIK wnioskuję o zawarcie umowy powierzenia przetwarzania, w opisanej sytuacji,⁴⁶ co wobec absurdalności stwierdzenia przez NIK naruszenia, tam gdzie owo nie zachodzi, nie powinno dzi-

⁴⁵ Wystąpienie pokontrolne. LZG. 410.002.03.2019. s. 11.

⁴⁶ Wystąpienie pokontrolne. LZG. 410.002.03.2019. s. 17.

wić, jednak dziwi, bo jest to wniosek o złamanie prawa. Co gorsza realizacja tego wniosku może doprowadzić przedsiębiorstwo świadczące usługę tomografii i rezonansu do sytuacji, w której owo przedsiębiorstwo, mylnie uważając, że jest podmiotem przetwarzającym, nie zrealizuje art. 13 RODO. Przedsiębiorstwo to i tak, jak sądzimy, nie realizuje obowiązku z art. 13 RODO wobec osób, które bada, ponieważ prawdopodobnie podpisuje ze zleceniodawcami umowy powierzenia przetwarzania, w których występuje jako podmiot przetwarzający. Czyni to jednak ono na swoje ryzyko, teraz będzie ono prawdopodobnie łamało prawo, zachęczone do tego przez NIK.

Przykłady z kolejnych wystąpień pokontrolnych NIK można mnożyć. Ewidentnie w NIK, w zakresie rozumienia zjawiska powierzenia przetwarzania, różnicy między administratorem danych a podmiotem przetwarzającym, zwłaszcza w realiach medycznych, zachodzi jakiś problem systemowy. To nie jest niekompetencja kontrolerów. Wręcz przeciwnie, kontrolerzy szukają naruszeń w konkretnej sferze i je znajdują. Tyle tylko, że o ile szukają dobrze, o tyle znajdują naruszenia tam gdzie ich nie ma. Konieczne wydaje się doszkolenie kontrolerów przez kogoś kompetentnego i wyjaśnienie im, że błędzą.

Działania do podjęcia przez podmiot.

Przed prawdziwym wyzwaniem stoją podmioty wykonujące działalność leczniczą. Muszą podjąć decyzję, czy wierzyć prawu i argumentom tu przedstawionym, czy wierzyć stanowisku NIK prezentowanemu w wystąpieniach pokontrolnych. Mam nadzieję, że NIK, zrozumie, że błędzi i przestanie wprowadzać podmioty kontrolowane w błąd, nim to jednak nastąpi, wiele czasu minąć może. Decyzje trzeba podejmować już. Codziennie.

Uczciwość zawodowa i jakakolwiek nie pozwala zalecić zawierania umów powierzenia przetwarzania tam gdzie jest to błędem i gdzie naraża to odbiorców – administratorów danych, na odpowiedzialność administracyjną i cywilną.

Jednocześnie rozumiem, że wiele podmiotów ugnie się przed autorytetem organu i zawrze umowy powierzenia przetwarzania tam, gdzie czynić tego nie należy. Takim podmiotom doradzam by zarchiwizowały sobie na papierze wystąpienia NIK, będące efektem kontroli w tych i innych podmiotach. By zachowali sobie te materiały i pier-

wotni administratorzy – zlecniodawcy i odbiorcy – kolejni administratorzy – zleceniobiorcy. Można liczyć, że w sytuacji odpowiedzialności administracyjnej, zwłaszcza w trybie odwoławczym, materiały te pomogą tym podmiotom w obronie swego stanowiska, że co prawda łamały prawo, nie realizowały (to odbiorcy) art. 13 RODO, jednak czyniły to w zaufaniu do NIK. Może PUODO nie będzie ścigał takiego naruszenia, może sąd uzna, że karanie za zaufanie do organu państwa byłoby niewłaściwe. Nie wiemy. Okaże się, jednak dobrze jest mieć papierowe argumenty, które, czy to pracownikom PUODO, czy to sądowi, przedstawić można.

Uważam, że z ostrożności podmiot, któremu zlecono wykonanie usługi, na przykład badania tomograficznego, powinien informować osoby, których dane dotyczą, że ich dane przetwarza. Informować w zakresie wynikającym z art. 13 RODO. Poinformować, dodając przy tym, że zawarło się umowę powierzenia przetwarzania ze szpitalem takim to a takim, że na podstawie tej umowy jest się podmiotem przetwarzającym i że na podstawie przepisów prawa jest się administratorem danych osobowych.

Nie są to rozwiązania doskonałe. Są to rozwiązania ostrożne. Na rozwiązania doskonałe będzie czas kiedy ktoś w NIK zrozumie, że błędzi i przeszkoli kontrolerów.

Reasumując, bezpodstawne są obawy tych to odbiorców danych będących faktycznie administratorami, a których to NIK zwykł traktować, jako podmioty przetwarzające, dotyczące zwiększenia ich zadań związanych z realizacją obowiązków informacyjnych, jakie będą mieć, jeśli przyjąć, iż są administratorami a nie podmiotami przetwarzającymi.

Powinność realizacji obowiązku informacyjnego, o jakim mowa w art. 13 i 14 RODO, nie dotyczy podmiotów przetwarzających. To administrator zobowiązany jest realizować obowiązek informacyjny, wynikający z art. 13 i 14 RODO.

Można zatem założyć, iż podmiot realizujący badania diagnostyczne na podstawie skierowania zawierającego konkretne dane osobowe pacjenta, jest administratorem, co skutkować powinno koniecznością realizacji obowiązku informacyjnego, o jakim mowa w art. 13 i 14 RODO, w zależności od trybu skierowania. Dodatkowo w praktyce założyć należy, iż jeden podmiot diagnostyczny, pozyska w ten sposób

dane jednego pacjenta, ale z kilku źródeł danych, z kilku podmiotów kierujących. Powyższe skutkować powinno realizacją obowiązku informacyjnego, o jakim mowa w art. 14 RODO, z każdorazowym wskazaniem źródła danych, jak wymaga tego przepis art. 14 ust. 2 lit. f. RODO. Czyli, teoretycznie przyjęcie, koncepcji, iż podmiot diagnostyczny, jest odbiorcą, będącym odrębnym administratorem – nie tak, jak wskazuje NIK, że jest podmiotem przetwarzającym – skutkować powinno intensyfikacją zadań związanych z realizacją obowiązku informacyjnego.

Na szczęście jednak tak nie jest, albowiem w tym przypadku działa wyłączenie, o jakim mowa w art. 14 ust. 5 lit c. RODO. Proces pozyskiwania lub ujawniania danych przez odbiorcę będącego odrębnym administratorem (podmiot diagnostyczny) został bowiem wyraźnie uregulowany przepisami prawa, któremu podlega, a dane chronione są przepisami o tajemnicy zawodowej, oraz restrykcyjnymi przepisami dotyczącymi udostępniania dokumentacji medycznej oraz informacji o stanie zdrowia pacjenta, czy udzielonych mu świadczeniach medycznych, jako środkami gwarantującymi ochronę prawnie uzasadnianego interesu podmiotu danych.

Reasumując zatem, odbiorca, będący odrębnym administratorem, jeśli pozyskuje dane realizując prawem określony tryb postępowania, któremu podlega, a dane te chronione są przez środki gwarantujące ochronę prawnie uzasadnionego interesu podmiotu danych, zwolniony jest z powinności realizacji obowiązku informacyjnego, o jakim mowa w art. 14 RODO. Powyższe nie dotyczy obowiązku, o jakim mowa w art. 13 RODO, ale w tym to przypadku, nie ma zagrożenia wynikającego z konieczności identyfikacji i wskazywania źródeł pochodzenia danych, albowiem dane pochodzą od samego podmiotu danych.

Zgoda osoby, której dane dotyczą

Zgoda jest jedną z przesłanek dopuszczalności przetwarzania danych osobowych, czy jak dziś powinno się to poprawnie określi, jednym z warunków zgodności z prawem przetwarzania danych osobowych. Jedną z wielu możliwych przesłanek. Dotyczy to zarówno danych osobowych zwykłych (czyli tych, o których nie ma mowy w art. 9 ust. 1 RODO), jak i danych osobowych szczególnych kategorii. Jeśli chodzi o zgodę na przetwarzanie danych osobowych zwykłych, to zapisana jest ona w art. 6 ust 1 lit. a RODO. Jeśli chodzi o zgodę na przetwarzanie danych osobowych wrażliwych (obecnie: szczególnych kategorii danych osobowych) to zapisana jest ona w art. 9 ust 2 lit. a RODO.

Podkreślenia wymaga, że chociaż zgoda jest jedną z wielu możliwych przesłanek dopuszczalności przetwarzania danych osobowych, to jeżeli zachodzi któraś z przesłanek dopuszczalności przetwarzania danych osobowych inna niż zgoda, to jednocześnie odbieranie zgody jest błędem. Należy wyobrazić sobie następujące zdarzenia:

- odbieramy zgodę
- przetwarzamy dane
- pacjent wycofuje zgodę
- przetwarzamy dane i wyjaśniamy pacjentowi, że odebraliśmy ją błędnie
- pacjent kieruje skargę do PUODO.

Zgoda nie stanowi podstawowej przesłanki dopuszczalności przetwarzania. W PWDL zgoda nie jest podstawą przetwarzania większości danych. Odebranie zgody na przetwarzanie danych pacjenta w dokumentacji medycznej jest błędem. Błąd ten może skutkować skargą do PUODO.

Podobnie, jeżeli na przykład administrator (danych) zamierza przetwarzać dane osobowe w celu wystawienia faktury, to zgoda na przetwarzanie danych osobowych w celu wystawienia faktury jest mu absolutnie niepotrzebna, ponieważ przetwarza on dane osobowe na podstawie art. 6 ust 1 lit. c RODO. Administrator (danych osobowych) nie powinien w takiej sytuacji odbierać zgody na przetwa-

rzanie danych osobowych w celu wystawienia faktury. Po pierwsze zgoda nie jest mu na nic potrzebna, bowiem dopuszczalność przetwarzania danych osobowych w celu wystawienia faktury wynika z 6 ust 1 lit. c RODO. Po drugie, jeżeli administrator danych osobowych poprosi osobę, której dane dotyczą, o wyrażenie zgody na przetwarzanie danych osobowych w celu wystawienia faktury i osoba ta nie wyrazi oczekiwanej zgody, to administrator danych osobowych jest w sytuacji ze wszech miar niekomfortowej, ma bowiem obowiązek wystawienia faktury, przetworzenia danych osobowych w celu wystawienia faktury, przechowywania faktury z danymi osobowymi do celów sprawozdawczości i jednocześnie osoba, której dane dotyczą, zakazuje mu przetwarzania dotyczących jej danych osobowych. Jeżeli osoba, której dane dotyczą, nie poda danych koniecznych do wystawienia faktury, to problemu nie ma, po prostu faktura nie zostanie wystawiona. Jeżeli osoba, której dane dotyczą zażąda wydania faktury, poda administratorowi danych dane potrzebne do wystawienia faktury i nie wyrazi zgody na przetwarzanie tych danych osobowych w celu wystawienia faktury, to uważam, że administrator ma obowiązek wystawić fakturę, przetwarzać dane, a zakaz przetwarzania danych osobowych w celu wystawienia faktury, sformułowany przez osobę, której dane dotyczą, w tym wypadku jest nieskuteczny, sytuacja jednak jest, jak napisałem wyżej, niekomfortowa, należy więc jej unikać. Jeżeli w tym samym stanie faktycznym administrator (danych osobowych) pragnie uzyskać od osoby której dane dotyczą, zgodę na przetwarzanie danych osobowych w celu innym niż wystawienie faktury, to nie wolno mu od wyrażenia tej zgody uzależniać realizacji umowy, co wynika z art. 7 ust. 4 RODO.

Treść dokumentu

Zgoda osoby, której dane dotyczą zdefiniowana jest w art. 4 pkt 11 RODO, jako dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych. Zgoda nie musi być zatem wyrażona słowami, zgoda nie musi być złożona na piśmie by

była ważna.⁴⁷ Z motywu 32 Preambuły RODO wynika, że zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności osoby, której dane dotyczą, która wyznacza jednoznaczne przyzwolenie na przetwarzanie dotyczących jej danych osobowych. .

Zgoda na przetwarzanie danych osobowych w realiach PWDL

Przykładowe formularze mogące posłużyć administratorowi do tego, aby odebrać i udokumentować złożenie oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych, prezentujemy na kolejnych stronach. Formularzami tymi posługujemy się tylko wtedy, kiedy przetwarzanie danych wymaga uzyskania zgody, czyli np. w związku z prowadzeniem działań marketingowych.

⁴⁷ Należy zwrócić uwagę, że zgoda, o której mowa w RODO, to, w istocie złożenie oświadczenia woli w przedmiocie zgody na przetwarzanie danych” osobowych. R. Szałowski. Ochrona danych osobowych. Komentarz do ustawy z dnia 29 sierpnia 1997 r. Zielona Góra. 2000. s. 76.

....., dn. OŚWIADCZENIE w sprawie wyrażenia zgody na przetwarzanie danych osobowych Ja niżej podpisana/podpisany oświadczam, że wyrażam zgodę na przetwarzanie moich danych osobowych podanych w niniejszym formularzu przez [dalej Jednostka / ADO] oraz, iż podane dane zgodne są ze stanem faktycznym, zobowiązując się jednocześnie do ich aktualizacji w przypadku wystąpienia ich zmiany, na niżej wymienionych zasadach:	
Określenie celu:	Przetwarzanie w celu marketingowym związanym z udzielanymi przez Jednostkę świadczeniami zdrowotnymi lub przez podmioty z nią kooperujące i przekazywanie informacji handlowych za pośrednictwem połączeń telefonicznych
Rodzaj danych:	Imię (imiona) i nazwisko Numer telefonu: Adres korespondencyjny:
TAK wyrażam zgodę	
Określenie celu:	Przetwarzanie w celu marketingowym związanym z udzielanymi przez Jednostkę świadczeniami zdrowotnymi lub przez podmioty z nią kooperujące i przekazywanie informacji handlowych za pośrednictwem środków komunikacji elektronicznej
Rodzaj danych:	Imię (imiona) i nazwisko: Adres e-mail:
TAK wyrażam zgodę	
Określenie celu:	
Rodzaj danych:	Imię (imiona) i nazwisko.....
TAK wyrażam zgodę	

Jednocześnie oświadczam, iż Administrator Danych Osobowych, zrealizował względem mnie obowiązek informacyjny o jakim mowa w art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1)

.....
 / Data / / Podpis składającego oświadczenie /

....., dn.

OŚWIADCZENIE

w sprawie wyrażenia zgody na przetwarzanie danych osobowych dziecka

Ja niżej podpisana/podpisany oświadczam, że jestem rodzicem
/ opiekunem prawnym dziecka / *imię i nazwisko dziecka* / /
PESEL i wyrażam zgodę na przetwarzanie danych osobowych moich
oraz dziecka przez [dalej Jednostka / ADO] oraz, iż podane dane zgodne są
ze stanem faktycznym, zobowiązując się jednocześnie do ich aktualizacji w przypadku wystąpienia zmiany, na
niżej wymienionych zasadach:

Określenie celu:	Przetwarzanie w celu marketingowym związanym z udzielanymi przez Jednostkę świadczeniami zdrowotnymi lub przez podmioty z nią kooperujące i przekazywanie informacji handlowych za pośrednictwem połączeń telefonicznych
Rodzaj danych:	Imię (imiona) i nazwisko Numer telefonu: korespondencyjny:
TAK wyrażam zgodę	
Określenie celu:	Przetwarzanie w celu marketingowym związanym z udzielanymi przez Jednostkę świadczeniami zdrowotnymi lub przez podmioty z nią kooperujące i przekazywanie informacji handlowych za pośrednictwem środków komunikacji elektronicznej
Rodzaj danych:	Imię (imiona) i nazwisko:-mail:
TAK wyrażam zgodę	
Określenie celu:	
Rodzaj danych:	Imię (imiona) i nazwisko
TAK wyrażam zgodę	

* niepotrzebne skreślić

Jednocześnie oświadczam, iż Administrator Danych Osobowych, zrealizował względem mnie obowiązek informacyjny o jakim mowa w art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1)

.....
/ Data / / Podpis składającego oświadczenie /

Jednoczesne stosowanie art. 9 RODO i art. 6 RODO

Zagadnieniem, które budzi, obserwowane przez nas, wśród praktyków niepotrzebne dyskusje jest podstawa prawna przetwarzania danych medycznych. Należy mieć świadomość, że jeśli chodzi o dane osobowe szczególnych kategorii, to art. 9 ust. 2 RODO nie stanowi wystarczającej podstawy na gruncie RODO. Wystarczającej nawet na gruncie RODO, należy bowiem pamiętać, że jeżeli przetwarzanie danych osobowych ma być zgodne z prawem, to oprócz realizowania odpowiednich warunków zapisanych w RODO, przetwarzanie to musi również realizować warunki spoza RODO – zwykle polega to na realizacji odpowiednich przepisów szeroko pojętego prawa medycznego. RODO nie stanowi autonomicznej podstawy do przetwarzania danych osobowych. Proponowane przez nas wzory dokumentów uwzględniają to zjawisko.

Nie jest to niestety jedyny problem, na jaki można napotkać przy ustalaniu podstawy prawnej przetwarzania danych szczególnych kategorii, w tym danych medycznych, danych medycznych osobowych, czy osobowych danych medycznych – jakkolwiek je nazwiemy. Otóż należy pamiętać, że jeśli chodzi o samą tylko podstawę prawną na gruncie RODO, to odpowiedni ustęp artykułu 9 ust. 2 RODO nie stanowi takowej podstawy. Podstawa prawna na gruncie RODO zawsze znajduje się w art. 6 ust. 1 RODO. Artykuł 9 RODO nie stanowi na gruncie RODO podstawy prawnej do przetwarzania danych osobowych. Z art. 9 ust. 1 RODO wynika zakaz przetwarzania danych osobowych szczególnych kategorii, zaś z art. 9 ust. 2 RODO wynika kiedy jednak, w jakich sytuacjach, przetwarzanie danych osobowych wskazanych w art. 9 ust. 1 RODO, jest dopuszczalne. Uzasadnienie dla przedstawionego tu poglądu prezentujemy niżej, tu wskazujemy schemat podstawy prawnej, która legalizuje przetwarzanie osobowych danych medycznych w dokumentacji medycznej. Schemat ten wygląda jak wskazujemy poniżej.

Art. 6 ust. 1 lit c RODO w zw. z art. 9 ust. 2 lit. h RODO w zw. z art. 24 UoPPiRPP.

Wskazany tu przykład stanowi pewną podstawę. Można go uzupełnić o wskazane dokładniej ustępy art. 24 UoPPiRPP, można go uzupełnić o odpowiednie ustępy art. 30 UoPPiRPP, w którym zapisana jest podstawa prawna do wydania rozporządzeń regulujących

prowadzenie dokumentacji. Można go wreszcie uzupełnić o wskazanie odpowiedniego rozporządzenia. Każde z tych rozwiązań jest dobre, tyle tylko, że mają one różny stopień szczegółowości. Nie wolno zrobić jednego, nie wolno wskazać jedynie odpowiedniego fragmentu art. 9 RODO, nawet łącznie ze wskazanymi tu uzupełnieniami. Podkreślenia wymaga, że o ile art. 6 RODO, stanowi podstawę do przetwarzania danych osobowych, o tyle art. 9 RODO podstawy takiej nie stanowi. Analizę konieczności jednoczesnego stosowania art. 6 i art. 9 RODO w sytuacji przetwarzania danych szczególnych kategorii zawarłem w odpowiednim miejscu mojej książki poświęconej głównie art. 5 RODO i art. 6 RODO, a wcześniej jeszcze zasygnalizowałem zjawisko w książce poświęconej dokumentacji ochrony danych osobowych. Rozważania temu poświęcone, z uwagi na ich świeżość, nie zdążyły się zdezaktualizować, (zwłaszcza) do pierwszej ze wskazanych książek odsyłam, poniżej zaś, dla porządku zamieszczam wybór podstawowych tez z tych rozważań.

Dla porządku przypomnijmy treść artykułu 6 RODO. Nosi on tytuł „Zgodność przetwarzania z prawem”. Część wprowadzająca przepisu stanowi: „Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków”. Już ze wskazanego fragmentu przepisu widać, że dotyczy on wszystkich danych osobowych, w tym danych osobowych szczególnych kategorii.

Z kolei artykuł 9 RODO nosi tytuł „Przetwarzanie szczególnych kategorii danych osobowych”. Przepis ten stanowi: „Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby”. I dalej, część wprowadzająca art. 2 RODO stanowi: „Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:”. Ze wskazanych tu fragmentów art. 9 RODO widać, że przepis ten ustanawia zakaz przetwarzania danych osobowych i wskazuje, kiedy zakaz ten nie znajduje zastosowania, jednak jednocześnie wynika z nich, że art. 9 RODO nie dotyczy zgodności przetwarzania danych osobowych z

prawem. Nie dotyczy przetwarzania z prawem, bowiem dotyczy czego innego – wskazanego wyżej zakazu i zwolnienia zeń.

Należy zwrócić uwagę na kilka wniosków, które wynikają z cytowanych (fragmentów) przepisów.

- Z art. 6 RODO wynika kiedy zgodne z prawem jest przetwarzanie danych osobowych, zarówno danych osobowych zwykłych jak i wrażliwych danych osobowych czyli danych osobowych szczególnych kategorii. Danymi zwykłymi nazywam tu dane osobowe, które nie są danymi osobowymi szczególnych kategorii.
- Dane osobowe szczególnych kategorii, stanowią podzbiór zbioru danych osobowych, również zwykłe dane osobowe stanowią podzbiór zbioru danych osobowych. Skoro przepis (art. 6 RODO) stanowi o zgodności z prawem przetwarzania danych osobowych i nie wskazuje żadnej konkretnej kategorii danych osobowych, to oznacza to, że przepis stanowi o zgodności z prawem przetwarzania wszystkich danych osobowych, zarówno zwykłych danych osobowych jak i danych osobowych szczególnych kategorii).
- Żeby zgodnie z prawem przetwarzać dane osobowe zwykłe należy spełnić co najmniej jeden warunek zgodności przetwarzania danych osobowych z prawem z art. 6 ust. 1 RODO.
- Żeby zgodnie z prawem przetwarzać dane osobowe szczególnych kategorii należy spełnić dwa warunki. Łącznie.
- **Pierwszy** z tych warunków to spełnienie co najmniej jednego zgodności przetwarzania danych osobowych z prawem z art. 6 ust. 1 RODO, jednak jeśli chodzi o dane szczególnych kategorii jest to niewystarczające.
- **Drugi** z tych warunków to spełnienie co najmniej jednej przesłanki z art. 9 ust. 2 RODO.

Przedstawiona powyżej argumentacja mnie przekonuje. Uważam, że wnioski wynikające z analizy treści art. 6 i art. 9 RODO są w przedmiotowej sprawie wystarczające. Z uwagi na częściowo poradnikowy charakter publikacji, zamieszczam poniżej tak zwane argumenty z autorytetu, innymi słowy wskazuję kto z identyfikowalnych powszechnie osób i podmiotów ma pogląd taki sam jak ja.

Kto jeszcze podziela pogląd o jednoczesnym stosowaniu art. 6 RODO i art. 9 RODO do przetwarzania danych osobowych szczególnych kategorii.

- **ICO, czyli brytyjski organ ochrony danych osobowych** (wspomniany też niżej). Na stronie ICO czytamy: „If you are processing special category data, you need to identify both a lawful basis for processing and a special category condition for processing in compliance with Article 9. You should document both your lawful basis for processing and your special category condition so that you can demonstrate compliance and accountability”.⁴⁸ Co tłumaczymy na: „Jeżeli przetwarzasz dane szczególnej kategorii to masz potrzebę zidentyfikowania zarówno prawnych podstaw przetwarzania i warunku przetwarzania danych szczególnej kategorii zgodnego z artykułem 9. Powinieneś udokumentować zarówno prawne podstawy przetwarzania jak i swój warunek przetwarzania danych osobowych szczególnej kategorii tak byś mógł wykazać zgodność i rozliczalność”.

Czytamy tam również: „In order to lawfully process special category data, you must identify both a lawful basis under Article 6 of the UK GDPR and a separate condition for processing under Article 9. These do not have to be linked.”⁴⁹. Tłumaczymy to na: Aby zgodnie z prawem przetwarzać szczególne kategorie danych musisz zidentyfikować zarówno prawne podstawy zgodne z artykułem 6 RODO jak i osobny warunek przetwarzania zgodnie z artykułem 9. One nie muszą być połączone.

- **Grupa ekspertów Komisji Europejskiej**. W dokumencie sporządzonym przez tę grupę czytamy: „The Commission recalled the approach to processing of special categories of data for which there is a prohibition principle coupled with an exhaustive lists of situations in

⁴⁸ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/> (Dostęp 2022.02.27. godz. 15:56) (Tłum: J. Rz. Niezgrabność tłumaczenia, z punktu widzenia języka polskiego, jest świadoma, tłumacz postawił na wierność, nie na urodę tłumaczenia.)

⁴⁹ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/> (Dostęp 2022.02.27. godz. 15:56) (Tłum: J. Rz. Niezgrabność tłumaczenia, z punktu widzenia języka polskiego, jest świadoma, tłumacz postawił na wierność, nie na urodę tłumaczenia.)

which processing is allowed (always supported by a legal basis in Article 6”).⁵⁰ Tłumaczymy to na: „Komisja przypomniała o podejściu do szczególnych kategorii danych w odniesieniu do których obowiązuje zasada zakazu, połączona z wyczerpującą listą sytuacji, w których przetwarzanie jest dozwolone (zawsze poparte przez podstawę prawną w art. 6)”.

- **Iga Małobęcka-Szwast i K. Syska** opublikowały⁵¹ w 2019 roku artykuł poświęcony stosowaniu art. 6 i art. 9 RODO. Brak jest w nim wyraźnego stanowiska własnego autorek, jednak z uwagi na pozwolne przeciskanie się prezentowanego tu poglądu do polskiej doktryny, artykuł ten stanowi głos doniosły. Autorki zrelacjonowały w nim stanowiska podmiotów uważających, że art. 6 należy stosować również wobec danych osobowych szczególnych kategorii. Podmioty o których piszą wskazane autorki wymieniam poniżej, oznaczając je dwoma myślnikami.
- **Grupa Robocza art. 29** (sic!),
- **Brytyjski Komisarz ds. Informacji (ICO),**
- **Irlandzka Komisja ds. Ochrony Danych Osobowych,**
- **Niemiecka Datenschutzkonferenz i niemiecka doktryna,**
- **EROD.**

Artykuł **I. Małobęckiej-Szwast i K. Syski** jest prawdopodobnie drugim w polskiej doktrynie wystąpieniem poglądu o konieczności stosowania art. 6 RODO do przetwarzania danych osobowych szczególnych kategorii. Pierwszym prawdopodobnie wystąpieniem poglądu o konieczności stosowania art. 6 RODO do przetwarzania danych osobowych szczególnych kategorii jest uwaga w książce napisanej przez J. Rzymowskiego, czyli przez jednego z autorów niniejszej publikacji, i wydanej latem roku 2019. Piszę tam między innymi: „Zwracam tu uwagę na jeszcze jeden niuans. Otóż odpo-

⁵⁰ *Minutes of the second meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680* 10 October 2016. Dokument ten wskazany jest, jako źródło w: L. Georgieva, Ch. Kuner w: *The EU General Data Protection Regulation (GDPR). A Commentary*. Edited by Ch. Kuner, L. A. Bygrave, Ch. Docksey, and Assistant Editor L. Drechsler. Oxford 2020. s. 384.

⁵¹ Wyczerpiecie stanowisk zaczerpnięte z artykułu: *Podwójne podstawy przetwarzania danych wrażliwych*. I. Małobęcka-Szwast, K. Syska. *ABI Expert* 4 (13) / 2019. s. 56-59.

wiednie ustępy art. 9 RODO, wraz z uzupełnieniami, o których wyżej piszę, nie stanowią, na gruncie RODO, wystarczającej podstawy prawnej przetwarzania. Jeżeli administrator przetwarza dane osobowe należące do kategorii wymienionych w art. 9 ust. 1 RODO, to podstawa prawna powinna być co najmniej trzelementowa. Pierwszy element to odpowiednia przesłanka z art. 6 RODO. Drugi element to odpowiednia przesłanka z art. 9 RODO. Trzeci element to uzupełnienie przesłanki z art. 9 RODO”.⁵²

- **Maciej Gawroński** również podziela analizowany tu pogląd dotyczący art. 6 i art. 9 RODO. Zarówno w napisanej wcześniej książce, jak i tu powołuję nietypowe nieco źródło, a mianowicie wymianę zdań z M. Gawrońskim. Wymiana ta zaowocowała przygotowaniem na moją prośbę przez M. Gawrońskiego, wypowiedzi, której fragment tu przytaczam. Mecenase Macieju Gawroński twierdzi, że: „art. 9 jest wadliwie skonstruowany, częściowo nakładając się z art. 6, jednak próby stosowania art. 9 w praktyce wykazały, że trzeba go stosować w zbiegu a nie zamiast art. 6”.⁵³ Uzasadnienie wypowiedzi znajduje się, dzięki uprzejmości M. Gawrońskiego w mojej książce poświęconej art. 5 i art. 6 RODO.
- **Ludmila Georgieva i Christopher Kuner** piszą w oxfordzkim komentarzu do RODO, że: „The processing of sensitive data always requires compliance with other provisions of the GDPR, in addition to those of Article 9.^(...) This raises the question of whether Article 9 constitutes a separate legal basis for data processing, or if it only complements Article 6 GDPR and therefore has to be supported by a legal basis in Article 6 as well^(...) The Commission has stated that the processing of sensitive data must always be supported by a legal basis under Article 6 GDPR^(...) in addition to compliance

⁵² J. Rzymowski. *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*. Kraków 2019. s. 130. Przypis, który tam zamieściłem to: *Pogląd taki wyraża brytyjski organ ochrony danych*. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/> (Dostęp 2022.02.27. godz. 15:58). *Wniosek taki wynika, jak się wydaje z motywu 51 Preambuly RODO*.

⁵³ Ponieważ wypowiedź pochodzi z wymiany zdań, która miała charakter korespondencji, to publikuję ją tu po uprzednim uzyskaniu zgody jej Autora, któremu z tego miejsca dziękuję.

with one of the situations covered in Article 9(2)”.⁵⁴ Tłumaczymy to na język polski na: „Przetwarzanie danych wrażliwych zawsze wymaga przestrzegania innych przepisów RODO, dodatkowo do tych z artykułu 9. W związku z tym pojawia się pytanie, czy art. 9 konstytuuje odrębną podstawę prawną przetwarzania danych, czy tylko uzupełnia art. 6 RODO, dlatego też musi być również wsparty podstawą prawną (mającą źródło – dodatek J. Rz.) w art. 6. Komisja stwierdziła, że przetwarzanie danych wrażliwych musi zawsze być wsparte podstawą prawną wynikającą z art. 6 RODO w dodatku do zgodności z jedną z okoliczności ujętych w art. 9.2”. Jak widać stanowisko L. Georgievej i Ch. Kunera jest ostrożne, choć dobór cytatów nie pozostawia wątpliwości co do przedmiotowej kwestii, czyli jednoczesnego stosowania art. 6 i art. 9 RODO, przyznam jednak, że jednoznacznego stanowiska autorów brakuje.

- **Paweł Barta, M. Kawecki i P. Litwiński** prezentują⁵⁵ w przedmiotowej kwestii ostrożny pogląd własny o charakterze, jak uważam, pośrednim. Omawiam go szerzej we wspomnianej wyżej książce o art. 5 i 6 RODO, do której, lub do dzieła źródłowego odsyłam. Istotą poglądu wskazanych autorów jest to, że uważają oni, iż przetwarzanie danych szczególnych kategorii jest zawsze związane z przetwarzaniem danych osobowych zwykłych i że właśnie ta dwoistość prowadzi do drugiej dwoistości, a to do konieczności stosowania art. 6 RODO, wtedy, kiedy stosuje się art. 9 RODO. Czyli zdaniem wskazanych autorów konieczność stosowania art. 6 RODO wtedy kiedy się stosuje art. 9 RODO nie wynika z faktu konieczności stosowania art. 6 kiedy się stosuje 9 RODO, ale z faktu, że kiedy się przetwarza dane szczególnych kategorii, to przetwarza się też dane pozostałych kategorii (zwykle) i w takim razie dane osobowe szczególnych kategorii przetwarza się w oparciu o art. 9 RODO, dane osobowe pozostałych kategorii przetwarza się w oparciu o art. 6 RODO a jednoczesne stosowanie art. 6 RODO i art. 9 RODO ma charakter technicznego zbiegu.

⁵⁴ L. Georgieva, Ch. Kuner. w: *The EU General Data Protection Regulation (GDPR). A Commentary*. Edited by Ch. Kuner, L. A. Bygrave, Ch. Docksey, and Assistant Editor L. Drechsler. Oxford 2020. s. 376.

⁵⁵ P. Barta, M. Kawecki, P. Litwiński. w: P. Barta, D. Dörre-Kolasa, M. Kawecki, A. Krzyżak, P. Litwiński [red.]. *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*. Warszawa 2021. s. 207.

- **Leszek Kępa** prawdopodobnie jako absolutnie pierwszy w Polsce wyraził pogląd⁵⁶ o podwójnej podstawie przetwarzania, z tym, że jeszcze przed pojawieniem się RODO, bo na gruncie UODO97.

⁵⁶ L. Kępa. *Ochrona danych osobowych w praktyce*. Warszawa 2014. s. 21.

Odpowiedzialność na gruncie RODO

Odpowiedzialność na gruncie RODO

Odpowiedzialność administracyjna

„W art. 5 RODO ustanowiono zasady dotyczące przetwarzania danych osobowych. Jednocześnie w art. 83 ust 5 pkt a ustanowiono karę, którą może ponieść administrator danych, jeżeli narusza przepisy dotyczące przetwarzania danych osobowych. Jest to kara administracyjna, sięgająca 20 milionów euro a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Jedna z zasad ustanowionych w art. 5 RODO to zasada rozliczalności. Zasada ta ustanowiona została w art. 5 ust 2 RODO, który brzmi: „Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).”. Wspomniany w cytowanym przepisie „ustęp 1” to ustęp 1 artykułu 5 RODO, w którym właśnie ustanowiono zasady. Administrator danych ma zatem obowiązek wykazać przestrzeganie zasad przetwarzania danych osobowych. Wykazać zaistnienie faktów w przeszłości można na różny sposób, można o tych faktach opowiedzieć, nagrać film, nagrać dźwięk, ale można też sporządzić pismo, pismo wręczyć odpowiedniej osobie, uzyskać od tej osoby pokwitowanie. Metody wykorzystujące pisma są stare, ale niezawodne.”⁵⁷

Poza niezawodnością, metody takie mają jeszcze jedną zaletę. Pismo jest idealnym wręcz, z punktu widzenia dowodowego dokumentem, zdatnym do przedstawienia w sądzie administracyjnym. Należy pogodzić się z perspektywą kontroli i nałożenia kary wskutek takiej kontroli. Założenie zgodnie z którym administrator może zabezpieczyć się tak dobrze, że nie zostanie ukarany, jest mrzonką. Mrzonką niebezpieczną. W związku z tym administrator danych powinien przygotować się do postępowania przed sądem administracyjnym, czyli odpowiednio wcześniej przygotować stosowną dokumentację.

⁵⁷ J. Rzymowski. *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*. Kraków 2019. s. 9.

„Postępowanie dotyczące nałożenia kary administracyjnej oparte jest o KPA. Artykuł 7a KPA⁵⁸ stanowi, w zakresie istotnym dla wyводу:

„§ 1. Jeżeli przedmiotem postępowania administracyjnego jest nałożenie na stronę obowiązku bądź ograniczenie lub odebranie stornie uprawnienia, a w sprawie pozostają wątpliwości co do treści normy prawnej, wątpliwości te są rozstrzygane na korzyść strony, chyba że sprzeciwiają się temu sporne interesy stron albo interesy osób trzecich, na które wynik postępowania ma bezpośredni wpływ.

§ 2. Przepisu § 1 nie stosuje się:

1) jeżeli wymaga tego ważny interes publiczny, w tym istotne interesy państwa, a w szczególności jego bezpieczeństwa, obronności lub porządku publicznego; (...)”.

Lektura przepisu wskazuje, że

W świetle tego przepisu widać, jak ważne jest posiadanie odpowiednich dokumentów, ponieważ jeśli nawet nie zagwarantują one czasem realizacji tej czy innej zasady przetwarzania danych, to na pewno będą pomocne w obronie przed karą za złamanie odpowiedniej zasady. Posiadanie przez ADO dokumentacji ochrony danych osobowych może okazać się jedyną, skuteczną obroną przed odpowiedzialnością administracyjną.”⁵⁹.

Odpowiedzialność administracyjną administrator może ponieść za naruszenie prawie każdego przepisu RODO. Również za brak dowodów realizacji przepisów. By zabezpieczyć się przed odpowiedzialnością administracyjną należy realizować przepisy i zbierać dowody na to, że się je zrealizowało.

Kto może ponieść odpowiedzialność administracyjną

Z artykułu 5 ust. 2 RODO wynika, że odpowiedzialność za naruszenie przepisów RODO ponosi administrator. Administrator zdefiniowany jest w artykule 4 pkt 7 RODO.

⁵⁸ Ustawa z dnia 14 czerwca 1960 r. *Kodeks postępowania administracyjnego*. Dz.U. 1960 nr 30 poz. 168 ze zm. t. j. Dz. U. 2021 poz. 735 ze zm.

⁵⁹ J. Rzymowski. *Op. cit.* Kraków 2019. s. 10.

„Administratorem danych może być osoba fizyczna.
Administratorem danych może być osoba prawna.
Administratorem danych może być organ publiczny.
Administratorem danych może być jednostka.
Administratorem danych może być inny podmiot.
Administratorem może być każdy podmiot lub osoba.

Warunkiem by wymieniony podmiot był administratorem danych osobowych jest, by ten podmiot samodzielnie lub wspólnie z innymi ustalał cele i sposoby przetwarzania danych osobowych. (...) Jeżeli cele i sposoby przetwarzania danych osobowych są określone w prawie UE lub w prawie państwa członkowskiego, to również w prawie UE lub w prawie państwa członkowskiego może zostać wyznaczony administrator danych osobowych, oraz, że w prawie UE lub w prawie państwa członkowskiego mogą zostać określone kryteria wyznaczenia administratora danych osobowych.”⁶⁰.

Jak zatem widać administratorem danych może być każdy kto ustala cele i sposoby przetwarzania danych. Niestety definicja zawarta w RODO jest daleka od doskonałości bowiem trudno jest znaleźć podmiot, który rzeczywiście sam ustala cele i sposoby przetwarzania danych osobowych.

W realiach medycznych sposoby przetwarzania danych osobowych do pewnego stopnia określane są przez podmiot, na przykład podmiot decyduje czy dokumentację będzie przechowywał w tym czy w innym pomieszczeniu lub z użyciem jakich środków (komputerowych czy nie) będzie ją prowadził.

Jeżeli chodzi o cele przetwarzania danych to PWDL same nie ustalają tych celów ponieważ są ustalone są w przepisach prawa. Można oczywiście twierdzić że PWDL konkretyzuje swoje cele i sposoby przetwarzania w związku z czym jest administratorem danych. Jest to oczywiście jedyna droga, natomiast rozwiązanie to nie odpowiada na pytanie o to, kto jest administratorem danych w przychodni. Jak widać z przepisu tak naprawdę nie wynika kto jest administratorem (danych) w przychodni lub szpitalu w sensie konkretnym. Z przepisu nie wynika czy administratorem danych jest przychodnia lub szpital czy gmina będąca właścicielem przychodni lub szpitala, czy spółka będąca

⁶⁰ J. Rzymowski. *RODO – GDPR. Komentarz*. Komentarz do art. 4 pkt. 7. (1. Art. 4 pkt 7. Komentarz).

właścicielem przychodni lub szpitala, czy administratorem jest dyrektor lub kierownik przychodni lub szpitala, czy zarząd lub prezes spółki, czy może wreszcie burmistrz gminy. Skoro z przepisu nie wynika kto jest administratorem (ponieważ wynika to tylko pozornie, czyli w istocie nie wynika) to można zaryzykować stwierdzenie że administratorem (danych) w podmiocie jest ten kto zostaje w dokumentacji przetwarzania danych osobowych tworzonej w tym podmiocie oznaczony jako administrator.

Administratorem w prowadzonej dokumentacji należy zatem wyznaczyć inteligentnie, bowiem to na podmiot który jest oznaczony w dokumentacji jako administrator, w pierwszej kolejności może zostać nałożona kara administracyjna.

Jeżeli zatem w dokumentacji wskażemy że administratorem (danych) w przychodni (szpitalu) jest dyrektor przychodni (szpitala), to istnieje ryzyko, poważne ryzyko, że karę administracyjną zapłaci dyrektor i to zdecydowanie z prywatnych środków.

Jeżeli w dokumentacji wskażemy że administratorem danych w przychodni (szpitalu) jest przychodnia (szpital) to obowiązek zapłaty kary administracyjnej spoczywać będzie na tej przychodni (szpitalu). (PUODO może próbować nasze wskazanie podważyć, jednak wydaje się to mało prawdopodobne.) Takie rozwiązanie może zupełnie uniemożliwić a przynajmniej zasadniczo utrudnić faktyczne nałożenie kary administracyjnej a przynajmniej jej egzekucję. Przychodnia (szpital) która należy do gminy, może po prostu nie posiadać środków umożliwiających zapłacenie kary administracyjnej. Gmina jest właścicielem przychodni (szpitala), nie jest jednak administratorem na którego nałożono karę.

Podobnie sytuacja wygląda jeżeli przychodnia (szpital) jest spółką lub należy do spółki. Jeżeli w dokumentacji wskazane jest, że administratorem danych w przychodni (szpitalu), która jest spółką, jest kierownik tej przychodni (szpitala) lub na przykład prezes zarządu lub zarząd to osoby lub podmioty te będą musiały zapłacić karę administracyjną, również z własnych środków.

Jeżeli w dokumentacji wskazane jest, że administratorem danych w przychodni (szpitalu) która jest spółką jest spółka, to karę administracyjną będzie musiała zapłacić spółka. Spółka czasem karę zapłaci, jeżeli posiad na to stosowne środki, czasem nie zapłaci ponieważ środków nie posiada. Postawienie spółki w stan upadłości

w odpowiednim momencie może uratować zarząd przed odpowiedzialnością. Rozwiązanie to nie sprawdza się tylko w przypadku spółki cywilnej która niewiele różni się od jednoosobowej działalności gospodarczej nie pojawia się tu bowiem osobowość prawna podmiotu, w związku z tym zobowiązani do zapłacenia kary są wspólnicy spółki lub osoba wykonująca jednoosobową działalność gospodarczą.

Uczciwość nie pozwala stwierdzić że oznaczenie administratora danych w dokumentacji jest na pewno dla PUODO wiążące należy jednak pamiętać o kilku kwestiach.

- Jeżeli jako administratora oznaczmy kierownika przychodni lub prezesa zarządu to ogromnie ułatwiamy nałożenie kary.
- Jeżeli jako administratora oznaczmy przychodnię lub spółkę, to ogromnie utrudniamy nałożenie kary administracyjnej, a czasem wręcz to uniemożliwiamy.

„Polityka ochrony jako narzędzie, odwrócenia ciężaru dowodu

Z art. 5 ust. 2 wynika, że ADO ma obowiązek wykazać, że przestrzega kolejnych zasad. Realizacja zasad następuje przez realizację przepisów szczególnych. W związku z tym, jeżeli ADO chce (a chce, bo musi) wykazać, że przestrzega kolejnych zasad, to musi wykazać, że przestrzega przepisów szczególnych, za pomocą których realizuje kolejne zasady. Jeżeli ADO nie jest w stanie wykazać, że przestrzega zasad, to za samą niemożność wykazania przestrzegania może zostać ukarany karą administracyjną. Kontrola z PUODO może po prostu zażądać wykazania realizacji kolejnych przepisów. Kontroler nie musi wykazywać naruszeń, to ADO musi wykazać, że kolejne przepisy realizuje. Jeśli ADO nie jest w stanie wykazać realizacji któregośkolwiek przepisu szczególnego, to w realiach kontroli musi sobie zdawać sprawę z kilku zagrożeń.

Zagraża mu odpowiedzialność administracyjna za brak realizacji przepisu szczególnego, do wykazania realizacji którego wezwał go kontrolujący. Jest tak, ponieważ jeżeli ADO nie może wykazać, że realizuje przepis, to wynika z tego, że go nie realizuje.

Zagraża mu odpowiedzialność administracyjna za brak realizacji którejś z zasad z art. 5 ust. 1 RODO. Jest tak, ponieważ jeżeli ADO nie może wykazać, że realizuje przepis, to wynika z tego, że go nie realizuje, więc tym samym, że nie realizuje którejś z zasad z art. 5 ust. 1 RODO.

Zagraża mu odpowiedzialność administracyjna za brak realizacji zasady wykazania realizacji którejs z zasad z art. 5 ust. 1 RODO, czyli za naruszenia art. 5 ust. 2 RODO w zw. z art. 5 ust. 1 RODO.

Zagrożeń tych można bardzo łatwo uniknąć. Jeżeli ADO, opisze jak realizuje wszystkie zasady z art. 5 ust. 1 RODO, czyli jeżeli ADO opisze za pomocą których i jak realizowanych przepisów⁽¹⁾ szczególnych realizuje które zasady z art. 5 ust. 1 RODO, to tym samym ADO realizuje obowiązek wykazania, że realizuje zasady. Obowiązek ten wynika z art., 5 ust. 2 RODO w zw. z art., 5 ust. 1 RODO. Proponowana tu przeze mnie polityka ochrony stanowi projekt takiego właśnie opisu. Oczywiście jest, że ADO powinien uzupełnić ją, zwłaszcza w zakresie opisu konkretnej realizacji przepisów szczególnych. Kiedy ADO to zrobi, to może po prostu na wezwanie kontrolera przedstawić mu tak przygotowaną politykę i wskazać odpowiedni jej fragment. W ten sposób ADO wykazuje realizację odpowiedniego przepisu szczególnego, realizację odpowiedniej zasady z art., 5 ust. 1 RODO i realizację zasady rozliczalności. Jeżeli ADO to zrobi, to kontroler z PUODO, by ukarać ADO za cokolwiek, musi udowodnić, że ADO obowiązków, czy obowiązku, nie realizuje. W ten prosty sposób odwracamy ciężar dowodu. Jeśli opiszemy detalicznie realizację kolejnych przepisów, to już nie ADO musi wykazać, że je realizuje, ale kontroler musi wykazać, że ADO przepisów nie realizuje. Może to nie być łatwe.”⁶¹.

Odpowiedzialność cywilna

Istota odpowiedzialności cywilnej

Odpowiedzialność cywilna to odpowiedzialność osoby, która wyrządziła szkodę wobec osoby, która szkodę tę poniosła.

Szkoda może mieć charakter majątkowy, kiedy osoba poszkodowana poniosła konkretna, wymierną w pieniądzu stratę.

Szkoda może mieć też charakter niemajątkowy. Szkoda niemajątkowa polega na tym, że osobę poszkodowaną coś boli lub odczuwa ona cierpienie psychiczne, czyli (upraszczając) jest jej przykro. RODO przewiduje obydwa rodzaje szkody.

⁶¹ J. Rzymowski. *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*. Kraków 2019. s. 330-331.

Jeżeli czynność na danych, której skutkiem była szkoda była wykonywana przez więcej niż jednego administratora albo przez więcej niż jeden podmiot przetwarzający albo przez więcej niż jednego administratora i więcej niż przez jeden podmiot przetwarzający, to wskazane podmioty ponoszą odpowiedzialność solidarną za całą szkodę powstałą wskutek naruszenia RODO, co wynika z art. 82 ust. 4 RODO. Odpowiedzialność solidarna polega na tym, że każdy z podmiotów odpowiada do całej wysokości szkody i że poszkodowany może dochodzić tej szkody od podmiotu wybranego przez siebie lub od obydwu podmiotów, do pełnej wysokości tej szkody.

Kto może ponieść odpowiedzialność cywilną w realiach medycznych

Odpowiedzialność cywilną w realiach medycznych może ponieść administrator danych lub podmiot przetwarzający.

Zasadą jest, że odpowiedzialność cywilną ponosi administrator, czyli przychodnia, spółka, szpital.

Administrator ponosi odpowiedzialność cywilną za szkody które zostały spowodowane przetwarzaniem danych osobowych naruszającym RODO.

Odpowiedzialność może ponieść też podmiot przetwarzający, jednak pod pewnymi warunkami.

Podmiot przetwarzający odpowiada za szkody, które zostały spowodowane przetwarzaniem danych osobowych wyłącznie w sytuacji w której podmiot przetwarzający nie dopełnił obowiązków które RODO nakłada na podmioty przetwarzające.

Podmiot przetwarzający odpowiada również za szkody które zaistniały kiedy podmiot przetwarzający działał poza instrukcjami administratora danych lub wbrew tym instrukcjom i jednocześnie instrukcje te były zgodne z prawem.

Jak administrator lub podmiot przetwarzający mogą zwolnić się z odpowiedzialności cywilnej

Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z art. 82 RODO, jeżeli udowodnią, że w nie ponoszą winy za zdarzenie, które doprowadziło do powstania

szkody. Zwolnienie się z odpowiedzialności cywilnej w warunkach opisanych w art. 82 ust. 3 RODO może być niezwykle trudne. Trudne ponieważ rozpatrujemy sytuacje, w której zaszło zdarzenie, zaszło naruszenie RODO, zaszła szkoda i mimo tych zdarzeń administrator lub podmiot przetwarzający musi udowodnić, że nie poniósł winy za jej zaistnienie. Należy zwrócić uwagę na dwa elementy, nie wystarczy, że administrator lub podmiot przetwarzający nie ponieśli winy za zdarzenie, by zwolnić się z odpowiedzialności muszą oni udowodnić to, że winy nie ponoszą.

Wydaje się, że jedynym narzędziem udowodnienia, przez administratora lub przez podmiot przetwarzający, że nie ponoszą oni winy za zdarzenie, które oznaczało naruszenie RODO i skutkowało szkodą jest dokumentacja, sporządzona przed zdarzeniem i opisująca dokładnie procedury mające takim ewentualnym zdarzeniom zapobiec.

Przykładowe naruszenia, mogące skutkować odpowiedzialnością cywilną

Pacjent pierwszorazowy przychodzi do rejestracji i zapisuje się na wizytę do konkretnego lekarza. Pracownik rejestracji zapisuje podstawowe dane pacjenta (zbieranie danych osobowych, art. 13 RODO). Pacjent dostaje karteczkę z zapisaną godziną i dniem wizyty (dowód, że zdarzenie miało miejsce). Pacjent wychodzi. Pacjentowi nie udostępniono informacji z art. 13 RODO.

Naruszenie:

- złamanie art. 13 RODO, złamanie art. 5 ust. 1 lit. a RODO (w zakresie zasady rzetelności i zasady przejrzystości).

Szkoda:

- niemajątkowa, pacjent odczuwa cierpienie psychiczne wynikające z faktu, że nie poinformowano go o szczegółach przetwarzania jego danych osobowych.

Ktoś pyta czy przychodnia posiada dane osobowe dotyczące konkretnego, wskazanego pacjenta i jakie dane przychodnia posiada (art. 15 ust. 1 lit. b RODO). Osoba pyta pocztą elektroniczną, przychodnia odpowiada, że posiada takie to a takie dane. Przychodnia nie sprawdziła, czy

osoba pytająca to naprawdę pacjent. W istocie pytał kto inny np. kolega pacjenta, pacjent się o tym dowiedział od tej osoby.

Naruszenie:

- art. 15 RODO, ponieważ informacja przysługuje pacjentowi a nie każdej osobie fizycznej
- art. 5 ust. lit. a (w zakresie zasady zgodności z prawem),
- art. 6 ust. 1 RODO, również ewentualnie (zależnie od kategorii ujawnionych informacji) art., 9 ust. 1 RODO
- złamanie art. 5 ust. 1 lit. f ROD (w zakresie zasady poufności).

Szkoda:

- niemajątkowa, pacjent odczuwa cierpienie psychiczne wynikające z faktu, że osoby postronne dowiedziały się, że leczy się w danej przychodni, że jego dane przetwarzane są niezgodnie z prawem, czyli że naruszono jego wolność od przetwarzania jego danych w sposób niezgodny z prawem.

Pacjent pyta czy przychodnia posiada dotyczące go dane osobowe i jakie dane przychodnia posiada (art. 15 ust. 1 lit. b RODO). Pacjent pyta mailem, przychodnia nie odpowiada na pytanie, nie podejmuje kroków w celu ustalenia tożsamości osoby pytającej.

Naruszenie:

- art. 15 RODO, ponieważ informacja przysługuje pacjentowi, jedynie trzeba ustalić, czy pytający to ten pacjent,
- art. 5 ust. lit. a RODO (w zakresie zasady rzetelności i zasady przejrzystości),

Szkoda:

- niemajątkowa, pacjent odczuwa cierpienie psychiczne, które wynika z faktu, że nie wiedział (co prawda w końcu się dowiedział, ale kiedy pytał to nie wiedział, więc cierpiał) kto przetwarza jego dane osobowe i w jakim zakresie.

Pacjent żąda poprawienia danych w swojej dokumentacji medycznej (literówka w nazwisku, zła data urodzenia etc.). Jego żądanie zostaje zignorowane.

Naruszenie:

- art. 16 RODO,
- art. 5 ust. lit. d RODO.

Szkoda:

- niemajątkowa, pacjent odczuwa cierpienie psychiczne, które wynika z faktu, że w dokumentacji znajdują się jego nieprawdziwe dane, że pracownicy podmiotu takie dane widzą itd.

Przychodnia podpisała umowę powierzenia przetwarzania z podmiotem, który nie jest podmiotem przetwarzającym tylko nowym administratorem, na przykład z inną przychodnią lub z laboratorium. Pacjent udaje się do tego nowego administratora, jednak ten nie realizuje art. 14 ponieważ uważa, że jest podmiotem przetwarzającym.

Naruszenie:

- złamanie art. 14 RODO, złamanie art., 5 ust. 1 lit. a RODO (w zakresie zasady rzetelności i zasady przejrzystości).

Szkoda:

- niemajątkowa, pacjent odczuwa cierpienie psychiczne, które wynika z faktu, że nie poinformowano go o szczegółach przetwarzania jego danych osobowych.

Pacjent zapytuje, w trybie ustawy o dostępie do informacji publicznej, przychodnię czy ta posiada rejestr czynności przetwarzania danych. Przychodnia nie odpowiada na pytanie ponieważ rejestru nie posiada, albo odpowiada, że rejestru nie posiada.

Naruszenie:

- art. 30 ust. 1 RODO w zw. z art. 30 ust. 5 RODO.

Szkoda:

- niemajątkowa, pacjent odczuwa cierpienie psychiczne, które wynika z faktu, że jego dane są niekompetentnie chronione.

„Odpowiedzialność cywilna spowodowana brakiem dokumentacji

Nałożenie kary administracyjnej nie jest jedynym zagrożeniem, z którym powinien liczyć się administrator danych. Artykuł 82 ust 1 RODO stanowi: „Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.”. Wydaje się, że szkodę niemajątkową można utożsamić z krzywdą. Łatwo wyobrazić sobie osobę, która podnosi przed sądem, że poniosła szkodę niemajątkową o charakterze krzywdy, a szkoda ta wynika z faktu, że ADO prze-

tworzą dane osobowe tej osoby z lekceważeniem zasad przetwarzania danych osobowych, że ADO łamie zasady lub zasadę. Lekceważenie takie łatwo jest wykazać. Jeżeli powód wykaże złamanie którejś z zasad, poprzez wykazanie niestosowania realizującego zasadę przepisu, to pozwanemu, czyli administratorowi danych nie pozostaje nic innego, jak tylko wykazać, że zasadę tę szanuje. Najprostszym sposobem wykazania poszanowania zasady, jest przedstawienie dokumentu, z którego wynika, że zasadę tę się szanuje. Artykuł 82 ust 1 RODO stanowi: „Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności (...), jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody”. Jeżeli istotą szkody niematerialnej jest zachodzący u administratora danych brak dokumentu lub nieposzanowanie zasady przetwarzania danych osobowych poprzez brak dokumentu i jeżeli administrator nie posiada przedmiotowego dokumentu, to nie ma on możliwości wykazać, że szkoda nie nastąpiła. Dokumenty trzeba zatem prowadzić, zarówno z racji poszanowania dla prawa, jak i z ostrożności.”⁶²

⁶² J. Rzymowski. *Op. cit.* Kraków 2019. s. 10-11.

Wdrożenie RODO w podmiocie

Krok po kroku

Wdrożenie RODO w podmiocie

Krok po kroku

Wdrożenie RODO to wdrożenie 3 elementów.

- 1) zadbanie o to by informacje o pacjentach były dobrze chronione przed zniszczeniem i przed udostępnieniem osobom nieuprawnionym
- 2) zadbanie o realizację uprawnień pacjentów (prawo do dostępu do danych, prawo do poprawiania, do usuwania)
- 3) zadbanie o właściwą dokumentację konieczną do wykazania obowiązków wskazanych w punktach 1 i 2.

Kolejność przygotowywania dokumentów

Poniżej wymieniamy w jakiej kolejności należy przygotowywać dokumentację związaną z RODO, tak by było to zbieżne z wdrożeniem i by uniknąć kilkukrotnego wykonywania tej samej pracy.

Najpierw należy przygotować:

Rejestr czynności przetwarzania (RCPD)

Kiedy mamy już RCPD, to w oparciu o rejestr:

- Przygotowujemy **dokument** informujący o szczegółach przetwarzania danych wymienionych w **art. 13 RODO**.
- Przygotowujemy **dokument** informujący o szczegółach przetwarzania danych wymienionych w **art. 14 RODO**.
- Przygotowujemy **dokument** informujący o szczegółach przetwarzania danych wymienionych w **art. 15 RODO**.

- W oparciu o RCPD przygotowujemy **upoważnienia do przetwarzania** (chyba, że ich nie przygotowujemy, odsyłam do rozdziału o upoważnieniach i poleceniach).
- Przeprowadzamy **ocenę ryzyka przetwarzania** – z wykorzystaniem dokumentów oceny ryzyka.
- Przygotowujemy **ogólny opis technicznych i organizacyjnych środków bezpieczeństwa**, który załączamy do RCPD.

- Przygotowujemy **politykę ochrony**, czyli dokument, w którym opisujemy jak w podmiocie realizowane są kolejne obowiązki z zakresu RODO interpretowanego łącznie z przepisami spoza RODO, doprecyzowującymi szczegóły przetwarzania danych osobowych.

Pierwszy etap wdrożenia

Za pierwszy etap wdrożenia bywa uważany audyt przestrzegania RODO. Jeden z autorów (D. S.) zaczyna wdrożenia od tego etapu, drugi (J. Rz.) uważa, że jeżeli RODO nie jest wdrożone w podmiocie, to robienie audytu jest zbędne. Oba stanowiska wydają się być uzasadnione.

Audyt przestrzegania RODO

- Celem audytu jest ustalenie czy obowiązki wynikające z RODO i ewentualnie z przepisów innych ustaw, są w danym podmiocie realizowane.
- Celem audytu może być też sprawdzenie czy RODO zostało dobrze wdrożone.
- Celem audytu może być sprawdzenie pracy IODA.

Pozyskanie i usystematyzowanie informacji dotyczących podmiotu, realiów jego funkcjonowania, otoczenia w jakim funkcjonuje, pozwala na racjonalizację czynności i merytoryczne opracowanie indywidualnego planu działania. **Audyt** służyć może także rozpoznaniu dobrych praktyk, których funkcjonowanie nie powinno zostać zaburzone wdrożeniem nowych projektowanych procedur. Pamiętać należy o sile przyzwyczajenia personelu do stosowania utartych metod postępowania oraz o tym, jak trudno jest je modyfikować.

Elementem istotnym, z punktu widzenia sprawności wdrażania poszczególnych rozwiązań, jest **zbudowanie zespołu osób**, które będą zaangażowane w proces. Warto jest zadbać o to, aby to zarządzający wskazali osoby właściwe do takiej współpracy. Konsekwencją powyższego wskazania jest wzbudzenie świadomości, po stronie zaangażowanych pracowników, iż oddelegowani zostaną do nowych zadań, ale i osoby decyzyjne pozyskują świadomość tego, iż nowe zadania realizowane będą w dotychczasowym wymiarze czasu pracy personelu wyznaczonego, czemu niewątpliwie muszą dać wyraz przy rozliczaniu z wykonania dotychczasowego zakresu powierzonych obowiązków

tym osobom. Takie posunięcie również pokazuje, iż realizacja procesu wdrożenia ma znaczenie dla osób zarządzających podmiotem a jego poprawna realizacja jest istotna z punktu widzenia żywotnych interesów jednostki.

Dobłą praktyką jest kierowanie, tak utworzonym zespołem, poprzez **rozdzielanie zadań, wskazywanie osób odpowiedzialnych** za ich realizację oraz **rozliczanie terminowości** ich wykonywania. Dokumentem pomocnym może być tutaj swego rodzaju „Karta Czynności”, jaką kierujący zespołem załączać może do każdej dyspozycji, do każdego dokumentu, który powinien wywołać określone skutki, czy działania. Dla przykładu, założmy, iż przygotowana została treść klauzul informacyjnych przy pomocy, których administrator realizuje swój obowiązek informacyjny na gruncie RODO i zgodnie z przyjętą w podmiocie procedurą konieczne jest zamieszczenie tych dokumentów na stronie internetowej podmiotu. Oczywiście jest, iż pion IT jest odpowiedzialny za tego rodzaju zadanie, aby jednak usprawnić realizację tego zadania oraz równocześnie stworzyć warunki do weryfikacji poprawności jego wykonania, możemy posłużyć się „Kartą Czynności”. Dokument ten nie tylko stanowił będzie dowód tego, iż dyspozycja umieszczenia na stronie gotowych plików zawierających klauzule informacyjne została wydana, będzie również potwierdzał, iż dokumentacja została przekazana osobie wyznaczonej, jako odpowiedzialnej za wykonanie procesu. Ponadto dokument ten będzie określał precyzyjnie czynności, jakie taka osoba powinna wykonać w związku z powierzonym jej do realizacji zadaniem oraz wskazywał będzie termin zobowiązana została do jego realizacji.

Tylko precyzyjne formułowanie zadań oraz wskazywanie osób odpowiedzialnych za ich realizację oraz terminów, w jakich powinny być one wykonywane, daje gwarancję, iż wdrożenie przebiegnie według przewidywanego scenariusza. Praktyka bowiem pokazuje, iż wyznaczanie zadań, z pominięciem elementu wyznaczania właściciela procesu odpowiedzialnego za jego realizację, może prowadzić do tego, iż zadanie nie zostanie zrealizowane, bądź zrealizowane zostanie po terminie, albo jego realizacja rozpocznie się dopiero wówczas, kiedy zlecający ponownie zainteresuje się tematem. Naturalnie jednak decyzja o stosowaniu „Kart Czynności” pozostawiana jest administratorowi, który rozpoznaje najskuteczniejsze metody i narzędzia do zarządzania procesami w swojej strukturze. Poniżej przedstawiamy „Karty

Czynności”, jakie przykładowo wypełniliśmy dla opisanego zadania, jakim jest zamieszczenie gotowych opracowanych dokumentów na stronie internetowej podmiotu. Na kolejnej stronie natomiast zamieszczamy wzór „Karty czynności”, jaką można bezpośrednio wykorzystać w procesie wdrożenia. Naturalnie, kartę można modyfikować według własnego uznania.

KARTA CZYNNOŚCI	
Wzory Klauzul Informacyjnych RODO / Zamieszczenie na stronie internetowej	
Sposób przekazania:	Dokumentacja przekazana za pośrednictwem email na adres kierownikit@..... .pl
Data przekazania:	 202...
Zalecane działania dotyczące dokumentu:	
Dokument należy wydrukować :	TAK / NIE
Dokument należy podpisać :	TAK / NIE
Należy wyznaczyć osobę odpowiedzialną za realizację zadań opisanych w dokumencie:	TAK / NIE
Należy podać imię i nazwisko osoby odpowiedzialnej za realizację zadań opisanych w dokumencie:	Imię / Nazwisko: Jan Kowalski / Kierownik IT
Należy zapoznać całą załogę z treścią dokumentu:	TAK / NIE
Należy zapoznać część załogi z treścią dokumentu:	TAK / NIE
Należy odebrać od załogi pisemne potwierdzenie zapoznania się z treścią dokumentu.	TAK / NIE
Data realizacji zadań określonych dokumentem:	12.11.2021
Uwagi IOD	Pliki przekazane w załączniku, należy zamieścić na stronie internetowej podmiotu w sekcji „Obowiązek Informacyjny RODO” zachowując ich format oraz publikując datę ich zamieszczenia w tej wersji na stronie WWW.
Zlecający	Prezes Zarządu
Data realizacji zadania oraz ewentualne uwagi	

KARTA CZYNNOŚCI	
Opis zadania / Rodzaj przekazywanych dokumentów	
Sposób przekazania:	
Data przekazania:	
Zalecane działania dotyczące dokumentu:	
Dokument należy wydrukować:	TAK / NIE
Dokument należy podpisać:	TAK / NIE
Należy wyznaczyć osobę odpowiedzialną za realizację zadań opisanych w dokumencie:	TAK / NIE
Należy podać imię i nazwisko osoby odpowiedzialnej za realizację zadań opisanych w dokumencie:	
Należy zapoznać całą załogę z treścią dokumentu:	TAK / NIE
Należy zapoznać część załogi z treścią dokumentu:	TAK / NIE
Należy odebrać od załogi pisemne potwierdzenie zapoznania się z treścią dokumentu.	TAK / NIE
Data realizacji zadań określonych dokumentem:	
Uwagi IOD	
Zlecający	
Data realizacji zadania oraz ewentualne uwagi	

Rejestr czynności przetwarzania

Obowiązek stworzenia rejestru czynności przetwarzania danych osobowych (dalej: RCPD), za który odpowiada administrator⁶³ (danych osobowych), wynika z art. 30 ust. 1 RODO, przepis ten stanowi: „Każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają.(...)”.

Obowiązek prowadzenia RCPD ma administrator, który przetwarza dane osobowe tak, że przetwarzanie, którego dokonuje, „obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 (...)”.

PWDL ma obowiązek prowadzić rejestr czynności przetwarzania danych osobowych

Wskazujemy niżej jak najlepiej sporządzić taki rejestr. Podczas kolejnych wdrożeń zauważyliśmy jednak, że RCPD jest dokumentem powtarzalnym. Są drobne różnice między RCPD dla przychodni jednospecjalistycznej, dwuspecjalistycznej a wielospecjalistycznej, ale są one właśnie drobne.

Zamieszczone poniżej fragmenty RCPD to tak na prawdę fragmenty RCPD sporządzanych przez nas przy okazji kolejnych wdrożeń i doskonalonych.

„Dla realizacji zasady rozliczalności dobrze jest opatrzyć każdy wpis w RCPD datą jego sporządzenia.⁶⁴ Należy pamiętać, że RCPD, ma charakter rejestru aktualizowanego. Aktualizacje nie będą może częste, ale jeżeli pojawi się nowa czynność przetwarzania, nowy cel przetwarzania, nowa kategoria odbiorców, to RCPD należy zaktualizować. Skoro ADO jest zgodnie z art. 5 ust. 2 RODO odpowiedzialny za realizację przepisów (przepis stanowi o zasadach, ale te realizuje

⁶³ <https://uodo.gov.pl/pl/225/659> (Dostęp: 2022.02.27 godz. 17:04)

⁶⁴ Podobnie: G. Sibiga, K. Syska, *Ogólne rozporządzenie o ochronie danych*. Warszawa 2017. s. 374 i s. 377.

się właśnie, choć nie tylko, przez przepisy), to dobrze by z RCPD wynikało, kiedy dokładnie ADO art. 30 ust 1 RODO zrealizował.”.⁶⁵

Zalecamy posługiwanie się papierowym RCPD, ze względu na wynikający z art. 30 ust. 3 RODO obowiązek prowadzenia RCPD w formie pisemnej w tym elektronicznej. Forma pisemna to forma z podpisem odręcznym. Forma pisemna elektroniczna, to forma z podpisem elektronicznym kwalifikowanym. Przypominamy jednak o tym, że jeżeli ktoś sporządzi RCPD i podpisze go podpisem kwalifikowanym, to jeśli uzupełni rejestr, poprzez dopisanie czegoś do podpisanego pliku, to podpis wewnętrzny zniknie a podpis zewnętrzny nie zostanie pozytywnie zweryfikowany. By tych problemów uniknąć, należy sporządzać rejestr na papierze i podpisywać każdą jego stronę.

Niestety i tu musimy wypowiedzieć się w kwestii zadziwiających wypowiedzi NIK. Otóż NIK, z nieznanych przyczyn uznał,⁶⁶ że konieczne są obie formy, pisemna i elektroniczna.

W trzech szpitalach rejestr prowadzono nierzetelnie. W trzech skontrolowanych szpitalach (12,5%) rejestr prowadzony był nierzetelnie.

Przykłady

W Szpitalu Wojewódzkim im. Mikołaja Kopernika w Koszalinie w prowadzonym rejestrze nie uwzględniono elementu wymaganego przepisami art. 30 ust 1 lit. a RODO, tj. informacji zawierającej imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także – gdy ma to zastosowanie – przedstawiciela administratora oraz IOD. Jednocześnie rejestr nie był prowadzony w wymaganej formie elektronicznej, a jedynie papierowej.

W Szpitalu Neuropsychiatrycznym im. Prof. Mieczysława Kaczyńskiego SP ZOZ w Lublinie rejestr czynności przetwarzania nie zawierał m.in. czynności związanych z przetwarzaniem danych osobowych pacjentów (oprócz realizacji recept), jak również nie uwzględniono w nim wszystkich czynności wskazanych w informacjach złożonych do IOD przez kierowników poszczególnych oddziałów szpitala.

Zaznaczamy i podkreślamy, że myli się NIK, kiedy twierdzi, że prowadzenie rejestru jedynie w formie papierowej jest „nierzetelne”. Niestety widać, że systemowy problem braku kompetencji w dzie-

⁶⁵ J. Rzymowski. *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*. Kraków 2019. s. 45.

⁶⁶ Informacja o wynikach kontroli. WDROŻENIE PRZEZ PODMIOTY LECZNICZE REGULACJI DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH. LBI. 430. 004.2019. Nr ewid. 149/2019/P/19/063/LBI. s. 22.
https://www.nik.gov.pl/plik/id,21467,v,artykul_20436.pdf (Dostęp: 2022.02.22 godz. 17:04)

dzinie prawa ochrony danych osobowych w NIK jest faktem. Jest i czyni wiele złego.

Konstrukcja RCPD

Poniżej przedstawiamy proponowaną strukturę dokumentu, w ramach której wyodrębniono

„**Czynności przetwarzania**”,

„**Część A**”, która ma charakter strony tytułowej oraz

„**Część B**”, która stanowi zasadniczą część Rejestru, w której kolejno ułożone zostały nazwane i wyodrębnione czynności przetwarzania, jako operacji na danych podejmowanych i realizowanych w związku zamiarem osiągnięcia określonego celu.

Skutkiem powyższego, czynności przetwarzania realizowane w określonym celu składać mogą się z szeregu różnych operacji podjęcie, których jest warunkiem koniecznym osiągnięcia zamierzonego rezultatu, czyli celu przetwarzania.

Zaznaczyć należy, iż proponowany kształt dokumentu nie ma charakteru ostatecznego i bezwzględnie wiążącego, zarówno w części odnoszącej się do sposobu wyodrębniania czynności przetwarzania, ich rodzaju i liczby, jak i struktury graficznej dokumentu. W praktyce spotkać można różne warianty jego tworzenia. W każdym jednak razie powinien on zawierać te informacje, o których mowa w przepisach prawa.

Wskazać także należy, że jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 Rozporządzenia RODO, może stanowić jego element, co nie jest jednak warunkiem koniecznym.

Ponadto warto spojrzeć na RCPD, jako na dokument istotnie pomocny przy realizacji obowiązku, jakim jest sporządzenie oceny ryzyka naruszenia praw lub wolności osób fizycznych. Zalecamy wykorzystanie struktury ww. Rejestru w celu wykonania ww. oceny.

REJESTR CZYNNOŚCI PRZETWARZANIA

Spis treści

Czynności przetwarzania

1. Obsługa kandydatów do pracy - rekrutacja własna.
2. Obsługa kandydatów do pracy - rekrutacja zewnętrzna.
3. Obsługa kandydatów do pracy - weryfikacja na podstawie rejestru sprawców przestępstw na tle seksualnym.
4. Obsługa pracowników - obsługa kadrowa.
5. Obsługa pracowników - obsługa płacowa, w tym w zakresie dokonywania zgłoszeń do ZUS, aktualizacja zgłoszeń i przekazywanie danych o zwolnieniach.
6. Obsługa pracowników - w zakresie realizacji przepisów dot. Bezpieczeństwa i Higieny Pracy (BHP) i ochrony przeciwpożarowej (P.POŻ).
7. Obsługa pracowników - dotyczy stażystów / praktykantów / wolontariuszy.
8. Obsługa pracowników - w zakresie zadań z medycyny pracy
9. Obsługa pracowników - w zakresie wniosków o rentę z tytułu niezdolności do pracy, o emeryturę.
10. Obsługa pracowników - w zakresie uprawnień wynikających z Zakładowego Funduszu Świadczeń Socjalnych (ZFŚS)
11. Obsługa pracowników - Pracownicze Plany Kapitałowe (PPK)
12. Obsługa pracowników - Kasy Zapomogowo Pożyczkowe (KZP)
13. Obsługa pracowników - w zakresie wynikającym z obowiązków dotyczących chorób zawodowych.
14. Obsługa umów cywilnoprawnych - zawartych w obszarze medycyny.
15. Obsługa umów cywilnoprawnych - zawartych poza obszarem medycyny.
16. Obsługa pacjentów - w zakresie zadań realizowanych przez jednostkę jako służbę medycyny pracy.
17. Obsługa pacjentów - w zakresie składania deklaracji wyboru lekarza /pielęgniarki / położnej / POZ.
18. Obsługa pacjentów - rejestracja na miejscu w siedzibie, telefonicznie, e-rejestracja.
19. Obsługa pacjentów - w zakresie wpisania do kolejki oczekujących.
20. Obsługa pacjentów - udzielanie świadczeń zdrowotnych.
21. Obsługa pacjentów - w zakresie skierowania na badania diagnostyczne

w związku z kontynuacją leczenia.

22. Obsługa pacjentów - w zakresie wykonywania badań diagnostycznych.
23. Obsługa pacjentów - w zakresie prowadzenie szczepień ochronnych.
24. Obsługa pacjentów - w zakresie obsługi zwolnienia lekarskiego.
25. Obsługa pacjentów - udzielanie informacji nt. stanu zdrowia.
26. Obsługa pacjentów - udostępnianie dokumentacji medycznej.
27. Obsługa pacjentów - w zakresie wystawiania / wydawania recept.
28. Obsługa pacjentów - w związku z realizacją obowiązków wynikających z ustawy z dnia 05 grudnia 2008 r., o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi.
29. Obsługa pacjentów - w zakresie przetwarzanie danych opieki środowiskowej i wizyt patronażowych.
30. Obsługa pacjentów - w zakresie transportu sanitarnego.
31. Obsługa pacjentów - w zakresie przyjmowania skarg, wniosków i petycji.
32. Obsługa pacjentów - w zakresie organizacji odwiedzin.
33. Obsługa kancelaryjna jednostki - ewidencja korespondencji.
34. Monitoring wizyjny - realizacja zadań związanych z funkcjonowaniem monitoringu wizyjnego.
35. Utrzymanie ciągłości i poprawności działania systemów informacyjnych.
36. Działania marketingowe.
37. Działania podejmowane w związku z ochroną roszczeń.
38. Archiwizacja - realizacja zadań związanych z archiwizowaniem dokumentacji oraz jej brakowaniem i niszczeniem.

REJESTR CZYNNOŚCI PRZETWARZANIA
CZĘŚĆ A

Rejestr prowadzony w oparciu o art. 30 ust. 1 przepisów Rozporządzenia PE
i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób
fizycznych w związku z przetwarzaniem danych osobowych

**Nazwa oraz dane kontaktowe
administratora oraz wszelkich
współadministratorów oraz w od-
powiednich przypadkach przed-
stawiciela administratora**

**Imię i nazwisko oraz dane kon-
taktowe Inspektora Ochrony
Danych Osobowych**

REJESTR CZYNNOŚCI PRZETWARZANIA CZĘŚĆ B	
Nazwa czynności przetwarzania	OBSŁUGA KANDYDATÓW DO PRACY. - rekrutacja własna
Cele przetwarzania	Przetwarzanie danych osobowych dla celów rekrutacji – czynności rekrutacyjne wykonywane we własnym zakresie
Opis kategorii osób, których dane dotyczą,	Osoba ubiegająca się o zatrudnienie. (Kandydat do pracy).
Opis kategorii danych osobowych, przetwarzanych w ramach czynności	) dane identyfikacyjne,) dane kontaktowe wskazane przez kandydata) dane o wykształceniu - gdy niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku) dane o kwalifikacjach zawodowych - gdy niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku) dane o przebiegu dotychczasowego zatrudnienia - gdy niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku) dane inne podane przez samą osobę ubiegającą się o zatrudnienie (kandydata do pracy) > imię (imiona) i nazwisko > data urodzenia > nazwisko rodowe > dane kontaktowe wskazane przez taką osobę > wykształcenie - gdy niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku (nazwa szkoły, rok ukończenia, zawód, specjalność, stopień naukowy, tytuł zawodowy, tytuł naukowy) > kwalifikacje zawodowe - gdy niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku (kursy, studia podyplomowe lub inne formy uzupełnienia wiedzy

	lub umiejętności) > przebieg dotychczasowego zatrudnienia - gdy niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku (okresy zatrudnienia u kolejnych pracodawców oraz zajmowane stanowiska pracy) > dane o stanie zdrowia - podane przez samą osobę ubiegającą się o zatrudnienie (kandydata do pracy) > wizerunek / zdjęcie - podane przez samą osobę ubiegającą się o zatrudnienie (kandydata do pracy)
Źródło danych	Osoba ubiegająca się o zatrudnienie (Kandydat do pracy)
Podstawa prawna przetwarzania stanowiąca uzasadnienie dla zgodnego z prawem wykonywania czynności przetwarzania	) Rozporządzenie RODO • art. 6 ust. 1 lit. b) RODO - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy, • art. 6 ust. 1 lit. c) RODO - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. • art. 6 ust. 1 lit. a) RODO – osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych a. w zakresie szerszym aniżeli dane określony przepisami prawa, b. na potrzebę realizacji kolejnych postępowań rekrutacyjnych. • art. 6 ust. 1 lit. c) w związku z art. 9 ust. 2 list a) RODO – osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie danych osobowych o jakich mowa w art. 9 ust. 1 RODO.) Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy > art. 22(1) par 1, par. 4 k.p.) Przepisy wykonawcze do Kodeksu Pracy – właściwe) Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej.) Ustawa z dnia 20 kwietnia 2004 r. o promocji

	zatrudnienia i instytucjach rynku pracy) Ustawa z dnia 09 lipca 2003 r. o zatrudnieniu pracowników tymczasowych) Ustawy z dnia 13 maja 2016r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym. > Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r., w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika > Rozporządzenie Ministra Rodziny , Pracy i Polityki Społecznej z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej
Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych	Poczta Kurier Internauci zapoznający się z danymi umieszczonymi na stronie WWW / BIP Zewnętrzna kancelaria prawna <u>Nazwa:</u> <u>Adres siedziby:</u>
Podmiot przetwarzający	) Zewnętrzny podmiot kadrowy <u>Nazwa:</u> <u>Adres siedziby:</u> ) Zewnętrzny podmiot płacowy <u>Nazwa:</u> <u>Adres siedziby:</u> ) Zewnętrzny podmiot usług IT <u>Nazwa:</u> <u>Adres siedziby:</u>

	) Zewnętrzny hostingodawca <u>Nazwa:</u> <u>Adres siedziby:</u>
Nazwa państwa trzeciego lub organizacji międzynarodowej, którym przekazywane są dane osobowe, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń	Nie dotyczy
Planowane terminy usunięcia poszczególnych kategorii danych	Niezwłocznie po zakończonym procesie rekrutacji, w sytuacji kiedy kandydat nie stał się Pracownikiem Jednostki, chyba że kandydat do pracy wyraził zgodę na udział w przyszłych procesach rekrutacji, wówczas dokumentacja przechowywana będzie do czasu wycofania zgody lub ustania celu dalszego przetwarzania.
Nazwa systemu informatycznego (Oprogramowania) służącego do przetwarzania danych osobowych	Nazwa
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art.	/a/ Dokumentacja przechowywana w wyznaczonym miejscu. /b/ Pomieszczenie zamykane jest na klucz. /c/ Dokumenty przechowywane w szafkach zamykanych na klucz. /d/ Dostęp do kluczy mają tylko upoważnione

32 ust. 1 RODO	osoby. /e/ Pomieszczenie objęte alarmem przeciwwłamaniowym. /f/ Szyfrowanie transmisji. /g/ Szyfrowanie danych składowany na nośnikach danych. /h/ Indywidualne konta dostępowe do systemów informatycznych. /i/ Zabezpieczanie kont użytkowników hasłami. /j/ Automatyczne blokowanie stacji roboczych po upływie 2 minut.
-----------------------	---

Jak widać, przedstawiony wzór zapisów RCPD przygotowanych dla przetwarzania danych w związku z prowadzonymi przez podmiot postępowaniami rekrutacyjnymi, uwypukla szereg kontrowersji, interpretacyjnych, z jakimi administratorzy będą musieli się zmierzyć. Począwszy od przyjęcia metodyki wyodrębniania poszczególnych czynności przetwarzania, poprzez przyjęcie stopnia szczególności przy określaniu kategorii danych osobowych przetwarzanych w ramach czynności. W przygotowanym przez nas wzorze zaprezentowaliśmy połączenie dwóch metod opisywania kategorii danych:

- a) metodę zakładającą posługiwanie się ogólną nazwą np. dane identyfikacyjne – zaznaczenie pozycji „)”
- b) oraz metodę precyzyjną, zgodnie, z którą w sposób szczegółowy określone są dane przetwarzane np. imię, nazwisko kandydata - zaznaczenie pozycji „>”.

Dalece kontrowersyjne wydaje się podejście przedstawione w treści Decyzji Prezesa Urzędu Ochrony Danych Osobowych z dnia 03 kwietnia 2019r. (ZSPU.421.8..2018)⁶⁷, cyt.: „(...) informacja o podmiocie, któremu Burmistrz W. powierzył przetwarzanie danych osobowych, w związku z prowadzeniem rejestru mieszkańców w systemie informatycznym A, w zakresie nazwy i adresu siedziby tego podmiotu powinna zostać przekazana osobie, której dane dotyczą, w związku z zasadą przejrzystego informowania (...)", co ozna-

⁶⁷ <https://uodo.gov.pl/decyzje/ZSPU.421.8.2018> (Dostęp: 2022.02.22 godz. 17:11)

cza tyle, iż tak precyzyjny zestaw danych powinien opisywać odbiorców danych, ze względu na konieczność respektowania zasady przejrzystości. Z tego względu zaprezentowaliśmy dwa sposoby prezentacji. W pierwszym określiliśmy kategorie ww. podmiotów, odwołując się do zakresu czynności przez nie realizowanych, w drugim zakres doprecyzowaliśmy poprzez podanie danych o nazwie i adresie takiego podmiotu przetwarzającego, czy odbiorcy.

Podnieść jednak należy, iż w treści wskazanej decyzji wydanej w indywidualnej sprawie, jaka dotyczyła podmiotu publicznego, zalecenie dotyczące precyzyjności określania odbiorców, podyktowane było przepisami o dostępie do informacji publicznej. Dlatego organ wydający decyzję zasygnalizował, że określenia odbiorców powinny mieć charakter precyzyjny w kontekście przepisów ustawy z 6.09.2001 r. o dostępie do informacji publicznej (Dz.U. z 2019 r. poz. 1429).

Postępując według przyjętego schematu, posługując się opracowanym wzorem, opisaliśmy poszczególne czynności przetwarzania. Dla zobrazowania złożoności tematu przedstawiliśmy kilka z nich poniżej. Zwracamy jednak szczególną uwagę na fakt, iż dokument ten opracowany w sposób rzetelny i kompletny w znaczny sposób ułatwia administratorowi wykonywanie dalszych czynności. Niestety jednak dynamika zmian otoczenia, w jakim funkcjonują jednostki, w tym otoczenia prawnego, wymusza na administratorze konieczność monitorowania ich oraz adekwatnego aktualizowania zapisów Rejestru Czynności Przetwarzania Danych.

Nazwa czynności przetwarzania	OBSŁUGA PRACOWNIKÓW - obsługa kadrowa
Cele przetwarzania	Przetwarzanie danych osobowych w związku z realizacją obowiązków pracodawcy, jako strony stosunku pracy.
Opis kategorii osób, których dane dotyczą,	) Pracownicy.) Członkowie najbliższej rodziny pracownika.) Osoby wskazane przez pracownika do kontaktu.) Byli pracownicy.
Opis kategorii danych osobowych, przetwarzanych w ramach czynności	) dane identyfikacyjne,) dane kontaktowe) dane o wykształceniu, kwalifikacjach, przebiegu dotychczasowego zatrudnienia - gdy jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku) inne dane osobowe pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy) dane dotyczące numeru rachunku płatniczego, jeżeli pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych) dane o warunkach zatrudnienia) dane o zajęciach komorniczych) dane o przynależności związkowej) dane o przynależności do branżowych struktur zawodowych) dane o stanie zdrowia > imię (imiona) i nazwisko > data urodzenia > dane kontaktowe > wykształcenie - gdy jest to niezbędne do wykonywania pracy określonego rodzaju lub

	na określonym stanowisku > kwalifikacje zawodowe - gdy jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku > przebieg dotychczasowego zatrudnienia - gdy jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku > dane dotyczące warunków zatrudnienia > dane o zajęciach komorniczych > dane o potrąceniach dokonywanych na wniosek > dane o przynależności związkowej > dane o przynależności do branżowych struktur zawodowych > dane o stanie zdrowia > adres zamieszkania > numer PESEL (a w przypadku jego braku – rodzaj i numer dokumentu potwierdzającego tożsamość) > imiona i nazwiska oraz daty urodzenia dzieci, a także dane osobowe innych członków najbliższej rodziny, w przypadku zamiaru korzystania ze szczególnych uprawnień przewidzianych w prawie pracy > numer rachunku płatniczego, jeżeli pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych > dane osoby, którą należy zawiadomić w razie wypadku, jeżeli pracownik wyrazi zgodę na podanie danych osobowych takiej osoby
Źródło danych	Pracownicy
Podstawa prawna przetwarzania stanowiąca uzasadnienie dla	) Rozporządzenie RODO • art. 6 ust. 1 lit. b) RODO - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której

zgodnego z prawem wykonywania czynności przetwarzania	dane dotyczą, przed zawarciem umowy, • art. 6 ust. 1 lit. c) RODO - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. • art. 6 ust. 1 lit. d) RODO - przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej. • art. 6 ust. 1 lit. c) w związku z art. 9 ust. 2 lit b) RODO - przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą. • art. 6 ust. 1 lit. a) RODO – osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych • art. 6 ust. 1 lit. a) w związku z art. 9 ust. 2 list a) RODO – osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie danych osobowych o jakich mowa w art. 9 ust. 1 RODO.) Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy) Przepisy wykonawcze do Kodeksu Pracy - właściwe > Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r., w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika > Rozporządzenie Ministra Rodziny , Pracy
---	---

	i Polityki Społecznej z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej > Rozporządzenie z dnia 30 grudnia 2016 r. Ministra Rodziny, Pracy i Polityki Społecznej w sprawie świadectwa pracy.) Ustawa z 13 października 1998 r. o systemie ubezpieczeń społecznych) Ustawa z dnia 8 czerwca 2017 r. o sposobie ustalania najniższego wynagrodzenia zasadniczego pracowników wykonujących zawody medyczne zatrudnionych w podmiotach leczniczych) Ustawa z 15 kwietnia 2011 r. o działalności leczniczej) Ustawa z 26 lipca 1991 r. o podatku dochodowym od osób fizycznych) Ustawa z 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych) Ustawa z 10 października 2002 r. o minimalnym wynagrodzeniu za pracę. > Rozporządzenie Ministra Zdrowia z 20 lipca 2011 r. w sprawie kwalifikacji wymaganych od pracowników na poszczególnych rodzajach stanowisk pracy w podmiotach leczniczych niebędących przedsiębiorcami
Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych	Poczta Kurier Zewnętrzna kancelaria prawna <u>Nazwa:</u> <u>Adres siedziby:</u> Przedsiębiorstwo ubezpieczeniowe ZUS/KRUS

	NFZ GUS Związek Zawodowy <u>Nazwa:</u> <u>Adres siedziby:</u> Kasa Zapomogowo Pożyczkowa Pracownicze branżowe struktury zawodowe <u>Nazwa:</u> <u>Adres siedziby:</u>
Podmiot przetwarzający	) Zewnętrzny podmiot kadrowy <u>Nazwa:</u> <u>Adres siedziby:</u>) Zewnętrzny podmiot usług IT <u>Nazwa:</u> <u>Adres siedziby:</u>) Zewnętrzny hostingodawca <u>Nazwa:</u> <u>Adres siedziby:</u>) Zewnętrzny podmiot bhp / p.poż <u>Nazwa:</u> <u>Adres siedziby:</u>
Nazwa państwa trzeciego lub organizacji	Nie dotyczy

międzynarodowej, którym przekazywane są dane osobowe, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń	
Planowane terminy usunięcia poszczególnych kategorii danych	) W stosunku do pracowników zatrudnionych po 31 grudnia 1998 r. a przed 1 stycznia 2019 r. – okres przechowywania dokumentacji pracowniczej wynosi 50 lat;) W stosunku do pracowników zatrudnionych po 31 grudnia 1998 r. a przed 1 stycznia 2019 r., za których pracodawca złoży raporty informacyjne do Zakładu Ubezpieczeń Społecznych – okres przechowywania dokumentacji pracowniczej wynosi 10 lat.) W stosunku do pracowników zatrudnionych po 31 grudnia 2018 r., - okres przechowywania dokumentacji pracowniczej wynosi 10 lat.
Nazwa systemu informatycznego (Oprogramowania) służącego do przetwarzania danych osobowych	Nazwa systemu do obsługi kadrowej
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,	/a/ Dokumentacja przechowywana w wyznaczonym miejscu. /b/ Pomieszczenie zamykane jest na klucz. /c/ Dokumenty przechowywane w szafkach zamykanych na klucz.

o których mowa w art. 32 ust. 1 RODO	/d/ Dostęp do kluczy mają tylko upoważnione osoby. /e/ Pomieszczenie objęte alarmem przeciwwłamaniowym. /f/ Szyfrowanie transmisji. /g/ Szyfrowanie danych składowany na nośnikach danych. /h/ Indywidualne konta dostępne do systemów informatycznych. /i/ Zabezpieczanie kont użytkowników hasłami. /j/ Automatyczne blokowanie stacji roboczych po upływie 2 minut.
--	---

Nazwa czynności przetwarzania	OBSŁUGA UMÓW CYWILNOPRAWNYCH - zawartych w obszarze medycyny
Cele przetwarzania	Realizacja umów cywilnoprawnych dotyczących zadań z zakresu świadczenia usług medycznych.
Opis kategorii osób, których dane dotyczą,	) Kontrahenci) Zleceniobiorcy) Wykonawcy
Opis kategorii danych osobowych, przetwarzanych w ramach czynności	) dane identyfikacyjne) dane firmowe) dane kontaktowe) dane o wykształceniu i przebieg dotychczasowego zatrudnienia) dane o kwalifikacjach zawodowych) dane o warunkach umownych) dane o stanie zdrowia) dane inne przekazane - gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z umowy/przepisu prawa > imię (imiona) i nazwisko > dane kontaktowe wskazane > wykształcenie > kwalifikacje zawodowe > przebieg dotychczasowego zatrudnienia – gdy jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku > dane o stanie zdrowia > wizerunek / zdjęcie > adres zameldowania / adres zamieszkania / adres korespondencyjny > numer PESEL (a w przypadku jego braku – rodzaj i numer dokumentu potwierdzającego tożsamość) > numer rachunku płatniczego > numer NIP

	> numer REGON > dane o zajęciach komorniczych
Źródło danych	) Kontrahenci) Zleceniobiorcy) Wykonawcy
Podstawa prawna przetwarzania stanowiąca uzasadnienie dla zgodnego z prawem wykonywania czynności przetwarzania	) Rozporządzenie RODO • art. 6 ust. 1 lit. a) RODO - osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych. • art. 6 ust. 1 lit. b) RODO - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy, • art. 6 ust. 1 lit. c) RODO - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. • art. 6 ust. 1 lit. f) RODO - przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę третią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem. • art. 6 ust. 1 lit. c) w związku z art. 9 ust. 2 lit b) RODO - przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą. • art. 6 ust. 1 lit. a) w związku z art. 9 ust. 2 lit

	a) RODO - osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych.) Ustawa Kodeks Cywilny z dnia 23 kwietnia 1964 r.) Ustawy z dnia 13 maja 2016r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym.) Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty) Ustawa z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej
Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych	Poczta Kurier Zewnętrzna kancelaria prawna <u>Nazwa:</u> <u>Adres siedziby:</u> Przedsiębiorstwo ubezpieczeniowe ZUS/KRUS NFZ GUS Związek Zawodowy <u>Nazwa:</u> <u>Adres siedziby:</u> Kasa Zapomogowo Pożyczkowa Pracownicze branżowe struktury zawodowe <u>Nazwa:</u> <u>Adres siedziby:</u>

Podmiot przetwarzający	) Zewnętrzny podmiot kadrowy <u>Nazwa:</u> <u>Adres siedziby:</u> ) Zewnętrzny podmiot płacowy <u>Nazwa:</u> <u>Adres siedziby:</u> ) Zewnętrzny podmiot bhp. p.poż <u>Nazwa:</u> <u>Adres siedziby:</u> ) Zewnętrzny podmiot usług IT <u>Nazwa:</u> <u>Adres siedziby:</u> ) Zewnętrzny hostingodawca <u>Nazwa:</u> <u>Adres siedziby:</u>
Nazwa państwa trzeciego lub organizacji międzynarodowej, którym przekazywane są dane osobowe, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń	Nie dotyczy

Planowane terminy usunięcia poszczególnych kategorii danych	) Przez okres realizacji umowy oraz przez okres niezbędny w celach archiwizacyjnych, kontrolnych i rozliczeniowych tj. przez okres 5 lat, a także przez okres dochodzenia ewentualnych roszczeń i odszkodowań i obrony przed roszczeniami) Zgodnie z Ustawą z dnia 29 sierpnia 1997 r. ordynacja podatkowa) Zgodnie z Ustawą Kodeks Cywilny z dnia 23 kwietnia 1964 r.
Nazwa systemu informatycznego (Oprogramowania) służącego do przetwarzania danych osobowych	Nazwa systemu do obsługi kadrowo / płacowej
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO	/a/ Dokumentacja przechowywana w wyznaczonym miejscu. /b/ Pomieszczenie zamykane jest na klucz. /c/ Dokumenty przechowywane w szafkach zamykanych na klucz. /d/ Dostęp do kluczy mają tylko upoważnione osoby. /e/ Pomieszczenie objęte alarmem przeciwwłamaniowym. /f/ Szyfrowanie transmisji. /g/ Szyfrowanie danych składowany na nośnikach danych. /h/ Indywidualne konta dostępowe do systemów informatycznych. /i/ Zabezpieczanie kont użytkowników hasłami. /j/ Automatyczne blokowanie stacji roboczych po upływie 2 minut.

Nazwa czynności przetwarzania	OBSŁUGA PACJENTÓW - rejestracja
Cele przetwarzania	Podjęcie działań umożliwiających zarejestrowanie Pacjenta do Jednostki.
Opis kategorii osób, których dane dotyczą,	) Pacjent) Osoba upoważniona) Przedstawiciel ustawowy) Opiekun faktyczny) Opiekun prawny
Opis kategorii danych osobowych, przetwarzanych w ramach czynności	) dane <u>identyfikacyjne</u> pacjenta / przedstawiciela ustawowego / osoby upoważnionej / opiekuna prawnego) dane <u>kontaktowe</u> pacjenta / przedstawiciela ustawowego / osoby upoważnionej / opiekuna prawnego) dane o miejscu <u>zamieszkania</u> pacjenta / przedstawiciela ustawowego / osoby upoważnionej / opiekuna prawnego) dane o stanie zdrowia pacjenta) dane o udzielonych świadczeniach zdrowotnych > nazwisko i imię (imiona) pacjenta > datę urodzenia pacjenta > oznaczenie płci pacjenta > adres miejsca zamieszkania pacjenta > numer PESEL pacjenta, jeżeli został nadany, > w przypadku noworodka – numer PESEL matki, > w przypadku osób, które nie mają nadanego numeru PESEL – rodzaj i numer dokumentu potwierdzającego tożsamość, > w przypadku gdy pacjentem jest osoba małoletnia, całkowicie ubezwłasnowolniona lub niezdolna do świadomego wyrażenia zgody – nazwisko i imię (imiona) przedstawiciela ustawowego oraz adres jego miejsca

	zamieszkania; > nazwisko i imię osoby upoważnionej do uzyskiwania informacji o stanie zdrowia pacjenta i udzielonych świadczeniach zdrowotnych, > nazwisko i imię osoby upoważnionej do dokumentacji medycznej pacjenta > dane umożliwiające kontakt z osobą upoważnioną do dokumentacji medycznej > dane umożliwiające identyfikację osoby upoważnionej do dokumentacji medycznej > dane umożliwiające kontakt z osobą upoważnioną do uzyskiwania informacji o stanie zdrowia i udzielonych świadczeniach zdrowotnych > dane umożliwiające identyfikację osoby upoważnionej do uzyskiwania informacji o stanie zdrowia i udzielonych świadczeniach zdrowotnych > oznaczenie podmiotu udzielającego świadczeń zdrowotnych ze wskazaniem komórki organizacyjnej, w której udzielono świadczeń zdrowotnych; > opis stanu zdrowia pacjenta lub udzielonych mu świadczeń zdrowotnych; > datę sporządzenia dokumentacji > numer telefonu pacjenta / przedstawiciela ustawowego pacjenta / osoby upoważnionej / opiekuna prawnego > adres email pacjenta / przedstawiciela ustawowego pacjenta / osoby upoważnionej / opiekuna prawnego > adres zamieszkania pacjenta / przedstawiciela ustawowego pacjenta / osoby upoważnionej . opiekuna prawnego > numer karty ubezpieczenia zdrowotnego albo numer poświadczenia potwierdzającego prawo do świadczeń opieki zdrowotnej
--	---

	> kod oddziału wojewódzkiego Narodowego Funduszu Zdrowia
Źródło danych	) Pacjent) Osoba upoważniona) Przedstawiciel ustawowy) Opiekun faktyczny) Opiekun prawny
Podstawa prawna przetwarzania stanowiąca uzasadnienie dla zgodnego z prawem wykonywania czynności przetwarzania	) Rozporządzenie RODO • art. 6 ust. 1 lit. c) RODO - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. • art. 6 ust. 1 lit c) w związku z art. 9 ust. 2 lit h) - przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia) Ustawa z dnia 6 listopada 2008r. o prawach pacjenta i rzeczniku Praw Pacjenta) Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia) Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej.) Ustawa z dnia 27 października 2017 r. o podstawowej opiece zdrowotnej) Ustawa z 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa lub innych właściwych przepisów z zakresu prawa ubezpieczeń społecznych) Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych

	ze środków publicznych.
Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych	) Podmioty uprawnione na podstawie Ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta) Podmioty uprawnione na podstawie właściwych odrębnych od Ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta przepisów prawa > Sanepid > NFZ
Podmiot przetwarzający	) Zewnętrzny podmiot usług IT <u>Nazwa:</u> <u>Adres siedziby:</u>
Nazwa państwa trzeciego lub organizacji międzynarodowej, którym przekazywane są dane osobowe, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń	Nie dotyczy
Planowane terminy usunięcia poszczególnych kategorii danych	) 20 lat co do zasady - chyba że przepis Ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta stanowi inaczej.
Nazwa systemu	Nazwa systemu do prowadzenia dokumentacji

informatycznego (Oprogramowania) służącego do przetwarzania danych osobowych	medycznej
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO	/a/ Dokumentacja przechowywana w wyznaczonym miejscu. /b/ Pomieszczenie zamykane jest na klucz. /c/ Dokumenty przechowywane w szafkach zamykanych na klucz. /d/ Dostęp do kluczy mają tylko upoważnione osoby. /e/ Pomieszczenie objęte alarmem przeciwwłamaniowym. /f/ Szyfrowanie transmisji. /g/ Szyfrowanie danych składowany na nośnikach danych. /h/ Indywidualne konta dostępowe do systemów informatycznych. /i/ Zabezpieczanie kont użytkowników hasłami. /j/ Automatyczne blokowanie stacji roboczych po upływie 2 minut.

Tak, jak wspominamy na wstępie, zaprezentowany wzór nie ma charakteru ostatecznego. Jest konkretną, ale jednak tylko propozycją. Podobnie, jak jest nią zaproponowana metodyka prezentowania informacji.

Forma dokumentu

RCPD zawiera kolejne cechy, charakteryzujące kolejne czynności przetwarzania danych osobowych. Rejestr można wyobrazić sobie jako książkę, skoroszyt. Na okładce umieszcza się dane administratora danych i dane inspektora ochrony danych. Każda kolejna strona książki poświęcona jest innej czynności przetwarzania danych.

Na górze strony wypisujemy czynność, po czym niżej odnotowujemy kolejne, wskazane w przepisie informacje, które charakteryzują odnotowaną czynność. Do książki załącza się opis technicznych i organizacyjnych środków bezpieczeństwa. Tak sporządzony rejestr wydaje się najwłaściwszy. Jeżeli rejestr jest prowadzony na papierze, to należy pamiętać, że art. 30 ust. 3 RODO stanowi, że rejestry (również ten prowadzony przez podmiot przetwarzający) mają mieć formę pisemną. W związku z tym rejestr należy podpisywać podpisem odręcznym. Rejestr podlega aktualizacji, najlepiej zatem podpisywać podpisem odręcznym każdą stronę rejestru i każdą nową stronę rejestru, dodawaną wskutek każdej aktualizacji. Najlepiej, z uwagi na zasadę rozliczalności, datować każdą stronę rejestru i każdą nową stronę rejestru i podpisywać je. Rejestr można również prowadzić w formie dokumentu elektronicznego. W takim wypadku należy opatrywać wpisy kwalifikowanym podpisem elektronicznym.⁶⁸

Dla realizacji zasady rozliczalności dobrze jest opatrzyć każdy wpis w RCPD datą jego sporządzenia.⁶⁹ Należy pamiętać, że RCPD, ma charakter rejestru aktualizowanego. Aktualizacje nie będą może

⁶⁸ Inną możliwość widzą P. Litwiński, P. Barta, M. Kawecki. Autorzy ci uważają, że sporządzenie RCPD nie jest czynnością prawną, tylko czynnością materialno-techniczną i że jako taką „Oznaczałoby to konieczność prowadzenia rejestru w formie pisemnej – oznaczającej sporządzenie dokumentu w takiej formie (utrwalonej na papierze), jak również (i jednocześnie) sporządzenie jego wersji elektronicznej – utrwalonej na innym trwałym nośniku w postaci elektronicznej.” P. Litwiński, P. Barta, M. Kawecki. w: P. Litwiński (red.) P. Barta, M. Kawecki. *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz.* Warszawa 2018. s. 497. Nie znajdują uzasadnienia dla zaprezentowanego poglądu P. Litwińskiego, P. Barty i M. Kaweckiego, jednak nie widzę powodu by udawać, że pogląd ten nie istnieje. Cytowani autorzy prezentują go zresztą jako jeden z dwóch poglądów, drugi, na tej samej stronie ich Komentarza jest zbliżony do poglądu, który prezentuję w wywodzie głównym.

⁶⁹ Podobnie: G. Sibiga, K. Syska, *Ogólne rozporządzenie o ochronie danych.* Warszawa 2017. s. 374 i s. 377.

częste, ale jeżeli pojawi się nowa czynność przetwarzania, nowy cel przetwarzania, nowa kategoria odbiorców, to RCPD należy zaktualizować. Skoro ADO jest zgodnie z art. 5 ust. 2 RODO odpowiedzialny za realizację przepisów (przepis stanowi o zasadach, ale te realizuje się właśnie, choć nie tylko, przez przepisy), to dobrze by z RCPD wynikało, kiedy dokładnie ADO art. 30 ust 1 RODO zrealizował.”⁷⁰

Możliwe błędy w RCPD

Błędem jest brak RCPD w PWDL.

Błędem jest zakładanie, że na przykład regulamin organizacyjny podmiotu może zastąpić RCPD.

Błędem jest brak podpisu pod RCPD.⁷¹

⁷⁰ J. Rzymowski *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*. Kraków 2019. s. 44-45.

⁷¹ Podobnie ale szerzej: J. Rzymowski *Op. cit.* Kraków 2019. s. 55-56.

Realizacja artykułu 13 RODO

Źródło obowiązku

Obowiązek udostępnienia informacji o szczegółach przetwarzania danych osobowych wynika z art. 13 RODO.

Z art. 13 ust. 1 RODO i z art. 13 ust. 2 RODO wynika obowiązek informowania o wymienionych w przepisie szczegółach przetwarzania danych podczas pozyskiwania tych danych od osoby, której one dotyczą.

Treść dokumentu

Treść dokumentu wynika wprost z art. 13 ust. 1 RODO w zw. z art. 13 ust. 2 RODO.

Należy zwrócić baczną uwagę na fakt, że całość obowiązku wynika nie tylko z art. 13 ust. 1 RODO ale, że równie istotny, przynajmniej co do zakresu udostępnianych informacji, jest art. 13 ust. 2 RODO.”⁷²

Administrator zobowiązany do realizacji obowiązku informacyjnego na gruncie przepisów RODO powinien nie tylko przygotować dokumentację, za pomocą której obowiązek informacyjny będzie realizował, ale także powinien określić przyjęte sposoby jego realizacji. Poniżej prezentujemy wzór klauzuli informacyjnej, za pomocą, której administrator realizuje swój obowiązek informacyjny. Przygotowaliśmy także dokument pozwalający na szybkie i sprawne określanie sposobów wykonania obowiązku informacyjnego z wykorzystaniem klauzul informacyjnych. Dokument taki stanowić może także element rozliczalności tego obowiązku przez administratora.

Realizując obowiązek informacyjny zwrócić należy uwagę na jego adresatów. Wiele jednostek pozostaje w przekonaniu, iż obowiązek informacyjny zobowiązane są wykonać tylko względem swoich pacjentów. Jest to błędne przeświadczenie. Jednostki medyczne bowiem pozyskują i przetwarzają dane osobowe nie tylko te dotyczące pacjentów. Jednostki przetwarzają także dane nie związane z udzielaniem świadczeń zdrowotnych. Oznacza to, iż przygotowując się do prawidłowej realizacji opisywanego obowiązku należy w sposób wyczerpujący rozpoznać mechanizmy pozyskiwania danych osobowych we wszystkich płaszczyznach funkcjonowania jednostki. Analiza taka

⁷² J. Rzymowski. *Op. cit.* s. 123.

pozwoli na opracowanie wykazu klauzul informacyjnych, jakie należy przygotować, w związku z pozyskiwaniem i przetwarzaniem przez administratora danych osobowych. Pomocnym w tym procesie jest przygotowany już wcześniej Rejestr Czynności Przetwarzania Danych. Jego bowiem lektura pokazuje nam nie tylko, kogo dane są przetwarzane, ale także odpowiada nam na pytanie, w jakim celu, jakimi kanałami i na jakiej podstawie są one pozyskiwane. Wszystkie te informacje będą nam niezbędne w procesie opracowania klauzul informacyjnych.

Wydaje się, iż każdy podmiot medyczny pozyskiwał będzie dane w celu udzielania świadczeń zdrowotnych. Uzasadnia więc to przygotowanie klauzuli informacyjnej dla pacjentów.

Za słuszne założenie również przyjąć należy, iż każdy podmiot medyczny prowadził będzie politykę kadrową, płacową, co oznacza, iż będzie pozyskiwał i przetwarzał dane od kandydatów do pracy, jak również pracowników, czy też zleceniobiorców i wykonawców.

Każdy podmiot także pozyskiwał będzie dane w związku z prowadzoną obsługą kancelaryjną, czy też funkcjonowaniem w obrocie gospodarczym wspólnie ze swoimi kontrahentami.

Rozważyć jednak należy, czy w odniesieniu do konkretnego przypadku nie będziemy mieli do czynienia z pozyskiwaniem danych np. wolontariuszy, praktykantów, osób uprawnionych do świadczeń z Zakładowego Funduszu Świadczeń Socjalnych bądź Kas Zapomogowo Pożyczkowych, osób korzystających z formularzy kontaktowych na stronach internetowych, osób przeglądających strony internetowe www / BIP – co w pewnych aspektach może decydować o konieczności realizacji względem nich obowiązku informacyjnego, a nawet obowiązku odebrania adekwatnych zgód na przetwarzanie ich danych.

Ponadto zaznaczyć należy, iż w zależności od przyjętych przez jednostkę zasad funkcjonowania, kształt klauzuli informacyjnej dotyczącej nawet tej samej grupy podmiotów danych może wyglądać odmiennie. W szczególności widoczne będzie to przy dokonywaniu opisu schematu przekazywania pozyskiwanych danych osobowych, wymiany danych, ich udostępniania, czy zlecenia ich przetwarzania podmiotom przetwarzającym. Opisanie dokładnego schematu przepływu danych wydaje się być koniecznością. Z analizy wynikać może, iż jeden administrator danych osobowych, obsługuje tę samą czynność przetwarzania danych, zmierzając do osiągnięcia tego samego celu przetwarzania, samodzielnie, a drugi z wykorzystaniem innych kate-

gorii podmiotów kooperujących. Dokumentem nie do przecenienia w tym zakresie jest Rejestr Czynności Przetwarzania Danych.

Reasumując, za punkt wyjścia przyjąć należy rozpoznanie zasadności formułowania odrębnych klauzul informacyjnych, uwzględniając cel i kategorie podmiotów danych których dane są przetwarzane.

W drugiej kolejności należy przygotować wnikliwą analizę jednostki pod względem jej otoczenia, kładąc nacisk na podmioty z nią kooperujące, którym dane są udostępnianie, bądź względem których doszło do zlecenia im przetwarzania danych w imieniu administratora.

Poniżej przedstawiamy wzór klauzuli informacyjnej, za pośrednictwem której podmiot realizuje swój obowiązek informacyjny względem swoich pacjentów. Naturalnie jest to wzór przygotowany w oparciu o konkretny stan faktyczny, co oznacza, jak piszemy powyżej, iż wymaga on dokonania stosownych modyfikacji, do stanu faktycznego, jaki obowiązuje w innych jednostkach – jeśli miałby zostać zastosowany w praktyce.

OBOWIĄZEK INFORMACYJNY RODO PACJENT PODMIOTU WYKONUJĄCEGO DZIAŁALNOŚĆ LECZNICZĄ

Zgodnie z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) (dalej „RODO”) informuje się co następuje

Dane Administratora Danych Osobowych [dalej ADO]	Nazwa ADO: ul.-..... e-mail: tel.:
Dane kontaktowe Inspektora Ochrony Danych [dalej IOD]	Imię i nazwisko Inspektora Ochrony Danych: Adres korespondencyjny IOD: ul.-..... e-mail: tel.: Z IOD można się kontaktować w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych.
Źródło danych osobowych. Skąd pozyskiwane są dane osobowe.	Co do zasady Pani/Pana dane osobowe pozyskiwane są bezpośrednio od Pani/Pana . W przypadku kontynuacji leczenia rozpoczętego w innym podmiocie medycznym, dane mogą być nam udostępnione przez inny podmiot medyczny . W przypadku usług medycyny pracy dane są nam udostępnione przez pracodawcę kierującego Panią/Pana . W szczególnych sytuacjach uzasadnionych Pani/Pana stanem zdrowia dane osobowe mogą być uzyskiwane od osób bliskich .
Zakres przetwarzanych danych osobowych.	Na potrzeby udzielania świadczeń zdrowotnych przetwarzane są wyłącznie niezbędne do tego celu dane obejmujące w szczególności następujące kategorie danych: Dane identyfikacyjne / pacjenta / przedstawiciela ustawowego pacjenta / osób upoważnionych do dokumentacji medycznej / osób upoważnionych do informacji o stanie zdrowia i udzielonych świadczeniach zdrowotnych / osoby opiekuna faktyczne-

	go pacjenta / osoby opiekuna prawnego pacjenta np.: imię (imiona) nazwisko, numer PESEL, jeżeli został nadany, w przypadku noworodka – numer PESEL matki, w przypadku osób, które nie mają nadanego numeru PESEL – rodzaj i numer dokumentu potwierdzającego tożsamość. Dane kontaktowe / pacjenta / przedstawiciela ustawowego pacjenta / osób upoważnionych do dokumentacji medycznej / osób upoważnionych do informacji o stanie zdrowia i udzielonych świadczeniach zdrowotnych <u>np.:</u> numer telefonu kontaktowego, adres e-mail. Dane dotyczące miejsca zamieszkania / zameldowania / pobytu w kraju / pacjenta przedstawiciela ustawowego pacjenta / osób upoważnionych do dokumentacji medycznej / osób upoważnionych do informacji o stanie zdrowia i udzielonych świadczeniach zdrowotnych/ osoby opiekuna prawnego <u>np.:</u> adres miejsca zamieszkania, zameldowania, pobytu. Dane o stanie zdrowia / pacjenta / członków rodziny pacjenta <u>np.:</u> informacje o stanie zdrowia, o udzielonych świadczeniach zdrowotnych.
--	--

Okres przechowywania danych.	ADO zobowiązany jest do prowadzenia, przechowywania, udostępniania i zabezpieczania dokumentacji medycznej, której treść i zakres określają obowiązujące przepisy prawa. Ustawy z dnia 06 listopada 2008 r. o Prawach Pacjenta i Rzeczniku Praw Pacjenta Co do zasady dokumentacja medyczna jest przechowywana, przez okres <u>20 lat</u> - licząc od końca roku kalendarzowego, w którym dokonano ostatniego w niej wpisu, za wyjątkiem: • dokumentacji medycznej w przypadku zgonu pacjenta na skutek uszkodzenia ciała lub zatrucia, która jest przechowywana przez okres <u>30 lat</u> - licząc od końca roku kalendarzowego, w którym nastąpił zgon; • dokumentacji medycznej zawierającej dane niezbędne do monitorowania losów krwi i jej składników, która jest przechowywana przez okres 30 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu; • zdjęć rentgenowskich przechowywanych poza dokumentacją medyczną pacjenta, które są przechowywane przez okres <u>10 lat</u> -, licząc od końca roku kalendarzowego, w którym wykonano zdjęcie; • skierowań na badania lub zleceń lekarza, które są
-------------------------------------	---

	przechowywane przez okres: <u>5 lat</u> - licząc od końca roku kalendarzowego, w którym udzielono świadczenia zdrowotnego będącego przedmiotem skierowania lub zlecenia lekarza, <u>2 lata</u> - licząc od końca roku kalendarzowego, w którym wystawiono skierowanie – w przypadku gdy świadczenie zdrowotne nie zostało udzielone z powodu niezgłoszenia się pacjenta w ustalonym terminie, chyba że pacjent odebrał skierowanie; • dokumentacji medycznej dotyczącej dzieci do ukończenia 2. roku życia, która jest przechowywana przez okres <u>22 lat</u>. Po upływie ustawowego czasu przechowywania dokumentacji medycznej będzie niszczone w sposób uniemożliwiający identyfikację Pacjenta, którego dotyczyła. Dokumentacja medyczna przeznaczona do zniszczenia może być wydana pacjentowi, jego przedstawicielowi ustawowemu lub osobie upoważnionej przez pacjenta. Jeżeli wyraził/a Pan/Pani na komunikację w celach marketingowych, dane będą przetwarzane <u>do momentu wycofania przez Panią/Pana zgody</u> na przetwarzanie danych osobowych w tych celach, lub do czasu kiedy ustanie cel takiego przetwarzania.	
Cel przetwarzania oraz podstawa prawna przetwarzania.	Przetwarzanie Pani/Pana danych osobowych jest niezbędne do celów udzielania świadczeń zdrowotnych w tym: • ustalenia, potwierdzenia Pani/Pana tożsamości przed udzieleniem świadczeń zdrowotnych: (podczas rejestracji, w gabinetach lekarskich), • diagnozy medycznej i leczenia, w tym prowadzenia dokumentacji medycznej, • zapewnienia opieki zdrowotnej oraz zarządzania udzielaniem świadczeń zdrowotnych, w tym rozpatrywania skarg i	Rozporządzenie RODO: • art. 6 ust. 1 lit. c) RODO • art. 6 ust. 1 lit. c) w związku z art. 9 ust. 2 lit h) RODO W związku z przepisami: • Ustawy z dnia 06 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta • Ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty • Ustawy z dnia 5 lipca 1996 r. o zawodach pielęgniarki i położnej • Ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia • Ustawy z dnia 29 czerwca

	wniosków, • podejmowania działań w zakresie profilaktyki zdrowotnej, w tym informowania o możliwości skorzystania ze świadczeń zdrowotnych lub przekazywania zaproszeń na badania, • zapewnienia zabezpieczenia społecznego, w tym wystawiania zaświadczeń lekarskich i zwolnień, • realizacji obowiązków prawem określonych w zakresie rejestracji i archiwizacji nagrań z rozmów telefonicznych w związku z udzielaniem przez jednostkę świadczeń zdrowotnych w ramach nocnej i świątecznej opieki zdrowotnej.	1995 r. o statystyce publicznej • Ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych • Ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej
	Pani/Pana dane mogą być także przetwarzane w celach archiwalnych, naukowych lub statystycznych	Rozporządzenie RODO: – art. 6 ust. 1 lit. c) – art. 6 ust. 1 lit. c) w związku z art. 9 ust. 2 lit j) – art. 6 ust. 1 lit. c) w związku z art. 9 ust. 2 lit f)
	Pani/Pana dane mogą być także przetwarzane na potrzeby prowadzenia ksiąg rachunkowych oraz rozliczeń podatkowych.	Rozporządzenie RODO: – art. 6 ust. 1 lit. c) W związku z przepisami: – Ustawy z dnia 29 września 1994 r. o rachunkowości.
	Pani/Pana dane mogą być również przetwarzane w celu obrony praw i dochodzenia roszczeń przez ADO w związku z prowadzoną przez niego działalnością.	Rozporządzenie RODO: – art. 6 ust. 1 lit. f)

	Jeśli wyraziła/ł Pani/Pan zgodę na komunikację marketingową, Pani/Pana dane mogą być wykorzystywane dla celów marketingowych.	Rozporządzenie RODO: – art. 6 ust. 1 lit. a) W związku z przepisami: Ustawy z dnia 16 lipca 2004 r., Prawo telekomunikacyjne. Ustawy z dnia 18 lipca 2002 r, o świadczeniu usług drogą elektroniczną.
Odbiorcy danych. Udostępnianie danych. Powierzenie przetwarzania danych.	Odbiorcy danych: Odbiorca jest oznaczona osoba fizyczna lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania. Kategorie odbiorców: poczta, kurier, kancelaria prawna, służby sanitarne Odbiorcy zdefiniowani: <u>Nazwa:</u> <u>Adres siedziby:</u> Podmioty, którym dane są udostępniane: Dokumentacja medyczna udostępniania jest tylko i wyłącznie zgodnie z przepisami prawa. Dokumentacja medyczna udostępniana jest także osobom wykonującym zawód medyczny zatrudnionym u ADO lub z nim współpracującym, podmiotom udzielającym świadczeń zdrowotnych do zapewnienia ciągłości świadczeń zdrowotnych oraz organom władzy publicznej, w tym Rzecznikowi Praw Pacjenta, Narodowemu Funduszowi Zdrowia, organom samorządu zawodów medycznych oraz konsultantom krajowym i wojewódzkim, w zakresie niezbędnym do wykonywania przez te podmioty ich zadań, w szczególności nadzoru i kontroli. Zlecenie przetwarzania danych osobowych: Pani/Pana dane osobowe mogą być przekazywane podmiotom przetwarzającym dane osobowe na zlecenie ADO osobowych	

	wykonującym czynności pomocnicze przy udzielaniu świadczeń zdrowotnych a także wykonującym czynności związane z utrzymaniem systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna, i zapewnieniem bezpieczeństwa tego systemu, jak również. dostawcom usług IT, technicznych, czy organizacyjnych które umożliwiają udzielanie świadczeń zdrowotnych - przy czym takie podmioty przetwarzają dane na podstawie stosownej Umowy powierzenia przetwarzania z ADO i wyłącznie zgodnie z jego poleceniami. Kategorie odbiorców: serwis IT, serwis sprzętu medycznego, Odbiorcy zdefiniowani: <u>Nazwa:</u> <u>Adres siedziby:</u>
--	--

Informacja o przekazywaniu danych do państw trzecich.	Pani/ Pana dane osobowe nie będą przekazywane do podmiotów zlokalizowanych poza Europejskim Obszarem Gospodarczym.
Prawa osoby której dane dotyczą.	Przysługuje Panu/Pani prawo: – Dostępu do Pani/Pana danych osobowych - uzyskania od ADO potwierdzenia, czy przetwarzane są Pani/Pana dane osobowe, a jeżeli ma to miejsce, uzyskania dostępu do nich oraz przekazania Pani/Panu informacji w zakresie wskazanym w art. 15 RODO, – Sprostowania Pani/Pana danych osobowych - żądania od ADO niezwłocznego sprostowania danych osobowych, które są nieprawidłowe, uzupełnienia niekompletnych danych osobowych, – Usunięcia Pana/Pani danych osobowych - żądania od ADO niezwłocznego usunięcia danych osobowych, <u>jeżeli spełniona została jedna z przesłanek określonych w art. 17 RODO</u>, m.in. dane osobowe nie są już niezbędne do celów, w których zostały zebrane. <u>Prawo do usunięcia danych może zostać ograniczone ze względu na obowiązki ADO związane z prowadzeniem dokumentacji medycznej art. 17 ust. 3 lit b) RODO</u> – Ograniczenia przetwarzania Pana/Pani danych osobowych w przypadkach wskazanych w art. 18 RODO - m.in.

	kwestionowania prawidłowość danych osobowych. <u>Prawo do ograniczenia przetwarzania danych może zostać ograniczone ze względu na obowiązki ADO związane z prowadzeniem dokumentacji medycznej.</u> – Przenoszenia danych osobowych – otrzymania od ADO Pani/Pana danych osobowych, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, <u>jeżeli Pani/Pana dane są przetwarzane na podstawie zgody oraz przetwarzanie odbywa się w sposób zautomatyzowany.</u> Może Pani/Pan przesłać te dane innemu administratorowi danych osobowych lub żądać, by zostały przesłane przez ADO, o ile jest to technicznie możliwe. – Wniesienia sprzeciwu wobec przetwarzania danych osobowych w przypadkach określonych w art. 21 RODO. – Wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych. W celu skorzystania z powyższych praw należy skontaktować się z ADO. Dane kontaktowe wskazane są wyżej.
Informacja o dobrowolności podania danych osobowych.	Podanie danych osobowych jest warunkiem niezbędnym do udzielenia świadczeń zdrowotnych ze względu na wymogi prawne nałożone na ADO, w tym m.in. konieczność prowadzenia, przechowywania, zabezpieczania i udostępniania dokumentacji medycznej. Odmowa podania danych może być podstawą do odmowy udzielenia świadczenia zdrowotnego. Podanie danych jest również niezbędne do wystawienia rachunku lub faktury. Podanie danych osobowych w celach marketingowych jest całkowicie dobrowolne, brak zgody na komunikację marketingową nie może być podstawą do odmowy udzielenia świadczenia zdrowotnego.
Informacje o zautomatyzowanym podejmowaniu decyzji.	Pani/Pana dane nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym o profilowaniu.

OBOWIĄZEK INFORMACYJNY RODO - PRACOWNIK Zgodnie z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) (dalej „RODO”) informuje się co następuje	
Dane Administratora Danych Osobowych [dalej ADO]	Nazwa ADO: ul. Kod pocztowy-..... Miejscowość:..... e-mail: tel.:
Dane kontaktowe Inspektora Ochrony Danych [dalej IOD]	Imię i nazwisko Inspektora Ochrony Danych: Adres korespondencyjny IOD: ul. Kod pocztowy-..... Miejscowość:..... e-mail: tel.: Z IOD można się kontaktować w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych.
Cel przetwarzania danych osobowych	Pana/Pani dane osobowe przetwarzane będą w celu: • zawarcia / wykonania umowy o pracę, • dochodzenia i obrony przed ewentualnymi roszczeniami.
Podstawa prawna przetwarzania	Podstawą prawną przetwarzania Pani/Pana danych osobowych jest: • art. 6 ust. 1 lit. b) RODO - przetwarzanie jest niezbędne do wykonania umowy, której jest Pani/Pan stroną, lub do podjęcia działań na Państwa żądanie przed zawarciem umowy, • art. 6 ust. 1 lit. c) RODO - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze • art. 6 ust. 1 lit. a) RODO – przetwarzanie dokonywane jest na podstawie zgody, • art. 6 ust. 1 lit. f) RODO - przetwarzanie jest niezbędne do

	celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO, • art. 6 ust. 1 lit c) w związku z art. 9 ust. 2 lit b) RODO - przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, Podstawą prawną przetwarzania Pani/Pana danych są przepisy ustaw i wydanych na ich podstawie aktów wykonawczych w szczególności: • Ustawa z 26 czerwca 1974 r. Kodeks Pracy • Ustawa z 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych • Ustawa z 26 lipca 1991 r. o podatku dochodowym od osób fizycznych • Ustawa z 10 października 2002 r. o minimalnym wynagrodzeniu za pracę • Ustawa z dnia 8 czerwca 2017 r. o sposobie ustalania najniższego wynagrodzenia zasadniczego pracowników wykonujących zawody medyczne zatrudnionych w podmiotach leczniczych
Informacja o dobrowolności podania danych osobowych.	Podanie danych związanych z zatrudnieniem jest obowiązkowe a ich zakres wynika z przepisów prawa, w szczególności z Ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy. Brak ich podania skutkuje brakiem możliwości nawiązania stosunku pracy. Nie dotyczy to sytuacji, w których podanie danych ma charakter dobrowolny, z konsekwencją tego, iż ich nie podanie skutkować może brakiem możliwości skorzystania z uprawnienia przez pracownika.
Odbiorcy danych. Udostępnianie danych. Powierzenie przetwarzania danych.	Pani/Pana dane osobowe będą udostępniane uprawnionym na podstawie przepisów prawa podmiotom i organom publicznym w szczególności takim podmiotom jak NFZ, Ministerstwo Zdrowia, Centrum e-Zdrowie, zewnętrzna kancelaria prawna, poczta, kurier, oraz podmiotom, z którymi ADO zawarł umowy powierzenia przetwarzania danych osobowych w szczególności takim podmiotom jak: zewnętrzny podmiot usług IT, zewnętrzny hostingodawca, zewnętrzny podmiot usług kadrowo/płacowe.
Okres przechowywania danych.	ADO zobowiązany jest do prowadzenia, przechowywania i zabezpieczania dokumentacji pracowniczej, której treść i zakres określają obowiązujące przepisy prawa. Okres przetwarzania Pani/Pana danych osobowych jest uzależniony od celu w jakim

	dane są przetwarzane. Okres, przez który Pani/Pana dane osobowe będą przechowywane jest obliczany w oparciu o następujące kryteria: czasu obowiązywania umowy, przepis prawa, które mogą ADO obligować do przetwarzania danych przez określony czas, okres, który jest niezbędny do obrony interesów ADO. Pani/Pana dane przechowywane będą przez okres trwania stosunku pracy oraz okresy prawem określone, w szczególności: • 50 lat zgodnie z Ustawą z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych. • 10 lat zgodnie z Ustawą z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych. • 10 lat zgodnie z Ustawą z dnia 26 czerwca 1974 r. Kodeks pracy. • 5 lat zgodnie z Ustawą z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych. • 5 lat zgodnie z Ustawą z dnia 29 sierpnia 1997 r. Ordynacja podatkowa. • 3 lata zgodnie z Ustawą z dnia 26 czerwca 1974 r. Kodeks pracy. • 1 rok zgodnie z Ustawą z dnia 26 czerwca 1974 r. Kodeks pracy. • 6 lat – zgodnie z Ustawą z dnia 23 kwietnia 1964 r., Kodeks Cywilny.
Prawa osoby której dane dotyczą.	Ma Pani/Pan prawo do: • żądania od ADO dostępu do danych osobowych Pani/Pana dotyczących, • żądania od ADO sprostowania danych osobowych Pani/Pana dotyczących, • żądania od ADO usunięcia danych osobowych Pani/Pana dotyczących, • żądania od ADO ograniczenia przetwarzania danych osobowych Pani/Pana dotyczących, • wniesienia sprzeciwu wobec przetwarzania danych osobowych Pani/Pana dotyczących, • żądania od ADO przeniesienia danych osobowych Pani/Pana dotyczących • cofnięcia zgody w dowolnym momencie bez konsekwencji dla przetwarzania, którego dokonano przed jej cofnięciem, jeśli dane zbierane są na podstawie zgody, Zakres każdego z tych praw oraz sytuacje, z których można

	z nich skorzystać, wynikają z przepisów Rozporządzenia. Z praw tych może Pan/Pani skorzystać składając wniosek u Administratora. Ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO. Pani/Pana dane nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym o profilowaniu
--	---

Dla uświadomienia sobie jak i kiedy, a zwłaszcza kiedy należy udostępniać informacje wynikające z art. 13 ust. 1 i 2 RODO należy przypomnieć sobie treść części wprowadzającej art. 13 ust. 1 RODO. Przepis ten stanowi: „Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje”. Jak więc widać ADO ma obowiązek podawać informacje z art. 13 „podczas pozyskiwania danych osobowych”.⁷³ Prezentuję poniżej kilka typowych sytuacji zbierania danych osobowych, wraz z najprostszymi sposobami udostępniania informacji z art. 13.

„Dokumentowanie realizacji art. 13 RODO, realizacja zasady rozliczalności.

Istotą realizacji art. 13 RODO jest podawanie informacji w przepisie wskazanych. Nie ma obowiązku odbierania pokwitowań, należy jednak pamiętać o zasadzie rozliczalności. Z art. 5 ust. 2 RODO (zasada rozliczalności) w zw. z art. 5 ust. 1 lit a RODO (zasada rzetelności i zasada przejrzystości) w zw. z art. 13 RODO wynika, że ADO powinien mieć sposób wykazania, że realizuje obowiązek wynikający z art. 13 RODO. Udokumentować realizację art. 13 można na przykład na jeden z opisanych poniżej sposobów.

- odebrać pokwitowanie – niekonieczne, ale nie jest to rozwiązanie złe,
- opisać w Polityce Ochrony sposób lub sposoby realizacji obowiązku wynikającego z art. 13 RODO – rozwiązanie dobre, wymaga jednak pewnej dyscypliny, tak by rzeczywiście robiono to co w Polityce Ochrony”⁷⁴, Polityce Bezpieczeństwa lub w załączniku do któregoś z wymienionych dokumentów opisano.

Określenie sposobu realizacji obowiązku informacyjnego, dokonane może być z wykorzystaniem prezentowanego przez nas dokumentu. Informacje w nim zawarte pozwolą na dokonanie właściwego sposobu realizacji obowiązku informacyjnego. Opracowanie i stosowanie takiego dokumentu stanowić będzie wyraz realizacji zasady

⁷³ J. Rzymowski RODO – GDPR. *Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*. Kraków 2019. s. 142-143.

⁷⁴ J. Rzymowski *Op. cit.* s. 146.

rozliczalności. Zatem po ustaleniu zasadności utworzenia konkretnego zestawu klauzul informacyjnych, określić należy konkretne sposoby realizacji obowiązku informacyjnego, względem każdej z klauzul osobno, indywidualnie wykorzystując do tego zestawy tabel, jakie prezentujemy. Za właściwe a wręcz wymagane uznać należy równoległe określenie kilku metod realizacji obowiązku. Tak przygotowana procedura daje także bazę w oparciu o którą będzie możliwe przeprowadzenie wewnętrznej kontroli poprawności stosowania przepisów w omawianym zakresie w jednostce

W dokumencie wskazujemy na rekomendowane rozwiązania sygnalizując jednak, iż nie są to wszystkie możliwe sposoby realizacji obowiązku informacyjnego. Specyfika jednostki, jej warunki lokalowe, mogą podpowiadać inne alternatywne sposoby, które mogą okazać się skuteczniejsze od proponowanych przez nas. Z tego względu warto po krótko przedstawić każdy z proponowanych sposobów po to, aby następnie świadomie dokonać najwłaściwszego wyboru metody przekazywania informacji zawartych w klauzulach informacyjnych do ich adresatów.

Dokument zatytułowany „**Przyjęte i stosowane metody realizacji obowiązku informacyjnego jednostce art. 13 ust. 1 i 2 Rozporządzenia RODO**”, jaki prezentujemy poniżej, jest przykładowym zbiorczym zestawieniem klauzul informacyjnych, za pośrednictwem których administrator realizuje obowiązek informacyjny. Dokument ten należy wypełnić zgodnie z wewnątrznie dokonanymi ustaleniami nt. tego, jakie klauzule zostały przygotowane, a których opracowywanie jest zbyteczne dla podmiotu. Tabelaryczne zestawienie pozwoli na sprawne zarządzanie taką dokumentacją.

Przyjęte i stosowane metody realizacji obowiązku informacyjnego jednostce Art. 13 ust. 1 i 2 Rozporządzenia RODO	
Rodzaje stosowanych klauzul informacyjnych	Przygotowana Brak zasadności wprowadzania
Klauzula Informacyjna – Pacjent	
Klauzula Informacyjna – Kandydat do pracy	
Klauzula Informacyjna – Pracownik	
Klauzula Informacyjna – Kontrahenci	
Klauzula Informacyjna – Praktykant / Wolontariusz / Stażysta	
Klauzula Informacyjna – Media społecznościowe	
Klauzula Informacyjna – Połączenia telefoniczne	
Klauzula Informacyjna – Formularz kontaktowy WWW	
Klauzula Informacyjna – ZFŚS	
Klauzula Informacyjna – KZP	
Klauzula Informacyjna – PPK	
Klauzula Informacyjna – Szczepienia COVID-19	

Dopiero po wypełnieniu ww. tabeli przechodzimy do kolejnych zestawień, jakie już precyzyjnie określać będą, sposoby realizacji obowiązku informacyjnego które stosuje w praktyce administrator. Należy zwrócić uwagę, iż dla każdej klauzuli informacyjnej, jaka wymieniona została w dokumencie zatytułowanym „**Przyjęte i stosowane metody realizacji obowiązku informacyjnego jednostce art. 13 ust. 1 i 2 Rozporządzenia RODO**” wskazane są propozycje rozwiązań, z których administrator samodzielnie wybiera właściwą dla niego metodę realizacji obowiązku informacyjnego, a dokonany przez siebie wybór odnotowuje w zestawieniu. Takiego wyboru administrator powinien dokonać w odniesieniu do każdej klauzuli informacyjnej, jaka została przygotowana. Naturalnie sposoby zaprezentowane w zestawieniach są jedynie przykładowymi, nie zamykają one możliwości posługiwania się innymi rozwiązaniami. Poniżej prezentujemy kilka uwag natury praktycznej, które warto uwzględnić dokonując wyboru konkretnego sposobu realizacji obowiązku informacyjnego, jaki proponujemy w poniższym zestawieniu.

Klauzula Informacyjna – przekazywana adresatowi:

Rozwiązanie takie stawia jednak przed ADO wyzwanie logistyczne, którego rozmiar i ciężar realizacji uzależniony jest od wielkości jednostki, od liczby pacjentów / kontrahentów / pracowników itd. Niektóre jednak podmioty mogą zdecydować się na wykorzystanie tej formy realizacji obowiązku informacyjnego np. w odniesieniu do wybranych tylko przez siebie klauzul informacyjnych.

Klauzula Informacyjna – w dokumentacji medycznej pacjenta:

Rozwiązanie proste do zastosowania, jednak zwrócić należy uwagę na fakt postępującej cyfryzacji służby zdrowia, oraz na to, iż w rzeczywistości w ograniczonych przypadkach pacjent ma dostęp do swojej dokumentacji fizycznie, dlatego też, jeśli jednostka zdecyduje się na tego rodzaju rozwiązanie dobrze byłoby, aby treść klauzuli znalazła się np. na odwrocie druku upoważnienia udzielanego osobom trzecim, tak aby uprawdopodobnić fakt, iż pacjent miał realnie możliwość zapoznania się z klauzulą.

Klauzula Informacyjna – na stronie internetowej WWW:

Rozwiązanie proste do realizacji, skuteczne i możliwe do wykorzystania łącznie z innymi metodami realizacji obowiązku informacyjnego, ze względu na możliwość posługiwania się adresem internetowym (www) w postaci linku kierującego do dokumentu w postaci cyfrowej. Ta metoda z powodzeniem może być stosowana dla większości klauzul informacyjnych.

Klauzula Informacyjna – w systemie informatycznym jednostki:

Istnieje możliwość umieszczenia klauzuli w postaci cyfrowej we wnętrzu systemu informatycznego, którym posługuje się pacjent np. przy e-rejestracji. Rozwiązanie proste do wdrożenia warto, aby informacja umieszczona w systemie była jednak łatwo osiągalna przez jej adresata.

Klauzula Informacyjna – w postaci nagrania audio / pełna wersja / skrócona wersja:

Tego rodzaju metoda powinna być stosowana w związku z pozyskiwaniem danych przez kanał telefoniczny. W tym miejscu należy wskazać, iż zgodnie z przepisami Ustawy z dnia 06 września 2008 r. o Państwowym Ratownictwie Medycznym (Dz.U. z 2017 r., poz.

2195 ze zm.) oraz treścią Rozporządzenie Ministra Zdrowia w sprawie świadczeń gwarantowanych z zakresu podstawowej opieki zdrowotnej z dnia 24 września 2013 r. (t.j. Dz.U. z 2016 r. poz. 86 ze zm.) w stosunku do nocnej i świątecznej opieki zdrowotnej obowiązkiem jednostek jest nie tylko wykorzystywanie tego kanału np. do obsługi zgłoszeń pacjentów, ale także obowiązkiem jest nagrywanie takich rozmów telefonicznych.

Należy jednak pamiętać o wartościowaniu dóbr oraz o tym, iż podstawowym zadaniem jednostki jest realizacja świadczeń zdrowotnych, co oznacza tyle, iż zmuszanie rozmówcy pacjenta, czy nawet kontrahenta do zapoznania się z pełną wersją klauzuli informacyjnej może pozostawać w sprzeczności z jego słuszenie rozumianym interesem. Z tego względu przyjąć należy, iż właściwszym rozwiązaniem będzie posługiwanie się opcją pozwalającą na zdecydowanie o chęci wysłuchania pełnej treści. Zasygnalizować można również, iż w prawem określonych przypadkach możemy mieć także ustawowo określony sposoby realizacji obowiązku informacyjnego, jak ma to miejsce np. na gruncie zapisów Ustawy z dnia 22 listopada 2013r., o systemie powiadamiania ratunkowego⁷⁵. Praktyczną radą może być również ograniczenie polegające na tym, iż formuła klauzuli nie będzie odtwarzana przy wykonywaniu połączeń wewnętrznych pomiędzy komórkami administratora.

Klauzula Informacyjna – w postaci email / pełna wersja / skrócona wersja:

Rozwiązanie rekomendowane do zastosowania w sytuacji pozyskiwania informacji tym kanałem. Rozwiązanie może zakładać automatycznie generowaną odpowiedź do kierującego zapytanie. Ustawienie tego rodzaju konfiguracji pozwala zachować pewność, co do tego, iż metoda jest i będzie realizowana względem adresatów z wykorzystaniem tego kanału kontaktu. Można także posługiwać się odpowiednio przygotowanymi stopkami do wiadomości email, zawierającymi obowiązek informacyjny realizowany warstwowo z odesłaniem we wskazane miejsca strony internetowej poprzez hiperłącze.

⁷⁵ <https://prostetorodo.pl/2021/03/05/klauzula-rodo-i-numery-alarmowe/>
(Dostęp: 2022.02.27. godz. 17.20)

Klauzula Informacyjna – w postaci SMS / pełna wersja / skrócona wersja:

Rozwiązanie rekomendowane zwłaszcza w odniesieniu do skróconej wersji klauzuli, w sytuacji pozyskiwania danych tym kanałem.

Klauzula Informacyjna – na tablicy informacyjnej w przestrzeni ogólnodostępnej:

Rozwiązanie najbardziej oczywiste i znane jednostkom medycznym, realizującym obowiązek podawania określonych informacji do wiadomości pacjentów zgodnie z art. 24 ust. 2 Ustawy z dnia 15 kwietnia 2011 r., o działalności leczniczej (Dz. U. 2011 Nr 112 poz. 654 ze zm.) przez ich wywieszenie w widoczny sposób w miejscu udzielania świadczeń oraz na stronie internetowej podmiotu wykonującego działalność leczniczą i udostępnienie w Biuletynie Informacji Publicznej, w przypadku podmiotu obowiązującego do jego prowadzenia. Ten sam sposób przekazywania informacji z powodzeniem można wykorzystać dla realizacji obowiązku informacyjnego z wykorzystaniem klauzul informacyjnych.

Klauzula Informacyjna – w regulaminie organizacyjnym:

Z wykorzystaniem tego rozwiązania w pewnych sytuacjach wiązać mogą się trudności natury techniczno-organizacyjnej. Nie wyklucza to jednak stosowania tej metody przy wyborze jej, jako właściwej do realizacji konkretnego obowiązku informacyjnego.

Klauzula Informacyjna – na drzwiach wejściowych do jednostki:

Pomijając aspekt estetyczny proponowanego rozwiązania, zwrócić należy uwagę na walor skuteczności takiego mechanizmu wdrożonego do stosowania.

Klauzula Informacyjna – przed pomieszczeniem docelowym:

Rozwiązanie rekomendowane do wprowadzenia z uwagi na fakt, iż pozyskiwanie danych osobowych realizowane może być poza pomieszczeniami ogólnodostępnymi współwystępującymi z pomieszczeniami rejestracji. Często pacjenci, kontrahenci, przemieszczają się swobodnie po jednostce kierując się docelowo do wybranego miejsca np. działu, czy oddziału, gdzie dopiero dochodzi do przekazania danych osobowych. Powyższe uzasadnia wdrożenie takiego rozwiązania

korelując je z charakterem podmiotów danych obsługiwanych w ramach danego pomieszczenia.

Klauzula Informacyjna – na drukach wewnętrznych:

W przypadku wykorzystywania wzorów druków, jak ma to np. miejsce w odniesieniu do składania wniosków o świadczenie z Zakładowego Funduszu Świadczeń Socjalnych, można zamieścić na odwrocie papierowego formularza treść klauzuli informacyjnej.

Klauzula Informacyjna – przekazywana w chwili zawarcia umowy:

Dobłą praktyką będzie stosowanie tego rozwiązania, aczkolwiek zwrócić należy uwagę, iż pozyskanie danych mogło nastąpić wcześniej, z tego względu warto jest dostrzec taką zależność i odpowiednio innym kanałem wcześniej przekazać stosowną informację jej adresatowi.

Klauzula Informacyjna – przy listach obecności

Rozwiązanie pozwalające na sprawną i szybką komunikację jednostronną z personelem jednostki, która tego rodzaju metodę stosuje do potwierdzania obecności w pracy.

Rzeczą oczywistą jest, iż wybrane metody realizacji obowiązku informacyjnego z wykorzystaniem klauzul informacyjnych i sposobu ich publikowania są jedynie propozycjami, które należy ocenić przez pryzmat jednostki. Poniżej prezentujemy zestawienia przygotowane według schematu, w którym to do każdego rodzaju klauzuli informacyjnej zaproponowane zostały określone metody realizacji obowiązku informacyjnego i to rolę administratora teraz jest dokonanie wyboru określonej metody, metod, z uwzględnieniem realiów funkcjonowania jednostki.

Sposób realizacji obowiązku informacyjnego z wykorzystaniem klauzuli informacyjnej	
Klauzula Informacyjna – Pacjent	
	Określenie sposobu realizacji podania do wiadomości KI
KI przekazywana Pacjentowi	
KI w dokumentacji medycznej Pacjenta	
KI na stronie internetowej www	
KI w systemie informatycznym	
KI pełne nagrania	
KI skrócone nagranie audio / link	
KI automatyczna odpowiedź na email	
KI skrócona jako email / link	
KI pełna w formie SMS	
KI skrócona w formie SMS / link	
KI na tablicy w przestrzeni ogólnodostępnej	
KI w regulaminie organizacyjnym	
KI na stronie e-rejestracji	
KI drzwi wejściowe do jednostki	
KI drzwi pomieszczeń jednostki	

Sposób realizacji obowiązku informacyjnego z wykorzystaniem klauzuli informacyjnej	
Klauzula Informacyjna – Kandydat do Pracy	
	Określenie sposobu realizacji podania do wiadomości KI
KI przekazywana do Kandydata	
KI na stronie internetowej www	
KI w systemie informatycznym	
KI pełna jako email	
KI skrócona jako email / link	
KI na tablicy w przestrzeni ogólnodostępnej	
KI w pomieszczeniu właściwy merytorycznie dział	

Sposób realizacji obowiązku informacyjnego z wykorzystaniem klauzuli informacyjnej	
Klauzula Informacyjna – Pracownik	
	Określenie sposobu realizacji podania do wiadomości KI
KI przekazywana pracownikowi w chwili zawarcia umowy	
KI w aktach osobowych	
KI na stronie internetowej www	
KI w systemie informatycznym	
KI pełna jako email	
KI skrócona jako email / link	
KI pełna w formie SMS	
KI skrócona w formie SMS / link	
KI na tablicy w przestrzeni ogólnodostępnej	
KI w pomieszczeniu właściwy merytorycznie dział	
KI przy liście obecności	

Sposób realizacji obowiązku informacyjnego z wykorzystaniem klauzuli informacyjnej	
Klauzula Informacyjna – Kontrahenci	
	Określenie sposobu realizacji podania do wiadomości KI
KI przekazywana do Kontrahenta	
KI jako załącznik do umowy	
KI na stronie internetowej www	
KI w systemie informatycznym	
KI pełna jako email	
KI skrócona jako email / link	
KI pełna w formie SMS	
KI skrócona w formie SMS / link	
KI na tablicy w przestrzeni ogólnodostępnej	
KI w pomieszczeniu właściwy merytorycznie dział	
KI przy liście obecności	

Sposób realizacji obowiązku informacyjnego z wykorzystaniem klauzuli informacyjnej	
Klauzula Informacyjna – Media Społecznościowe	
	Określenie sposobu realizacji podania do wiadomości KI
KI na stronie Media Społecznościowe	
KI na stronie internetowej www	
KI pełna jako email	
KI skrócona jako email / link	
KI pełna w formie SMS	
KI skrócona w formie SMS / link	

Sposób realizacji obowiązku informacyjnego z wykorzystaniem klauzuli informacyjnej	
Klauzula Informacyjna – Połączenia telefoniczne	
	Określenie sposobu realizacji podania do wiadomości KI
KI na stronie internetowej www	
KI pełne nagrania audio	
KI skrócone nagranie audio / link	

Sposób realizacji obowiązku informacyjnego z wykorzystaniem klauzuli informacyjnej	
Klauzula Informacyjna – Formularz Kontaktowy przez WWW	
	Określenie sposobu realizacji podania do wiadomości KI
KI na stronie internetowej www	
KI pełna jako email	
KI skrócona jako email / link	
KI pełna jako email – autoodpowiedź	
KI skrócona jako email / link – autoodpowiedź	
KI pełna w formie SMS	
KI skrócona w formie SMS / link	

Sposób realizacji obowiązki informacyjnego z wykorzystaniem klauzuli informacyjnej	
Klauzula Informacyjna – ZFŚS	
	Określenie sposobu realizacji podania do wiadomości KI
KI na stronie internetowej www	
KI pełna jako email	
KI skrócona jako email / link	
KI pełna w formie SMS	
KI skrócona w formie SMS / link	
KI nadrukowana na wnioskach	

Sposób realizacji obowiązki informacyjnego z wykorzystaniem klauzuli informacyjnej	
Klauzula Informacyjna – KZP	
	Określenie sposobu realizacji podania do wiadomości KI
KI na stronie internetowej www	
KI dołączana do umowy	
KI pełna jako email	
KI skrócona jako email / link	
KI pełna w formie SMS	
KI skrócona w formie SMS / link	
KI nadrukowana na wnioskach	

Sposób realizacji obowiązku informacyjnego z wykorzystaniem klauzuli informacyjnej	
Klauzula Informacyjna – Praktykanci / Wolontariusze / Stażyści	
	Określenie sposobu realizacji podania do wiadomości KI
KI przekazywana osobie zainteresowanej	
KI na stronie internetowej www	
KI w systemie informatycznym	
KI pełna jako email	
KI skrócona jako email / link	
KI na tablicy w przestrzeni ogólnodostępnej	
KI w pomieszczeniu właściwy merytorycznie dział	
KI obowiązek przerzucony na podmiot kierujący na praktykę	

Uwaga. Ostrożnościowa realizacja art. 13 RODO

„Dla bezpieczeństwa należy przyjąć, że jeżeli jakąś drogą do organizacji wpływają dane, to przy tej drodze należy niejako postawić tabliczkę z informacjami z art. 13 RODO, a dla bezpieczeństwa, jeżeli dane z urzędu wypływają, to do każdej komunikacji wychodzącej należy również dołączyć informacje z art. 13 RODO. Czy jest to nadmierne czy tylko ostrożne – okaże się to za lat kilka.”⁷⁶

Uwaga. Informacje o odbiorcach.

Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją.

Zwrócić należy uwagę, iż podając informacje o odbiorcach danych w pierwszy wskazany sposób czyli poprzez wskazanie ich, jako skonkretyzowane podmioty, staniemy przed problemem wielości takich podmiotów a już na pewno zmierzyć będziemy musieli się z problemem ciągłego aktualizowania zapisów klauzul informa-

⁷⁶ J. Rzymowski. *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*. Kraków 2019. s. 144.

cyjnych a co za tym idzie odpowiedniego komunikowania o powyższym podmiotom danych.

Nie mniej jednak z treści Decyzji UODO z dnia 3 kwietnia 2019r. [ZSPU.421.8.2018]⁷⁷ wynika, iż administrator zobligowany został do usunięcia uchybienia w procesie przetwarzania danych osobowych, poprzez wskazanie w klauzuli informacyjnej dla osób realizujących obowiązki meldunkowy podmiotu świadczącego usługi serwisowe systemu informatycznego o nazwie [A], przy użyciu którego prowadzony jest rejestr mieszkańców, tj. [A. Sp. z o.o.] Oznacza to, iż organ stoi na stanowisku, iż to zasada przejrzystości wymusza, aby w treści klauzuli informacyjnej administrator wskazywał nazwy i adresy siedzib odbiorców danych.

Dodatkowo sprawę komplikuje fakt, iż **odbiorca** zgodnie z definicją RODO oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania. Niby wszystko jasne, ale czy za odbiorcę uważać należy podmioty, które występują już w określonej roli nazwanej przez RODO np. czy za odbiorcę uznać należy także podmioty przetwarzające, albo osoby upoważnione. Mając na względzie stanowisko zaprezentowane w ww. Decyzji UODO przyjąć należy, iż koniecznością będzie ujęcie w treści klauzuli informacyjnej odbiorców w szerokim rozumieniu, jako podmioty którym zlecono przetwarzanie danych osobowych, oraz de facto wszelkich odrębnych administratorów danych osobowych, którym dane są udostępniane.

„Możliwe błędy

Błędem jest lekceważenie obowiązku i nierealizowanie go.

Błędem jest przyjmowanie założenia, zgodnie z którym osoba, od której zbierane są dane osobowe, posiada już informacje wynikają-

⁷⁷ <https://uodo.gov.pl/decyzje/ZSPU.421.8.2018> (Dostęp: 2019.12.13. godz. 7:49)

ce z art. 13 RODO, podczas gdy osoba ta ich nie posiada. ADO może zakładać, że osoba, od której zbiera dane osobowe, posiada informacje wynikające z art. 13 RODO jedynie wtedy, jeżeli wcześniej je tej osobie, w ten czy inny sposób podał.

Błędem jest zakładanie, że jeżeli ktoś zwraca się do ADO, ale nie jako osoba fizyczna, tylko reprezentując inny podmiot, to wobec tego człowieka ADO nie musi realizować obowiązków wynikających z art. 13 RODO.”⁷⁸

⁷⁸ J. Rzymowski. *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*. Kraków 2019. s. 144-145.

Realizacja artykułu 14 RODO

Źródło obowiązku

Obowiązek udostępnienia informacji o szczegółach przetwarzania danych osobowych wynika z art. 14 RODO, podobnie jak z art. 13 RODO, o ile jednak udostępniane dane są podobne (jedynie podobne, nie w pełni te same), o tyle pozostałe okoliczności udostępniania danych są odmienne.

Z art. 14 ust. 1 RODO wynika obowiązek informowania o wymienionych w przepisie szczegółach przetwarzania danych podczas pozyskiwania tych danych nie od osoby, której one dotyczą. Przepis mówi o pozyskiwaniu⁷⁹ danych osobowych „w sposób inny niż od osoby, której dane dotyczą”. Przepis nie stanowi jak i od kogo trzeba dane pozyskać, by pojawił się obowiązek. Jedynym warunkiem, jeśli chodzi o źródło danych, jest, by były one pozyskiwane z innego źródła niż od osoby, której one dotyczą.

Treść dokumentu

Treść dokumentu wynika wprost z art. 14 ust 1 RODO w zw. z art. 14 ust. 2 RODO.

Należy zwrócić baczną uwagę na fakt, że całość obowiązku wynika nie tylko z art. 14 ust. 1 RODO, ale że równie istotny, przynajmniej co do zakresu udostępnianych informacji, jest art. 14 ust. 2 RODO.

⁷⁹ Podobnie: M. Krzysztofek. *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*. Warszawa 2016. s. 132.

KLAUZULA INFORMACYJNA

W związku z pozyskaniem Pani/Pana danych osobowych od **[Zleceniobiorca / Wykonawca]**, działając zgodnie z **art. 14** ogólnego Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE [dalej RODO] informuję, iż:

Dane Administratora Danych Osobowych [dalej ADO]	Nazwa ADO: ul. Kod pocztowy-..... Miejscowość:..... e-mail: tel.:
Dane kontaktowe Inspektora Ochrony Danych [dalej IOD]	Imię i nazwisko Inspektora Ochrony Danych: Adres korespondencyjny IOD: ul. Kod pocztowy-..... Miejscowość:..... e-mail: tel.: Z IOD można się kontaktować w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych.
Cel przetwarzania danych osobowych	Pana/Pani dane osobowe przetwarzane będą w celu: • związanym z prawidłową realizacją Umowy głównej • dochodzenia ewentualnych roszczeń.
Podstawa prawna przetwarzania	Podstawą prawną przetwarzania Pani/Pana danych osobowych jest: • art. 6 ust. 1 lit. f) RODO – przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO.
Źródło pozyskania	Pani/ Pana dane pozyskano z [Zleceniobiorca / Wykonawca] ,

danych:	
Zakres danych pozyskanych:	Zakres danych, które zostały pozyskane to: • imię (imiona) / nazwisko • stanowisko • adres email • numer telefonu
Odbiorcy danych. Udostępnianie danych. Powierzanie przetwarzania danych.	Pani/Pana dane osobowe będą udostępniane uprawnionym na podstawie przepisów prawa podmiotom i organom publicznym oraz w szczególności: zewnętrznej kancelarii prawnej, poczcie, kurierom, oraz podmiotom, z którymi ADO zawarł umowy powierzenia przetwarzania danych osobowych w szczególności: zewnętrzny podmiot usług IT, zewnętrzny hostingodawca, zewnętrzny podmiot usługi kadrowo/płacowe. Kategorie odbiorców: poczta, kurier, kancelaria prawna, służby sanitarne, Odbiorcy zdefiniowani: <u>Nazwa:</u> <u>Adres siedziby:</u> Kategorie podmiotów przetwarzających: serwis IT, zewnętrzne usługi kadrowe, zewnętrzne usługi płacowe, zewnętrzny hostingodawca. Podmioty przetwarzające zdefiniowane: <u>Nazwa:</u> <u>Adres siedziby:</u>
Okres przechowywania danych.	Okres przetwarzania Pani/Pana danych osobowych jest uzależniony od celu w jakim dane są przetwarzane. Okres, przez który Pani/Pana dane osobowe będą przechowywane jest obliczany w oparciu o następujące kryteria: czas obowiązywania umowy, przepis prawa, które mogą ADO

	obligować do przetwarzania danych przez określony czas, okres, który jest niezbędny do obrony interesów ADO. Pani/Pana dane przechowywane będą w szczególności przez czas obowiązywania Umowy głównej w związku z jej wykonywaniem i ewentualnym dochodzeniem roszczeń oraz przez okresy prawem określone, w szczególności: • 6 lat – zgodnie z <u>art. 118</u> Ustawy z dnia 23 kwietnia 1964 r., Kodeks Cywilny.
Prawa osoby której dane dotyczą.	Ma Pani/Pan prawo do: • dostępu do danych osobowych Pani/Pana dotyczących, • żądania od ADO sprostowania danych osobowych Pani/Pana dotyczących, • żądania od ADO usunięcia danych osobowych Pani/Pana dotyczących, • żądania od ADO ograniczenia przetwarzania danych osobowych Pani/Pana dotyczących, • wniesienia sprzeciwu wobec przetwarzania danych osobowych Pani/Pana dotyczących, • żądania od ADO przeniesienia danych osobowych Pani/Pana dotyczących, • cofnięcia zgody w dowolnym momencie bez konsekwencji dla przetwarzania, którego dokonano przed jej cofnięciem, jeśli dane zbierane są na podstawie zgody. Zakres każdego z tych praw oraz sytuacje, w których można z nich skorzystać, wynikają z przepisów RODO. Z praw tych może Pani/Pan skorzystać składając wniosek u ADO. Ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO. Pani/Pana dane nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym o profilowaniu.
Przekazywanie danych osobowych odbiorcom w państwach trzecich.	Administrator nie będzie przekazywał Pani/Pana danych osobowych odbiorcom w państwach trzecich oraz organizacjom międzynarodowym.

KLAUZULA INFORMACYJNA

Dla danych pozyskanych z innych źródeł niż osoba, której dane dotyczą:

W związku z pozyskaniem Pani/Pana danych osobowych od [Zleceniobiorca / Wykonawca], działając zgodnie z art. 14 ogólnego Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE [dalej Rozporządzenie RODO] informuję, iż:

1. Administratorem Pani/Pana danych osobowych jest [Zleceniodawcy / Zamawiającego] z siedzibą w [pełen adres], [dalej ADO] którego reprezentuje [imię i nazwisko, funkcja], z ADO skontaktować można się w następujący sposób:
 - a. Listownie – przesyłając list na ww. adres siedziby ADO
 - b. Telefonicznie – pod numerem telefonu [numer telefonu]
 - c. E-mai – za pośrednictwem korespondencji email [adres email]
2. Inspektorem Ochrony Danych jest
Z Inspektorem można się kontaktować we wszystkich sprawach dotyczących przetwarzania przez nas Pani/Pana danych osobowych oraz korzystania z praw związanych z tym przetwarzaniem.
 - a. Listownie przesyłając list n ww. adres siedziby ADO
 - b. Telefonicznie – pod numerem telefonu
 - c. E-mail – za pośrednictwem korespondencji email.....,
3. Pani/Pana dane osobowe przetwarzane będą w celach związanych z realizacją Umowy nr
z dnia [Umowa główna] a podstawą ich przetwarzania jest prawnie uzasadniony interes ADO - art. 6 ust. 1 lit. f) Rozporządzenia RODO.
4. Zakres danych, które zostały pozyskane to: [np. imię / nazwisko / stanowisko / adres email]
5. Pani/ Pana dane pozyskano z [Zleceniobiorca / Wykonawca],
6. Okres przetwarzania Pani/Pana danych osobowych jest uzależniony od celu w jakim dane są przetwarzane. Okres, przez który Pani/Pana dane osobowe będą przechowywane jest obliczany w oparciu o następujące kryteria: czasu obowiązywania umowy, przepis prawa, które mogą ADO obligować do przetwarzania danych przez określony czas (np. 5-letni obowiązek archiwizacyjny dotyczący dokumentów przechowywanych w celach podatkowych) okres, który jest niezbędny do obrony interesów ADO.

7. Pana/Pani dane mogą być udostępniane podmiotom upoważnionym na podstawie przepisów prawa oraz podmiotom, którym ADO powierzył dane w celu prawidłowego wykonania swoich obowiązków w celu i zakresie niezbędnym do tych czynności.
8. Ma Pani/Pan prawo
 - a. żądania od nas dostępu do danych osobowych Pani, Pana dotyczących,
 - b. żądania od nas sprostowania danych osobowych Pani, Pana dotyczących
 - c. żądania od nas usunięcia danych osobowych Pani, Pana dotyczących,
 - d. żądania od nas ograniczenia przetwarzania danych osobowych Pani, Pana dotyczących,
 - e. wniesienia sprzeciwu wobec przetwarzania danych osobowych Pani, Pana dotyczących,
9. W związku z przetwarzaniem Pani/Pana danych nie są podejmowane zautomatyzowane decyzje.
10. Istnieje możliwość wniesienia skargi do organu nadzorczego na tryb i sposób przetwarzania danych osobowych przez ADO, jeśli uzna Pani/ Pan za uzasadnione, że Pani/ Pana dane osobowe są przetwarzane niezgodnie z Rozporządzeniem RODO.
- 11.** Administrator nie będzie przekazywał Pani/Pana danych osobowych odbiorcom w państwach trzecich oraz organizacjom międzynarodowym.

Zwolnienia ze stosowania art. 14 RODO w realiach medycznych

Należy się zastanowić czy w realiach medycznych zastosowanie znajduje którekolwiek ze zwolnień z obowiązków wynikających z artykułu 14 ust. 1 RODO.

Zwolnienie z art. 14 ust. 5 lit. a RODO

Jeżeli skierowanie do podmiotu zostaje dostarczone inną drogą niż za pośrednictwem pacjenta, to podmiot ten otrzymuje dane dotyczące pacjenta od podmiotu kierującego nie zaś od pacjenta. Z tego zwolnienia nie można skorzystać. Nie oznacza to jednak, że podmiot do którego skierowano pacjenta powinien poinformować pacjenta o informacjach wynikających z artykułu 14 ust. 1 RODO ponieważ funkcjonuje zwolnienie wynikające z art. 14 ust. 5 lit c RODO.

Jeżeli pacjent stawia się w podmiocie by zrealizować świadczenie, to podmiot do którego go skierowano powinien zrealizować wobec tego pacjenta obowiązek informacyjny, jednak dlatego, że obowiązek ten wynika z art. 13 ust. 1 RODO.

Zwolnienie z art. 14 ust. 5 lit. b RODO

Nie wydaje się by PWDL mógł skorzystać z tego zwolnienia. Stan faktyczny, który sugeruje ewentualną, acz odradzaną przeze mnie możliwość skorzystania ze zwolnienia, zachodzi kiedy podmiot otrzyma skierowanie jednak zostanie ono dostarczone zdalnie, czyli nie przez pacjenta, zaś pacjent w ogóle nie stawia się do podmiotu w celu realizacji świadczenia. Kusząca jest wizja skorzystania w takiej sytuacji ze zwolnienia z realizacji obowiązku z artykułu 14 ust. 1 RODO, wydaje się jednak że nie należy tej pokusie ulegać, jest to bowiem pokusa procesowo niebezpieczna.

Zwolnienie z art. 14 ust. 5 lit. c RODO

Z tego właśnie przepisu wynika zwolnienie, z którego PWDL powinien korzystać. Ze względu na poważne zagrożenie procesowe, w wypadku, gdyby PWDL nie realizował obowiązku a zwolnienie nie zachodziło, poniżej wyjaśniamy dlaczego ono zachodzi.

Z przepisu, z którego wynika zwolnienie, czyli art. 14 ust. 5 lit. c RODO wynika, że administrator nie powinien realizować obowiązku wynikającego z art. 14 ust. 1 RODO, jeżeli: „pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa

członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą”.

Pierwszy warunek, od którego uzależnione jest zwolnienie z obowiązku, to czy „pozyskiwanie lub ujawnianie” (zapewne danych osobowych) „jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator”.

Drugi warunek od którego uzależnione jest zwolnienie z obowiązku, to czy prawo (UE lub prawo państwa członkowskiego), o którym mowa przewiduje „odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą”.

Jeśli chodzi o pierwszy warunek, to uważam, że jest on zrealizowany. Jeżeli chodzi o pozyskiwanie informacji o pacjencie, to lekarz lub inny pracownik PWDL ma obowiązek wykonywać swoje czynności w oparciu właśnie o informacje o pacjencie. Pewna ilość tych informacji zostaje zamieszczona w skierowaniu, inne uzyskiwane są od pacjenta w wyniku wywiadu, jeszcze inne uzyskiwane są na drodze badania pacjenta. Swoją drogą, to przy badaniu pacjenta mamy do czynienia ze zjawiskiem wytwarzania danych osobowych. Jeśli chodzi o ujawnianie informacji o pacjencie, to również jest ono uregulowane prawem. Informacje ujawniane są pacjentowi oraz osobom, na które wskazuje UoPPiRPP oraz inne akty prawa medycznego. Nawet sprawa tak drobna jak to, że na życzenie pacjenta przy udzielaniu świadczeń zdrowotnych może być obecna osoba bliska opisane jest w art. 21 ust. 1 UoPPiRPP.

Jeśli chodzi o drugi warunek, to uważam, że jest on również zrealizowany. Z UoPPiRPP wynika tajemnica medyczna, ustawa ta przewiduje również komu i jak udostępniać dokumentację medyczną. Inne akty prawa medycznego konstytuują odpowiednie tajemnice, za złamanie których są w dodatku przewidziane sankcje karne.

Zwolnienie z art. 14 ust. 5 lit. d RODO

Tajemnica, do której w realiach PWDL, odnosi się ten przepis, na przykład tajemnica medyczna, nie obowiązuje wobec osoby, której informacja dotyczy. Jednocześnie to właśnie wobec tej osoby realizowany jest obowiązek wynikający z art. 14 ust. 1 RODO, co z kolei prowadzi do wniosku, że w realiach PWDL, zwolnienie wynikające z tego przepisu nie zachodzi.

„Możliwe błędy

Błędem jest lekceważenie obowiązku i nierealizowanie go.

Błędem jest przyjmowanie założenia, zgodnie z którym osoba, której dane osobowe uzyskano nie od niej, posiada już informacje wynikające z art. 14 RODO. Osoba tych danych, w zasadzie, posiadać nie może. ADO może zakładać, że osoba, od której zbiera dane osobowe, posiada informacje wynikające z art. 14 RODO jedynie wtedy, jeżeli wcześniej je tej osobie, w ten czy inny sposób podała.

Błędem jest zakładanie, że jeżeli ADO otrzymuje dane od podmiotu innego niż osoba fizyczna, to nie ma obowiązku realizacji art. 14 RODO wobec osoby fizycznej, której dane dotyczą.

Błędem jest nadużywanie zwolnienia wynikającego z art. 14 ust. 5 lit b RODO, czyli: „udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku (...)”, zwłaszcza kiedy udzielenie jest możliwe lub wysiłek jest pomijalny.”⁸⁰

Błędem jest realizowanie obowiązku z art. 5 ust. 1 RODO, wtedy, kiedy nie ma on miejsca.

⁸⁰ J. Rzymowski. *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*. Kraków 2019. s. 171-172.

Realizacja artykułów 15 - 22 RODO

Nie wchodząc w dywagacje na temat tego, czy udostępnienie kopii danych zawartych w dokumentacji medycznej, zgodnie z art. 15 ust. 3 RODO jest, czy nie jest równoznaczne z obowiązkiem udostępnienia danych w formie i strukturze właściwej dla udostępnienia dokumentacji medycznej, zgodnie z UoPPiRP, stwierdzić należy, iż w realiach medycznych będziemy mieli do czynienia z udostępnianiem danych osobowych zgodnie z przepisami art. 15 RODO, jak i zgodnie z regulacjami branżowymi traktującymi o udostępnianiu informacji o stanie zdrowia pacjentów, informacji o udzielonych im świadczeniach, skończywszy na udostępnianiu dokumentacji medycznej.

W pierwszym ze wskazanych trybów, realizowanym zgodnie z art. 15 RODO, mamy do czynienia z faktem udostępniania danych o szerszym zakresie, aniżeli dane zawarte w dokumentacji medycznej.

W drugim trybie, zakładającym udostępnianie dokumentacji i informacji według przepisów branżowych, udostępniać będziemy dokumentację medyczną oraz informacje, które zawierać będą oprócz danych osobowych pacjentów, także dane osobowe podmiotów danych np. tworzących dokumentację medyczną bądź w niej zapisanych np. członkowie rodziny pacjenta.

Należy również zauważyć, iż realizacja, przez podmioty danych, pozostałych uprawnień, o jakich mowa w treści przepisu art. 15-21 RODO, wiązać będzie się z przekazywaniem danych lub informacji ich dotyczących. Powyższe również powinno bezwzględnie zostać ujęte w polityce ochrony jednostki, jako administratora danych osobowych.

Za zasadne uznać należy przygotowanie jednostki do obsługi wniosków kierowanych do niej zgodnie z uprawnieniami określonymi przepisami art. 15 – 22 RODO. Do tego celu można wykorzystać zamieszczone poniżej formularze opisujące kolejno tryby postępowania w zależności od stanu faktycznego.

Poniżej prezentujemy dokumentację, którą można wykorzystać bezpośrednio w jednostce. Każde z praw podmiotu danych, jakie przysługuje na gruncie przepisów RODO przedstawione zostało według schematu.

W pierwszej części zestawienia tabelarycznego ujęte zostały informacje, które pozwalać będą na dokumentowanie aktualizacji kolejnych wersji dokumentu opisującego procedurę realizacji praw podmiotów danych na gruncie RODO oraz krótkie wprowadzenie.

W drugiej części zestawienia tabelarycznego przetoczone zostały przepisy właściwe RODO traktujące o każdym z praw podmiotu danych na gruncie RODO, jakie jest kolejno opisywane.

W trzeciej natomiast części zestawienia tabelarycznego znajdują się właściwe wzory wniosków podmiotów danych oraz wzory schematów proponowanych odpowiedzi ADO.

Poniżej zatem prezentujemy to, jak może wyglądać praktycznie gotowa dokumentacja, którą ADO może stosować do obsługi wniosków podmiotów danych. Zestawienia tabelaryczne stanowiące ww. dokumentację uzupełnione są także komentarzem i dodatkowymi wyjaśnieniami, których treść można pominąć przy przygotowywaniu dokumentacji ostatecznej przez ADO.

Procedura realizacji praw osób których dane dotyczą zgodnie z art. 15 - 22 RODO			
Dotyczy jednostki:.....			
Rejestr zmian:			
Wersja	Data	Opracował	Opis aktualizacji
v-1-0-0			utworzenie dokumentu

Wprowadzenie

1. Administrator ma obowiązek poszanowania praw podmiotów danych określonych w art. 15 - 22 RODO. W tym celu w przypadku wystąpienia jakichkolwiek wątpliwości, co do tożsamości osoby występującej z żądaniem, jako podmiotu danych, którego dane dotyczą, administrator zobowiązany jest do podjęcia czynności ukierunkowanych na jednoznaczne ustalenie lub potwierdzenie tożsamości osoby wnioskodawcy.
2. Realizacja praw podmiotu danych nie może naruszać praw osób trzecich.
3. Administrator zobowiązany jest do niezwłocznego reagowania na zgłoszone mu żądania, w szczególności informując o konieczności uzupełnienia wniosku, celem jego rozpatrzenia.
4. Administrator ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15–22 RODO.
5. Administrator bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15–22 RODO. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.
6. Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Prawo dostępu do danych / uzyskania informacji / uzyskania kopii danych – art. 15 RODO

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:
 - a) cele przetwarzania,
 - b) kategorie odnośnych danych osobowych,
 - c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,
 - d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
 - e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
 - f) informacje o prawie wniesienia skargi do organu nadzorczego,
 - g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle,
 - h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem.
3. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.
4. Prawo do uzyskania kopii, o której nie może niekorzystnie wpływać na prawa i wolności innych.

Realizacja prawa dostępu do danych / uzyskania informacji / uzyskania kopii danych

1. Wnioskodawca będący podmiotem danych, którego dane dotyczą, ma prawo dostępu do danych / uzyskania informacji / uzyskania kopii danych jego dotyczących przetwarzanych przez ADO.
2. W ramach struktury organizacyjnej ADO żądania wnioskodawców w ww. zakresie obsługuje
3. Żądania wnioskodawców przyjmowane są przez ADO:
 - a) osobiście przez:.....
 - b) telefonicznie pod numerem telefonu:
 - c) drogą listową:.....
 - d) drogą elektroniczną:.....
4. Dla ułatwienia obsługi administracyjnej żądań wnioskodawców zaleca się stosowanie wzoru wniosku stanowiącego załącznik do niniejszej procedury. Wykorzystanie wzoru formularza jednak nie jest warunkiem koniecznym realizacji żądania.
5. Wzór wniosku dostępny jest:
 - a) w lokalu jednostki:
 - b) do pobrania z adresu www:
6. Żądanie wnioskodawcy powinno zawierać informacje umożliwiające w sposób jednoznaczny identyfikację osoby podmiotu danych, których dane dotyczą oraz jego zakres.
7. Podmiotowi danych, w ramach prawa dostępu należy umożliwić dostęp do tych danych.
8. ADO dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych.
9. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się w powszechnie stosowanej formie elektronicznej.
10. Prawo do uzyskania kopii, o której mowa powyżej, nie może niekorzystnie wpływać na prawa i wolności innych osób.
11. ADO dokumentuje sposób udzielenia informacji w odpowiedzi na wniosek wnioskodawcy.

Konieczność weryfikacji tożsamości wnioskodawcy

Jakiegokolwiek uprawnienia wynikające z przepisu przysługują jedynie osobie, której dane dotyczą. Wynika z tego, że zanim ADO zrealizuje którykolwiek z obowiązków wynikający z art. 15 RODO, to musi najpierw upewnić się, czy osoba podająca się za kogoś jest rzeczywiście osobą, za którą się podaje. Jest to niezwykle ważne. ADO, który tego zaniedba, ryzykuje, że udostępni informacje osobie nieuprawnionej a w końcu, że udostępni osobie nieuprawnionej nawet dane osobowe.

Obowiązki informacyjne, wynikające z art. 15 RODO spoczywają na ADO. Kto, jaka osoba fizyczna, zrealizuje te obowiązki w ramach działalności ADO – tego przepis nie reguluje, jednak, jeżeli obowiązki nie zostaną zrealizowane, to odpowiedzialność poniesie ADO.

„Dokumentowanie realizacji art. 15 RODO

– realizacja zasady rozliczalności

Istotą realizacji art. 15 RODO jest podawanie informacji w przepisie wskazanych na żądanie osób, których dane dotyczą. Nie ma obowiązku odbierania pokwitowań po realizacji żądania, należy jednak pamiętać o zasadzie rozliczalności. Z art. 5 ust. 2 RODO (zasada rozliczalności) w zw. z art. 5 ust. 1 lit a RODO (zasada rzetelności i zasada przejrzystości) w zw. z art. 15 RODO wynika, że ADO powinien mieć sposób wykazania, że realizuje obowiązek wynikający z art. 15 RODO. Udokumentować realizację art. 15 można na przykład na jeden z opisanych poniżej sposobów.

- odebrać pokwitowanie – niekonieczne, ale nie jest to rozwiązanie złe,
- opisać w Polityce Ochrony sposób lub sposoby realizacji obowiązku wynikającego z art. 15 RODO – rozwiązanie dobre, wymaga jednak pewnej dyscypliny, tak by rzeczywiście robiono to, co w Polityce Ochrony opisano,
- archiwizację żądań składanych na podstawie art. 15 ust. 1 RODO i archiwizację kopii informacji udzielanych na konkretne żądania konkretnych osób.”⁸¹

⁸¹ J. Rzymowski RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora. Kraków 2019. s. 186.

Zastosowanie formularzy

Zamieszczone wzory dokumentacji w formie zestawień tabelarycznych pomyślane są w taki sposób by ułatwić osobom których dane dotyczą składanie żądań umożliwiających tym osobom korzystanie z uprawnień które przysługują im na gruncie RODO. Możliwa jest jednak sytuacja, w której osoba której dane dotyczą składa żądanie ustnie, drogą mailową, na papierze, czy w jakikolwiek inny sposób jednak bez wykorzystania formularzy, którymi posługuje się administrator. Również w takiej sytuacji warto by administrator skorzystał z formularzy mogą one bowiem ułatwić administratorowi podjęcie odpowiedniej decyzji jednocześnie zarchiwizowane kopie wypełnionych formularzy stanowią dowód realizacji przepisu a tym samym umożliwiają wykazanie zasady rozliczalności.

**WNIOSEK O REALIZACJĘ PRAWA DOSTĘPU DO DANYCH /
UDOSTĘPNIENIE INFORMACJI / KOPII DANYCH**

Zgodnie z **art. 15** Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) (dalej „**RODO**”)

działając w imieniu własnym, jako osoba której dane dotyczą wnoszę jak poniżej.

I.

Dane identyfikujące wnioskodawcę, jako osobę ,której dane dotyczą	
Imię wnioskodawcy:	
Nazwisko wnioskodawcy:	
PESEL wnioskodawcy:	
Inne dane pozwalające na jednoznaczną identyfikację osoby wnioskodawcy, jako osoby, której dane dotyczą:	
Data złożenia wniosku:	

II.

Zakres żądania wnioskodawcy:	Wnioskodawca dokonuje wyboru TAK
Żądam dostępu do danych osobowych mnie dotyczących:	
Żądam udostępnienia mi informacji:	
Żądam udzielenia mi kopii danych osobowych mnie dotyczących:	

Pouczenie:

ADO dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną. Prawo do uzyskania kopii, nie może niekorzystnie wpływać na prawa i wolności innych.

III.

Wybrany przez wnioskodawcę sposób udzielenia informacji / sposób przekazania kopii danych	Wnioskodawca dokonuje wyboru TAK
Odbiór osobisty przez wnioskodawcę	
Wysyłka do wnioskodawcy	
Wysyłka drogą elektroniczną	

IV.

Sposób złożenia wniosku:	
Osobiście	
Za pośrednictwem korespondencji listowej	
Za pośrednictwem korespondencji email	
Podpis osoby przyjmującej	Imię i nazwisko Stanowisko:..... Data:
Numer referencyjny wniosku	

**STANOWISKO ADMINISTRATORA DANYCH OSOBOWYCH
W PRZEDMIOCIE WNIOSKU O REALIZACJĘ PRAWA
DOSTĘPU DO DANYCH / UDOSTĘPNIENIE INFORMACJI /
KOPII DANYCH**

I.

Miejscowość i data sporządzenia stanowiska:	
Stanowisko dotyczy wniosku o numerze referencyjnym:	
Administrator Danych Osobowych:	
Adresat Stanowiska:	

II.

Wnioskodawca żądał:	
Dostępu do danych osobowych go dotyczących:	
Udostępnienia mu informacji:	
U udzielenia mu kopii danych osobowych mnie dotyczących:	

III.

Odpowiedź administratora	Informacja administratora
Potwierdzenie faktu przetwarzania danych osobowych wnioskodawcy, jako osoby której dane dotyczą:	
Informacja o celu przetwarzania danych osobowych wnioskodawcy, jako osoby, której dane dotyczą:	
Informacja o kategoriach danych osobowych wnioskodawcy, jako osoby, której dane dotyczą	
Informacja o odbiorcach / kategoriach odbiorców którym dane osobowe wnioskodawcy, jako osoby, której dane dotyczą, zostały lub zostaną ujawnione w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,	
Informacja o planowanym okresie przechowywania danych osobowych wnioskodawcy, jako osoby, której dane dotyczą, a gdy nie jest to możliwe kryteria ustalenia tego okresu.	
Informacja o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania:	
Informacja o prawie wniesienia skargi do organu nadzorczego:	
W przypadku kiedy dane nie zostały zebrane od osoby, której dotyczą, wszelkie dostępne informacje o ich źródle:	

Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą:			
Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem:			
Umożliwienie dostępu do danych wnioskodawcy, jako osoby której dane dotyczą:	<table> <tr> <td data-bbox="693 777 874 936">Czy dostęp został umożliwiony i zrealizowany</td><td data-bbox="874 777 1066 936"></td></tr> </table>	Czy dostęp został umożliwiony i zrealizowany	
Czy dostęp został umożliwiony i zrealizowany			
Uzyskanie kopii danych osobowych podlegających przetwarzaniu przez ADO.	<table> <tr> <td data-bbox="693 936 874 1086">Czy przekazano kopię danych osobowych</td><td data-bbox="874 936 1066 1086"></td></tr> </table>	Czy przekazano kopię danych osobowych	
Czy przekazano kopię danych osobowych			

IV.

Wskazany we wniosku przez wnioskodawcę sposób udzielenia informacji / sposób przekazania kopii danych	TAK	Potwierdzenie udzielenia informacji / uzyskania kopii danych
Odbiór osobisty przez wnioskodawcę		Podpis wnioskodawcy
Wysyłka do wnioskodawcy		Nr korespondencji wychodzącej:.....
Wysyłka drogą elektroniczną		Potwierdzenie nadania korespondencji drogą elektroniczną:
Podpis (ADO), pracownika ADO podejmującego decyzję	Podpis: Data:	

Prawo do sprostowania danych – art. 16 RODO.

1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
2. Administrator informuje o sprostowaniu którego dokonał, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Realizacja prawa do sprostowania danych

1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
2. Administrator informuje o sprostowaniu którego dokonał, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.
3. Wnioskodawca będący podmiotem danych, którego dane dotyczą, ma prawo do sprostowania danych osobowych.
4. W ramach struktury organizacyjnej ADO żądania wnioskodawców w ww. zakresie obsługuje
5. Żądania wnioskodawców przyjmowane są przez ADO:
 - a. osobiście przez:
 - b. telefonicznie pod numerem telefonu:
 - c. drogą listową:
 - d. drogą elektroniczną:
6. Dla ułatwienia obsługi administracyjnej żądań wnioskodawców zaleca się stosowanie wzoru wniosku stanowiącego załącznik do niniejszej procedury. Wykorzystanie wzoru formularza jednak nie jest warunkiem koniecznym realizacji żądania.
7. Wzór wniosku dostępny jest:
 - a. w lokalu jednostki:
 - b. do pobrania z adresu www:.....
8. Żądanie wnioskodawcy powinno zawierać informacje umożliwiające w sposób jednoznaczny identyfikację osoby podmiotu danych, których dane dotyczą oraz jego zakres.
9. Realizacja wniosku nie powinna doprowadzić do sytuacji, w jakiej uzupełnienie danych łamałoby zasadę minimalizacji lub prawidłowości danych. Oświadczenie wnioskodawcy musi w sposób jednoznaczny wskazywać swój zakres oraz dane osobowe podlegające sprostowaniu.
10. ADO dokumentuje sposób załatwienia sprawy z wniosku wnioskodawcy.

WNIOSEK O REALIZACJĘ PRAWA DO SPROSTOWANIA DANYCH OSOBOWYCH

Zgodnie z **art. 16** Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) (dalej „**RODO**”) **działając w imieniu własnym, jako osoba której dane dotyczą wnoszę jak poniżej.**

I.

Dane identyfikujące wnioskodawcę, jako osobę ,której dane dotyczą	
Imię wnioskodawcy:	
Nazwisko wnioskodawcy:	
PESEL wnioskodawcy:	
Inne dane pozwalające na jednoznaczną identyfikację osoby wnioskodawcy, jako osoby, której dane dotyczą:	
Data złożenia wniosku:	

II.

Żądanie: POPRAWIENIA DANYCH	Wskazanie danych wymagających sprostowania	Wskazanie danych prawidłowych
Żądam sprostowania danych osobowych mnie dotyczących jako danych nieprawidłowych. Żądając powyższego składam oświadczenie o zasadności takiego sprostowania.		
Żądanie: UZUPEŁNIENIE DANYCH	Niekompletność danych polega na / wynika z:	Wskazanie danych, których uzupełniania żąda wnioskodawca.
Żądam sprostowania danych osobowych mnie dotyczących jako danych niekompletnych poprzez ich uzupełnienie.		
W załączeniu do niniejszego wniosku przedkładam stosowne dokumenty potwierdzające zasadność uzupełnienia niekompletnych danych		

III.

Wybrany przez wnioskodawcę sposób udzielenia odpowiedzi w przedmiocie rozstrzygnięcia.	Wnioskodawca dokonuje wyboru TAK
Odbiór osobisty przez wnioskodawcę	
Wysyłka do wnioskodawcy	
Wysyłka drogą elektroniczną	

IV.

Sposób złożenia wniosku:	
Osobiście	
Za pośrednictwem korespondencji listowej	
Za pośrednictwem korespondencji email	
Podpis osoby przyjmującej	Imię i nazwisko Stanowisko:..... Data:
Numer referencyjny wniosku	

**STANOWISKO ADMINISTRATORA DANYCH OSOBOWYCH
W PRZEDMIOCIE WNIOSKU O REALIZACJĘ PRAWA
DOSTĘPU DO DANYCH / UDOSTĘPNIENIE INFORMACJI /
KOPII DANYCH**

I.

Miejscowość i data sporządzenia stanowiska:	
Stanowisko dotyczy wniosku o numerze referencyjnym:	
Administrator Danych Osobowych:	
Adresat Stanowiska:	

II.

Wnioskodawca żądał:	
Poprawienia danych:	
Uzupełnienia danych:	

III.

Żądanie wnioskodawcy w zakresie POPRAWIENIA DANYCH	Uwzględniono w całości	Uwzględniono w części	Nie uwzględniono w całości
Uzasadnienie stanowiska ADO:			
Żądanie: UZUPEŁNIENIE DANYCH	Uwzględniono w całości	Uwzględniono w części	Nie uwzględniono w całości
Uzasadnienie stanowiska ADO:			

IV.

Wybrany przez wnioskodawcę sposób poinformowania go o sposobie załatwienia sprawy	TAK	Potwierdzenie
Odbiór osobisty przez wnioskodawcę		Podpis wnioskodawcy
Wysyłka do wnioskodawcy		Nr korespondencji wychodzącej:
Wysyłka drogą elektroniczną		Potwierdzenie nadania korespondencji drogą elektroniczną:
Podpis (ADO)	Podpis: Data:	

Prawo do usunięcia danych – prawo do bycia zapomnianym – art. 17 RODO

1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
 - a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,
 - b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) RODO lub art. 9 ust. 2 lit. a) RODO, i nie ma innej podstawy prawnej przetwarzania,
 - c) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania,
 - d) dane osobowe były przetwarzane niezgodnie z prawem,
 - e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator,
 - f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 RODO
3. Jeżeli administrator upublicznił dane osobowe, a na mocy ust. 1 ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.
4. Opisane uprawnienia nie będą miały zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:
 - a) do korzystania z prawa do wolności wypowiedzi i informacji,
 - b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania

- zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
- c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3 RODO
 - d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
 - e) do ustalenia, dochodzenia lub obrony roszczeń
5. Administrator informuje o usunięciu danych osobowych którego dokonał, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.
 6. Prawo do usunięcia danych, do bycia zapomnianym nie ma charakteru bezwzględnego.

Jeśli chodzi o omawiane tu prawo do bycia zapomnianym, to w realiach PWDL, w odniesieniu do danych pacjentów, jest ono pewną niedogodnością dla administratora, jednak zwykle realizowane być nie może, co więcej, w realiach medycznych zwykle ono pacjentom nie przysługuje, pacjenci jednak o tym nie wiedzą i w związku ze swoją niewiedzą mogą żądać usuwania dotyczących ich danych. Podmioty lecznicze mają obowiązek przechowywać dokumentację medyczną przez wiele lat. Wynika to z art. 29 UoPPiRPP.

Zwracamy zwłaszcza uwagę na treść art. 17 ust. 4 lit b RODO. Przepis ten stanowi, że:

„Opisane uprawnienia nie będą miały zastosowania, w zakresie w jakim przetwarzanie jest niezbędne: (...)

- b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,(...)”.

Wskazane tu „Opisane uprawnienia” to właśnie prawo do bycia zapomnianym. Jak zatem widać osobie, której dane dotyczą, w naszym rozważaniu pacjentowi, nie przysługuje prawo do bycia zapomnianym, jeżeli przetwarzanie jest niezbędne w celu wskazanym w przepisie. Cel wskazany w przepisie, który jest istotny dla PWDL to wywiązanie się „z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator”. Takim właśnie obowiązkiem jest obowiązek przechowywania dokumentacji medycznej. Podkreślenia wymaga, że z art. 17 ust. 4 lit b RODO wynika, że pacjentom nie przysługuje prawo do żądania usunięcia dotyczących ich danych osobowych, które znajdują się w dokumentacji medycznej. Może się zdarzyć, zupełnie wyjątkowo, że pacjentowi takie prawo przysługuje. Dzieje się tak, kiedy PWDL przechowuje dokumentację której przechowywać nie powinien, ponieważ termin jej przechowywania upłynął. Oczywiście wtedy podmiot powinien na żądanie pacjenta dokumentację usunąć, pamiętając przy tym, że w ogóle nie powinien jej już mieć.

Zwracamy uwagę, że ze względu na zrozumiałość, a zwykle dodatkowo zwiększaną przez media, niewiedzę osób, których dane dotyczą – pacjentów, osoby te mogą składać żądania usunięcia danych osobowych, mimo braku prawa do tego. Wydaje się, że mimo nie przysługującego prawa, administrator powinien żądanie takie przyjąć, udokumentować fakt jego przyjęcia, poprzez na przykład zarchiwizowanie treści żądania, po czym tą samą drogą, jaką żądanie zostało złożone administrator powinien wyjaśnić osobie, której dane dotyczą, że prawo do żądania usunięcia danych jej nie przysługuje. Nie sposób wskazać przepisu, z którego wynikałaby nasza rada. Formułujemy tę radę dlatego, że uważamy, że lepiej by administrator poświęcił czas na podnoszenie świadomości pacjenta, niż na udzielanie wyjaśnień pracownikom PUODO.

WNIOSEK O REALIZACJĘ PRAWA DO USUNIĘCIA DANYCH / DO BYCIA ZAPOMNIANYM

Zgodnie z **art. 17** Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) (dalej „RODO”) działając w imieniu własnym, jako osoba której dane dotyczą wnoszę jak poniżej.

I.

Dane identyfikujące wnioskodawcę, jako osobę ,której dane dotyczą	
Imię wnioskodawcy:	
Nazwisko wnioskodawcy:	
PESEL wnioskodawcy:	
Inne dane pozwalające na jednoznaczną identyfikację osoby wnioskodawcy, jako osoby, której dane dotyczą:	
Data złożenia wniosku:	

II.

Żądam usunięcia danych ponieważ:	Wnioskodawca wskazuje TAK
Dane osobowe nie są już niezbędne do celów, w których zostały zebrane.	
Dane osobowe nie są już niezbędne do celów, w których są przetwarzane.	
Wycofałam/łem zgodę na przetwarzanie danych osobowych mnie dotyczących, jaką uprzednio wyraziłam/łem zgodnie z art. 6 ust. 1 lit. a) RODO lub art. 9 ust. 2 lit. a) RODO, i nie ma innej podstawy prawnej przetwarzania.	
Wniosłam/łem sprzeciw na mocy art. 21 ust. 1 RODO ⁸² wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą.	
Wniosłam/łem sprzeciw na mocy art. 21 ust. 2 RODO ⁸³ wobec przetwarzania,	
Dane osobowe były przetwarzane niezgodnie z prawem.	
Dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator.	
Dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 ⁸⁴	

⁸² Art. 21 ust. 1 RODO. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) RODO, w tym profilowania na podstawie tych przepisów. Admini-

II.

Uzasadnienie merytoryczne wniosku wnioskodawcy:

stratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

⁸³ Art. 21 ust. 2 RODO Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

⁸⁴ Art. 8 ust. 1 RODO Jeżeli zastosowanie ma art. 6 ust. 1 lit. a) RODO, w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgodnie z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. Jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowwała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody. Państwa członkowskie mogą przewidzieć w swoim prawie niższą granicę wiekową, która musi wynosić co najmniej 13 lat.

IV.

Wybrany przez wnioskodawcę sposób udzielenia odpowiedzi w przedmiocie rozstrzygnięcia.	Wnioskodawca dokonuje wyboru TAK
Odbiór osobisty przez wnioskodawcę	
Wysyłka do wnioskodawcy	
Wysyłka drogą elektroniczną	

V.

Sposób złożenia wniosku:	
Osobiście	
Za pośrednictwem korespondencji listowej	
Za pośrednictwem korespondencji email	
Podpis osoby przyjmującej	Imię i nazwisko Stanowisko:..... Data:
Numer referencyjny wniosku	

**STANOWISKO ADMINISTRATORA DANYCH OSOBOWYCH
W PRZEDMIOCIE WNIOSKU O USUNIĘCIE DANYCH /
BYCIE ZAPOMNIANYM**

I.

Miejscowość i data sporządzenia stanowiska:	
Stanowisko dotyczy wniosku o numerze referencyjnym:	
Administrator Danych Osobowych:	
Adresat Stanowiska:	

II.

Żądanie wnioskodawcy wyrażone treścią wniosku:	Uwzględniono w całości	Uwzględniono w części	Nie uwzględniono w całości
Dane osobowe nie są już niezbędne do celów, w których zostały zebrane.			
Dane osobowe nie są już niezbędne do celów, w których są przetwarzane.			
Wycofałam/łem zgodę na przetwarzanie danych osobowych mnie dotyczących, jaką uprzednio wyraziłam/łem zgodnie z art. 6 ust. 1 lit. a) Rozporządzenia RODO lub art. 9 ust. 2 lit. a) Rozporządzenia RODO, i nie ma innej podstawy prawnej przetwarzania.			
Wniosłam/łem sprzeciw na mocy art. 21 ust. 1 Rozporządzenia RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą.			
Wniosłam/łem sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania,			
Dane osobowe były przetwarzane niezgodnie z prawem.			
Dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator.			
Dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 RODO			

III.

Wybrany przez wnioskodawcę sposób poinformowania go o sposobie załatwienia sprawy	TAK	Potwierdzenie
Odbiór osobisty przez wnioskodawcę		Podpis wnioskodawcy
Wysyłka do wnioskodawcy		Nr korespondencji wychodzącej:
Wysyłka drogą elektroniczną		Potwierdzenie nadania korespondencji drogą elektroniczną:
Podpis (ADO)	Podpis: Data:	

Prawo do ograniczenia przetwarzania

1. Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w następujących przypadkach:
 - a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych,
 - b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
 - c) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
 - d) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.
2. Ograniczenie przetwarzania oznacza to oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.
3. Wśród metod pozwalających ograniczyć przetwarzanie danych osobowych mogą się znaleźć między innymi:
 - a) czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania,
 - b) uniemożliwienie użytkownikom dostępu do wybranych danych,
 - c) czasowe usunięcie opublikowanych danych ze strony internetowej,
 - d) w zautomatyzowanych zbiorach danych przetwarzanie należy zasadniczo ograniczyć środkami technicznymi w taki sposób, by dane osobowe nie podlegały dalszemu przetwarzaniu ani nie mogły być zmieniane. Fakt ograniczenia przetwarzania danych osobowych należy wyraźnie zaznaczyć w systemie.
4. Jeżeli przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby

fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

5. Przed uchyceniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia.
6. Administrator informuje o ograniczeniu przetwarzania którego dokonał, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

WNIOSEK O REALIZACJĘ PRAWA DO OGRANICZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie z **art. 18** Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) (dalej „**RODO**”) **działając w imieniu własnym, jako osoba której dane dotyczą wnoszę jak poniżej.**

I.

Dane identyfikujące wnioskodawcę, jako osobę, której dane dotyczą	
Imię wnioskodawcy:	
Nazwisko wnioskodawcy:	
PESEL wnioskodawcy:	
Inne dane pozwalające na jednoznaczną identyfikację osoby wnioskodawcy, jako osoby, której dane dotyczą:	
Data złożenia wniosku:	

II.

Żądam ograniczenia przetwarzania danych osobowych mnie dotyczących, jako wnioskodawcy:	Wnioskodawca wskazuje TAK
Kwestionuję prawidłowość danych osobowych.	
Przetwarzanie moich danych osobowych jest niezgodne z prawem, jednak sprzeciwiam się ich usunięciu.	
Ze względu na to, że ADO nie potrzebuje już danych osobowych mnie dotyczących do celów przetwarzania, ale są one potrzebne mnie, do ustalenia, dochodzenia lub obrony roszczeń,	
Ze względu na fakt, iż wniosłam/łem sprzeciw na mocy art.	

21 ust. 1 Rozporządzenia RODO wobec przetwarzania danych mnie dotyczących – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.	
--	--

Żądam ograniczenia przetwarzania ze względu na ww. wskazane uzasadnienie wszystkich danych osobowych mnie dotyczących:	Należy wybrać tylko wtedy, kiedy wnioskodawca żąda ograniczenia przetwarzania wszystkich danych osobowych jego dotyczących:
Żądam ograniczenia przetwarzania ze względu na ww. wskazane uzasadnienie określonych danych osobowych mnie dotyczących:	Należy wskazać dane względem których wnioskodawca żąda ograniczenia ich przetwarzania:

III.

Żądam ograniczenia przetwarzania danych osobowych mnie dotyczących, poprzez:	Wnioskodawca dokonuje wyboru TAK	Wnioskodawca wskazuje okres ograniczenia przetwarzania
czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania		Do czasu
uniemożliwienie użytkownikom dostępu do wyżej wskazanych danych		Do czasu
czasowe usunięcie opublikowanych danych ze strony internetowej		Do czasu
oznaczenie danych w celu usunięcia w przyszłości w terminie:.....		W terminie
oznaczenie danych w celu ograniczenia ich przetwarzania w przyszłości.		Ograniczenie polegać ma na

IV.

Wybrany przez wnioskodawcę sposób udzielenia odpowiedzi w przedmiocie rozstrzygnięcia.	Wnioskodawca dokonuje wyboru TAK
Odbiór osobisty przez wnioskodawcę	
Wysyłka do wnioskodawcy	
Wysyłka drogą elektroniczną	

V.

Sposób złożenia wniosku:	
Osobiście	
Za pośrednictwem korespondencji listowej	
Za pośrednictwem korespondencji email	
Podpis osoby przyjmującej	Imię i nazwisko Stanowisko:..... Data:
Numer referencyjny wniosku	

STANOWISKO ADMINISTRATORA DANYCH OSOBOWYCH W PRZEDMIOCIE WNIOSKU O OGRANICZENIE PRZETWARZANIA DANYCH OSOBOWYCH

I.

Miejscowość i data sporządzenia stanowiska:	
Stanowisko dotyczy wniosku o numerze referencyjnym:	
Administrator Danych Osobowych:	
Adresat Stanowiska:	

II.

W odpowiedzi na wniosek wnioskodawcy ADO zastosował ograniczenie przetwarzania danych polegające na:	
Ograniczenie przetwarzania wyżej opisane odnosi się do następujących danych osobowych:	
ADO informuje, iż przetwarzał będzie dane osobowe wyłącznie za zgodą podmiotu danych, w celu ustalenia, dochodzenia lub obrony roszczeń, w celu ochrony praw innej osoby fizycznej, albo prawnej, bądź też ze względu na ważny interesu publiczny Unii lub państwa członkowskiego. (*niepotrzebne skreślić)	

III.

Wybrany przez wnioskodawcę sposób poinformowania go o sposobie załatwienia sprawy	TAK	Potwierdzenie
Odbiór osobisty przez wnioskodawcę		Podpis wnioskodawcy
Wysyłka do wnioskodawcy		Nr korespondencji wychodzącej:
Wysyłka drogą elektroniczną		Potwierdzenie nadania korespondencji drogą elektroniczną:
Podpis (ADO)	Podpis: Data:	

**STANOWISKO ADMINISTRATORA DANYCH OSOBOWYCH
W PRZEDMIOCIE POINFORMOWANIA OSOBY KTÓREJ
DANE DOTYCZĄ O ZAMIARZE UCHYLENIA
OGROANICZENIA PRZETWARZANIA.**

Zgodnie z **art. 18 ust. 3** Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) (dalej „RODO”)

informuję co następuje:

I.

Miejscowość i data sporządzenia stanowiska:	
Stanowisko dotyczy wniosku o numerze referencyjnym:	
Administrator Danych Osobowych:	
Adresat Stanowiska:	

II.

Informujemy, o zamiarze uchylenia ograniczenia przetwarzania wskazanych danych osobowych:	
Podstawą uzasadniającą uchylenie ograniczenia przetwarzania jest:	
ADO ustalił, iż dane osobowe są prawidłowe	
ADO poprawił nieprawidłowe dane osobowe	
ADO doszedł do wniosku, iż prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą, jaki złożyła.	

III.

Sposób dostarczenia stanowiska wnioskodawcy	ADO wskazuje wybrany sposób doręczenia stanowiska	Potwierdzenie
Odbiór osobisty przez wnioskodawcę		Podpis wnioskodawcy
Wysyłka do wnioskodawcy		Nr korespondencji wychodzącej:
Wysyłka drogą elektroniczną		Potwierdzenie nadania korespondencji drogą elektroniczną:
Podpis (ADO)	Podpis: Data:	

STANOWISKO ADMINISTRATORA DANYCH OSOBOWYCH W PRZEDMIOCIE UCHYLENIA OGRANICZENIA PRZETWARZANIA DANYCH OSOBOWYCH.

Zgodnie z **art. 18 ust. 3** Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) (dalej „RODO”)

informuję co następuje:

I.

Miejscowość i data sporządzenia stanowiska:	
Stanowisko dotyczy wniosku o numerze referencyjnym:	
Administrator Danych Osobowych:	
Adresat Stanowiska:	

II.

Informujemy, o uchyleniu ograniczenia przetwarzania wskazanych danych osobowych:	
Data uchylenia ograniczenia przetwarzania wskazanych wyżej danych osobowych:	Data:
Podstawą uzasadniającą uchylenie ograniczenia przetwarzania było to, iż:	
ADO ustalił, iż dane osobowe są prawidłowe	
ADO poprawił nieprawidłowe dane osobowe	
ADO doszedł do wniosku, iż prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą, jaki złożyła.	

III.

Sposób dostarczenia stanowiska wnioskodawcy	ADO wskazuje wybrany sposób doręczenia stanowiska	Potwierdzenie
Odbiór osobisty przez wnioskodawcę		Podpis wnioskodawcy
Wysyłka do wnioskodawcy		Nr korespondencji wychodzącej:
Wysyłka drogą elektroniczną		Potwierdzenie nadania korespondencji drogą elektroniczną:
Podpis (ADO)	Podpis: Data:	

Prawo do przenoszenia danych – art. 20 RODO

1. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli:
 - a) przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) RODO lub art. 9 ust. 2 lit. a) RODO lub na podstawie umowy w myśl art. 6 ust. 1 lit. b); RODO oraz
 - b) przetwarzanie odbywa się w sposób zautomatyzowany.
2. Wykonując prawo do przenoszenia danych osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.
3. Wykonanie prawa do przenoszenia danych pozostaje bez uszczerbku dla prawa do usunięcia danych. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.
4. Prawo, do przenoszenia danych nie może niekorzystnie wpływać na prawa i wolności innych.

**WNIOSEK O REALIZACJĘ PRAWA
DO PRZENOSZENIA DANYCH OSOBOWYCH**

Zgodnie z **art. 19** Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) (dalej „RODO”)
działając w imieniu własnym, jako osoba której dane dotyczą
wnoszę jak poniżej.

I.

Dane identyfikujące wnioskodawcę, jako osobę ,której dane dotyczą	
Imię wnioskodawcy:	
Nazwisko wnioskodawcy:	
PESEL wnioskodawcy:	
Inne dane pozwalające na jednoznaczną identyfikację osoby wnioskodawcy, jako osoby, której dane dotyczą:	
Data złożenia wniosku:	

II.

Żądam przeniesienia danych osobowych mnie dotyczących, jako wnioskodawcy a przetwarzanie		Wnioskodawca wskazuje TAK
Odbywa się na podstawie mojej zgody w myśl art. 6 ust. 1 lit. a) RODO lub art. 9 ust. 2 lit. a) RODO		
Odbywa się na podstawie umowy w myśl art. 6 ust. 1 lit. b) RODO		
Odbywa się w sposób zautomatyzowany.		
Żądam przeniesienia wszystkich moich danych osoba, przez ADO bezpośrednio innemu wskazanemu ADO, o ile jest to technicznie możliwe:	Należy wskazać dane innego administratora:	
Żądam przeniesienia określonych moich danych osoba, przez ADO bezpośrednio innemu wskazanemu ADO, o ile jest to technicznie możliwe:	Należy wskazać dane innego administratora:	
	Należy wskazać dane względem których wnioskodawca żąda przeniesienia:	

III.

Wybrany przez wnioskodawcę sposób udzielenia odpowiedzi w przedmiocie rozstrzygnięcia.	Wnioskodawca dokonuje wyboru TAK
Odbiór osobisty przez wnioskodawcę	
Wysyłka do wnioskodawcy	
Wysyłka drogą elektroniczną	

IV.

Sposób złożenia wniosku:	
Osobiście	
Za pośrednictwem korespondencji listowej	
Za pośrednictwem korespondencji email	
Podpis osoby przyjmującej	Imię i nazwisko Stanowisko: Data:
Numer referencyjny wniosku	

STANOWISKO ADMINISTRATORA DANYCH OSOBOWYCH W PRZEDMIOCIE PRZENIESIENIA DANYCH OSOBOWYCH DO INNEGO ADMINISTRATORA

I.

Miejscowość i data sporządzenia stanowiska:	
Stanowisko dotyczy wniosku o numerze referencyjnym:	
Administrator Danych Osobowych:	
Adresat Stanowiska:	

II.

Żądanie wnioskodawcy wyrażone treścią wniosku:	Uwzględniono w całości	Uwzględniono w części	Nie uwzględniono w całości
Żądam przeniesienia wszystkich moich danych osoba, przez ADO bezpośrednio innemu wskazanemu ADO, o ile jest to technicznie możliwe:			
Żądam przeniesienia określonych moich danych osoba, przez ADO bezpośrednio innemu wskazanemu ADO, o ile jest to technicznie możliwe:			

III.

Sposób dostarczenia stanowiska wnioskodawcy	ADO wskazuje wybrany sposób doręczenia stanowiska	Potwierdzenie
Odbiór osobisty przez wnioskodawcę		Podpis wnioskodawcy
Wysyłka do wnioskodawcy		Nr korespondencji wychodzącej:
Wysyłka drogą elektroniczną		Potwierdzenie nadania korespondencji drogą elektroniczną:
Podpis (ADO)	Podpis: Data:	

Możliwe błędy

Błędem jest brak upewnienia się przez ADO, czy żądania wynikające z art. 15 – 22 RODO składa osoba, której dane dotyczą.

Błędem jest lekceważenie obowiązków i nierealizowanie ich.

Błędem jest brak odpowiedzi w sytuacji kiedy żądania wynikające z art. 15 – 22 RODO nie mogą być spełnione. Odpowiedzi, niezależnie od tego jakiej, należy udzielić.

Błędem jest brak możliwości wykazania realizacji art. 15 – 20 RODO.

Błędem jest realizacja art. 15 – 22 RODO i jednocześnie niezabezpieczenie sobie przez ADO dowodów potwierdzających fakt, że tej realizacji dokonał.

Błędem jest uzależnienie realizacji obowiązków wynikających z art. 15 – 22 RODO od złożenia przez osoby, których dane dotyczą na formularzach przewidzianych przez ADO.⁸⁵

Błędem jest usuwanie danych z dokumentacji medycznej przed upływem terminu obowiązkowego przechowania.

⁸⁵ Szerzej: K. Wygoda w: M. Sakowska–Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre. *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*. Warszawa 2018. s. 238.

**Udostępnianie danych
osobowych
poprzez
udostępnianie dokumentacji
medycznej oraz
informacji o stanie zdrowia
i udzielonych świadczeniach
zdrowotnych**

Udostępnianie danych osobowych poprzez udostępnianie dokumentacji medycznej oraz informacji o stanie zdrowia i udzielonych świadczeniach zdrowotnych.

Prawo do dokumentacji medycznej

Pacjent ma prawo do dostępu do dokumentacji medycznej dotyczącej jego stanu zdrowia. Ponadto ma także prawo do przekazania mu informacji na temat jego stanu zdrowia, rozpoznania, proponowanych oraz możliwych metodach diagnostycznych i leczniczych, informacji o dających się przewidzieć następstwach ich zastosowania albo następstwach ich zaniechania, informacji o wynikach leczenia oraz informacji o rokowaniu. Aby prawa te mogły być realizowane podmioty udzielające świadczeń zdrowotnych mają obowiązek prowadzić, przechowywać, udostępniać i chronić dokumentację medyczną swoich pacjentów⁸⁶. Widać zatem, że z prawem pacjenta do dokumentacji

⁸⁶ Zgodnie z Wyrokiem Wojewódzkiego Sądu Administracyjnego z dnia 10 maja 2017r., (VII SA/Wa 361/17) cyt.: „(...) przechowywanie (...) dokumentacji medycznej w pomieszczeniu z dojściem do maszynowni windy, do obsługi urządzeń wentylacyjnych, i do skrzynki alarmowej (...) nie stanowi o zapewnieniu odpowiednich warunków zabezpieczających tą dokumentację przed zniszczeniem, uszkodzeniem lub utratą i dostępem osób nieupoważnionych. Konieczność konserwacji ww. urządzeń może spowodować, że dostęp do tej dokumentacji będą miały osoby wykonujące ww. czynności a więc osoby nieupoważnione. W dodatku dokumentacja ta nadal jest narażona na zniszczenie, utratę lub uszkodzenie. (...)”.

Zgodnie z Wyrokiem Naczelnego Sądu Administracyjnego z dnia 10 kwietnia 2018r. (II OSK 69/18) cyt.: „(...) Podmiot udzielający świadczeń zdrowotnych jest obowiązany prowadzić, przechowywać i udostępniać dokumentację medyczną. Wykonanie tego obowiązku obciążającego podmiot udzielający świadczeń zdrowotnych wymaga podjęcia działań zapewniających ochronę dokumentacji medycznej, przy czym przy jego wykonaniu obowiązany jest do dołożenia szczególnej staranności w tym i wystąpienia okoliczności utraty kontroli nad dokumentacją medyczną. Zaniechania działania, które obarczone jest

i prawem do informacji łączy się obowiązek podmiotu wykonującego działalność leczniczą prowadzenia, przechowywania udostępniania i ochrony dokumentacji. Z tego to względu jednostki powinny z należytą starannością traktować procedurę udostępniania dokumentacji medycznej, albowiem jej prawidłowa realizacja stanowi obowiązek podmiotu medycznego.

Definicja dokumentacji medycznej

Przepisy prawa nie wprowadzają definicji dokumentacji medycznej. Jednak na podstawie ich analizy można pokusić się o jej sformułowanie. Zatem uznać należy, że dokumentacja medyczna to zbiór dokumentów, prowadzonych, przechowywanych, udostępnianych i zabezpieczanych przez podmiot udzielający świadczeń zdrowotnych. Dokumentów dotyczących stanu zdrowia pacjenta, opisujących stan zdrowia pacjenta. Dokumentów dotyczących udzielonych świadczeń zdrowotnych pacjentowi, opisujących udzielone mu świadczenia zdrowotne. Dokumentację medyczną tworzą także wszelkie oświadczenia pacjenta, przedstawiciela ustawowego pacjenta oraz informacje odnoszone na podstawie udostępnionej jednostce przez pacjenta innej dokumentacji medycznej o istotnym charakterze dla procesu diagnostycznego, leczniczego lub pielęgnacyjnego.

Forma prowadzenia dokumentacji medycznej

Należy zwrócić uwagę na istotną różnicę, jaką wprowadza w praktyce Rozporządzenie Ministra Zdrowia z dnia 06 kwietnia 2020r., w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania wchodzi w życie z dniem 15 kwietnia 2020r. (Dz.U. z 2020r., poz. 666). (Rozporządzenie RDM) Zgod-

cechą szczególnej staranności stanowi praktykę naruszającą zbiorowe prawa pacjenta. Od takiej oceny zaniechania naruszającego zbiorowe prawa pacjenta podmiot udzielający świadczeń zdrowotnych może się uwolnić, gdy utrata dokumentacji medycznej następuje w wyniku zdarzeń, które rozsądnie przewidująca jednostka nie mogła przewidzieć (np. zdarzenie siły wyższej, kradzież). W razie gdy okoliczności utraty przez podmiot leczniczy dokumentacji medycznej można było przewidzieć, wynikały bowiem z okoliczności faktycznej w jakiej podmiot udzielający świadczeń zdrowotnych ją wykonywał, nie można przyjąć, że nie było to bezprawne zaniechanie. (...) Brak zatem przez zaniechanie zabezpieczenia dokumentacji medycznej wypełnia przesłankę bezprawnego zaniechania naruszającego zbiorowe prawa pacjenta (...).”

nie z Rozporządzeniem RDM zasadą staje się, iż dokumentacja medyczna ma być prowadzona w postaci elektronicznej. Jednostka nie ma już prawa dokonywania swobodnego wyboru tego, w jakiej postaci, czy w papierowej, czy w elektronicznej, prowadzić będzie dokumentację medyczną. Jedyne w wyjątkowych sytuacjach, ustawodawca dał możliwość prowadzenia dokumentacji w postaci papierowej, czyli w sytuacji kiedy przepisy tak stanowią, jak również w sytuacji, kiedy warunki organizacyjno-techniczne uniemożliwiają prowadzenie jej w postaci elektronicznej. Należy jednak dodatkowo zasygnalizować, iż w sytuacji, w której podmiot udzielający świadczeń zdrowotnych zobligowany został zobowiązany, przepisami prawa, do prowadzenia Elektronicznej Dokumentacji Medycznej, potocznie nazywanej EDM, wówczas także musi zachować taką postać prowadzenia dokumentacji. W takiej sytuacji nie ma prawa dokonywania wyboru. Nie może postanowić, iż będzie prowadził, określone wskazane dokumenty, w innej postaci niż w postaci Elektronicznej Dokumentacji Medycznej.

Zwracamy także uwagę na to, iż Rozporządzenie RDM zakazuje prowadzenia dokumentów medycznych równolegle w dwóch postaciach, czyli w postaci elektronicznej oraz równocześnie w postaci papierowej. Celem takiego rozwiązania jest wyeliminowanie z obrotu dwóch oryginałów jednego dokumentu utworzonego w postaci elektronicznej i papierowej.

Dokumentacja medyczna w postaci papierowej

Jest to dokumentacja tworzona i przechowywana w postaci papierowej. Oczywiście do tworzenia takiej dokumentacji w postaci papierowej można i wykorzystuje się komputery i aplikacje do jej przygotowywania, co nie oznacza, jeszcze, że mamy w takim przypadku do czynienia z dokumentacją w postaci elektronicznej. W takiej sytuacji mamy do czynienia z dokumentacją prowadzoną w postaci papierowej wydrukowaną po jej sporządzeniu z wykorzystaniem komputera. Błędem jest sporządzanie dokumentacji w postaci elektronicznej, z wykorzystaniem aplikacji, które nie spełniają prawem określonych kryteriów do tego, aby można było za ich pomocą prowadzić dokumentację w postaci elektronicznej.

Dokumentacja medyczna w postaci elektronicznej

Jak wspominaliśmy wyżej, zasadą staje się, iż dokumentacja medyczna ma być prowadzona w postaci elektronicznej. Dokumentacja może być prowadzona w postaci papierowej, jeżeli przepis tak stanowi lub warunki organizacyjno-techniczne uniemożliwiają prowadzenie dokumentacji w postaci elektronicznej. Aby dokumentacja medyczna mogła być prowadzona w postaci elektronicznej, a w tym w postaci Elektronicznej Dokumentacji Medycznej, należy zapewnić aby system teleinformatyczny⁸⁷, w jakim dokumentacja jest tworzona, przechowywana, zapisywana spełniał określone prawem funkcjonalności.

EDM – Elektroniczna Dokumentacja Medyczna

Dostrzegaliśmy jej niezrozumienie tematu polegające na myleniu pojęć dokumentacji prowadzonej w postaci elektronicznej, z EDM, czyli z Elektroniczną Dokumentacją Medyczną.

Zgodnie z definicją zawartą w art. 2 pkt 6) Ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia⁸⁸ (Dalej: Ustawa OSIOZ) cyt.: „(...) Użyte w ustawie określenia oznaczają: (...) elektroniczna dokumentacja medyczna - dokumenty wytworzone w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności

⁸⁷ Zgodnie z art. 2 pkt. 3) Ustawa z dnia 18 lipca 2002 r., o świadczeniu usług drogą elektroniczną (Dz.U. z 2002 nr 144, poz. 1204 ze zm.) cyt.: „(...) system teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu ustawy z dnia 16 lipca 2004r. – Prawo telekomunikacyjne (Dz.U. 2018 r., poz.1954 i 2245) (...)”.

Zgodnie z art. 3 pkt. 3 Ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2019 r. poz. 700 z późn. zm.) cyt.: „(...) system teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004r. – Prawo telekomunikacyjne (Dz.U. z 2018r. poz. 1954, 2245 i 2354); (...)”.

⁸⁸ Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. 2011 r., Nr 113, poz. 657 ze zm.).

danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych:

- recepty,
- określone w przepisach wydanych na podstawie art. 13a,
- skierowania określone w przepisach wydanych na podstawie art. 59aa ust. 2 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2020 r. poz. 1398, z późn. zm.),
- zlecenia na zaopatrzenie i zlecenia naprawy, o których mowa w art. 38 ust. 4a ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2020 r. poz. 357, 945, 1493, 1875 i 2401 oraz z 2021 r. poz. 159),
- Karty Szczepień, o których mowa w art. 21a ust. 1 ustawy z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (Dz. U. z 2020 r. poz. 1845, 2112 i 2401 oraz z 2021 r. poz. 159, 180 i 255);(...)

Nie wystarczy jednak jedynie zapisanie danego dokumentu w postaci cyfrowej, aby taki dokument zyskał miano Elektronicznej Dokumentacji Medycznej. Dla uznania danego rodzaju dokumentu za taki, który jest Elektroniczną Dokumentacją Medyczną i musi w związku z tym być prowadzony w szczególnej formie, dokument taki musi być wymieniony wprost w art. 2 pkt. 6 USIOZ, albo w przepisach wydanych na podstawie art. 13a Ustawy SIOZ.

Zdarza się, że jednostki zobligowane do prowadzenia EDM zapisując dokumenty jedynie w postaci elektronicznej, nie składając prawem określonych podpisów pod taką dokumentacją, co oznacza, iż nie realizują swoich obowiązków w tym zakresie. Z ostrożności zalecamy, aby podejmując decyzję o wdrożeniu EDM w jednostce z wykorzystaniem konkretnego informatycznego rozwiązania, przed przystąpieniem do tego procesu w sposób dokładny zweryfikować dostawcę usługi pod kątem spełniania przez proponowane przez niego rozwiązanie funkcjonalności prawem przewidzianych. Naturalnie warto jest także, podjąć działania zmierzające do uruchomienia szkoleń dla personelu opisujących zasady posługiwania się nowym rozwiązaniem informatycznym.

Dla obowiązku prowadzenia dokumentacji medycznej, jako Elektronicznej Dokumentacji Medycznej, bez znaczenia jest to, czy dana jednostka realizuje świadczenia w związku z umową z publicznym płatnikiem (NFZ), czy też nie. Obowiązek prowadzenia określonych dokumentów – Elektronicznej Dokumentacji Medycznej, jest obowiązkiem powszechnym.

Szczególne wymogi

Kiedy dokumentacja medyczna prowadzona jest w postaci elektronicznej przepisy przewidują dodatkowe obowiązki dla podmiotów udzielających świadczeń zdrowotnych, jeśli chodzi o udostępnianie tak prowadzonej dokumentacji medycznej.

Zacząć należy od tego, że przepisy prawa nakładają obowiązek zagwarantowania określonych funkcjonalności systemów teleinformatycznych, przy wykorzystaniu których będzie prowadzona, zapisywana, przechowywana i udostępniania dokumentacja medyczna w postaci elektronicznej. System ma zagwarantować możliwość prowadzenia i udostępniania dokumentacji w formatach i standardach wydanych na podstawie art. 11 ust. 1a i 1b Ustawy OSIOZ, a w przypadku ich braku – możliwość prowadzenia i udostępniania dokumentacji w standardach HL7 oraz DICOM lub innych standardach i formatach. System teleinformatyczny, w którym jest prowadzona dokumentacja w postaci elektronicznej ma zapewniać także możliwość eksportu całości danych w wyżej wymienionych standardach i formatach, w sposób umożliwiający odtworzenie ich w innym systemie teleinformatycznym. System teleinformatyczny musi posiadać funkcjonalność, która pozwoli na przetworzenie dokumentacji udostępnianej przez samego pacjenta na postać elektroniczną. Po takim przetworzeniu w sposób zapewniający czytelność, spójność i dostępność dokument załączany jest do dokumentacji medycznej.

W przypadku gdy dokumentacja prowadzona w postaci elektronicznej jest udostępniana w formie wydruku, osoba upoważniona przez podmiot potwierdza jego zgodność z dokumentacją i opatruje swoim oznaczeniem, zawierającym imię (imiona), nazwisko, stanowisko i podpis. Wydruk sporządza się w sposób umożliwiający identyfikację osoby udzielającej świadczeń zdrowotnych, zgodnie z § 10 pkt 3 Rozporządzenia RDM.

Pamiętać także należy, iż udostępnianie dokumentacji tworzonej w postaci elektronicznej za pośrednictwem środków komunikacji elektronicznej, czy to na informatycznym nośniku danych, musi być dokonane z zachowaniem zasad bezpieczeństwa. Dokumentację udostępnia się z zachowaniem jej integralności, poufności oraz autentyczności, bez zbędnej zwłoki. Mowa tutaj o szyfrowaniu korespondencji przesyłanej do adresata, o przekazywaniu haseł dostępowych do plików odrębnym kanałem przekazu, stosowaniu takich formatów zapisu, które nie będą miały wpływu na treść, na spójność na czytelność dokumentu dostarczonego.

Zgodnie z § 10 pkt 6) Rozporządzenia RDM. dokumentacja indywidualna, jeżeli przepisy nie stanowią inaczej, zawiera adres poczty elektronicznej lub elektronicznej skrzynki podawczej pacjenta, na który ma być przekazana dokumentacja medyczna – w przypadkach udostępniania dokumentacji w sposób, o którym mowa w art. 27 ust. 1 pkt 4 i ust. 3 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta.

System teleinformatyczny do prowadzenia dokumentacji medycznej w postaci elektronicznej.

Należy pamiętać, że opisane w Rozporządzeniu RDM wymagania dotyczące systemu teleinformatycznego⁸⁹ odnosić należy nie tylko do aplikacji, która tworzy i zapisuje dokumentację medyczną w postaci cyfrowej. Wymagania te należy odnosić do całego systemu telein-

⁸⁹ Zgodnie z art. 2 pkt. 3) Ustawa z dnia 18 lipca 2002 r., o świadczeniu usług drogą elektroniczną cyt.: „(...) system teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu ustawy z dnia 16 lipca 2004r. – Prawo telekomunikacyjne (Dz.U. 2018 r. poz. 1954 i 2245) (...)”

Zgodnie z art. 3 pkt. 3 Ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne1 cyt.: „(...) system teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004r. – Prawo telekomunikacyjne (Dz.U. 2018 r. poz. 1954, 2245 i 2354); (...)”

formatycznego w jednostce, czyli do całej infrastruktury. Zagadnienie dostosowania systemu teleinformatycznego do wymogów ustawodawcy, jest tematem często pomijanym i bagatelizowanym przez jednostki, które nie dostrzegają istoty zagadnienia oraz tego, iż innego rodzaju zagrożenia wiążą się z prowadzeniem dokumentacji medycznej w postaci papierowej niż zagrożenia towarzyszące prowadzeniu dokumentacji medycznej w postaci elektronicznej, z naciskiem na to, iż dokumentacja prowadzona w systemie teleinformatycznym narażona jest o wiele bardziej, co wymaga zastosowania innego rodzaju środków organizacyjnych, ale niestety i poniesienia nakładów finansowych⁹⁰.

Podmioty uprawnione do dokumentacji medycznej i informacji

Zgodnie z przepisami UoPPiRP podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną pacjentowi, lub jego przedstawicielowi ustawowemu, bądź osobie upoważnionej przez pacjenta.

Powyższe wymusza na jednostce obowiązek weryfikowania statusu osób wnioskodawców, czy organów występujących o dostęp do dokumentacji medycznej, w celu ustalenia, czy uprawnienie dostępu do dokumentacji im przysługuje.

Definicje kategorii osób uprawnionych

Pacjent

Osoba zwracająca się o udzielenie świadczeń zdrowotnych lub korzystająca ze świadczeń zdrowotnych udzielanych przez podmiot udzielający świadczeń zdrowotnych lub osobę wykonującą zawód medyczny⁹¹, w odniesieniu do udostępniania dokumentacji medycznej, dodać należy do ww. definicji element, który

⁹⁰ <https://prostetorodo.pl/2020/05/19/dokumentacja-prowadzona-w-postaci-elektronicznej-jakie-wymogi/>

⁹¹ Zgodnie z art. 3 ust. 1 pkt 4) UoPPiRP cyt.: „(...) użyte w ustawie określenia oznaczają: (...) pacjent – osobę zwracającą się o udzielenie świadczeń zdrowotnych lub korzystającą ze świadczeń zdrowotnych udzielanych przez podmiot udzielający świadczeń zdrowotnych lub osobę wykonującą zawód medyczny (...)”,

łączy ww. osobę fizyczną, z podmiotem udostępniającym dokumentację medyczną, tj. fakt udzielania jej, bądź udzielenia jej w przeszłości, albo zwrócenia się o udzielenie świadczeń zdrowotnych. Tylko bowiem w takiej sytuacji wystąpi stan faktyczny przejawiający się w utworzeniu dokumentacji medycznej, która będzie mogła dopiero być udostępniona albo powstaną informacje, które będą mogły zostać udzielone. Powyższe weryfikowane będzie na etapie rozpatrywania wniosku o udostępnienie mu dokumentacji medycznej. Nie sposób przyjąć z góry założenia, iż złożenie wniosku o udostępnienie dokumentacji medycznej oznacza, iż wskazana w nim osoba, której dokumentacja ma być udostępniona - jest / była pacjentem danego podmiotu będącego adresatem wniosku. Uzasadnia to konieczność dokonywania weryfikacji tożsamości osoby wskazanej we wniosku, jako pacjent.

Przedstawiciel ustawowy pacjenta

Osoba, która z mocy przepisu prawa może działać w cudzym imieniu i ze skutkiem dla osoby, którą reprezentuje. Czynności dokonane przez przedstawiciela ustawowego wywołują bezpośrednio skutki dla reprezentowanej przez nią osoby. Przedstawicielem ustawowym są: rodzice małoletnich dzieci, ustanowiony przez sąd opiekun⁹², kurator.

Dokumentem potwierdzającym status osoby, jako rodzica – będącego przedstawicielem ustawowym pacjenta może być akt urodzenia dziecka, jeśli weryfikacja nie jest możliwa do dokonania w oparciu o posiadane przez podmiot informacje w szczególności zawarte w dokumentacji medycznej pacjenta.

Dokumentem potwierdzającym status osoby, jako opiekuna ustanowionego przez sąd, bądź kuratora działającego w roli przedstawiciela ustawowego pacjenta – jest stosowne postanowienie sądu.

Wskazać należy, iż literalne brzmienie art. 26 UoPPiRP prowadzi do konkluzji, iż jedynie pacjent posiada uprawnienie do złożenia oświadczenia woli w zakresie określenia osoby trzeciej, jako osoby

⁹² Zgodnie z art. 155 § 1 i 2 Ustawy z dnia 25 lutego 1964r., Kodeks rodzinny i opiekuńczy (Dz. U. 1964 r., Nr 9 poz. 59 ze zm.) cyt.: „(...) § 1. Opiekun sprawuje pieczę nad osobą i majątkiem pozostającego pod opieką; podlega przy tym nadzorowi sądu opiekuńczego (...) § 2. Do sprawowania opieki stosuje się odpowiednio przepisy o władzy rodzicielskiej z zachowaniem przepisów poniższych (...)”.

upoważnionej do otrzymania jego dokumentacji medycznej, czy do uzyskiwania informacji o jego stanie zdrowia i udzielonych świadczeniach zdrowotnych. Należy jednak pamiętać o przepisach dotyczących pełnomocnictwa ujętych w Ustawie z dnia 23 kwietnia 1964 r. - Kodeks Cywilny, które stanowią podstawę dla ustanowienia przez przedstawiciela ustawowego pacjenta, osoby trzeciej - jako jej pełnomocnika, z uprawnieniem do udostępnienia mu dokumentacji medycznej pacjenta, którego jest przedstawicielem ustawowym.

Zgodnie z art. 98 § 1 Ustawy z dnia 25 lutego 1964r., Kodeks rodzinny i opiekuńczy (Dz.U. z 1964r., nr 9 poz. 59 ze zm.) cyt.: „(...) **rodzice są przedstawicielami ustawowymi dziecka pozostającego pod ich władzą rodzicielską. Jeżeli dziecko pozostaje pod władzą rodzicielską obojga rodziców, każde z nich może działać samodzielnie jako przedstawiciel ustawowy dziecka (...)**”. Innymi słowy, nie ma potrzeby składania przez jednego z rodziców oświadczenia w zakresie upoważnienia do dokumentacji medycznej, do udzielania informacji nt. stanu zdrowia dziecka względem drugiego z rodziców. Z pragmatycznego jednak punktu widzenia za zasadne i celowe uznać należy odnotowanie danych identyfikujących obojga rodziców, jako przedstawicieli ustawowych tak, aby na podstawie ww. informacji stworzyć możliwość ich. identyfikacji.

Osoba upoważniona

W dokumentacji indywidualnej wewnętrznej zamieszcza się lub dołącza do niej oświadczenie pacjenta o wyrażeniu zgody na udzielanie informacji o jego stanie zdrowia i udzielonych świadczeniach zdrowotnych, ze wskazaniem imienia i nazwiska osoby upoważnionej oraz danych umożliwiających kontakt z tą osobą⁹³, co oznacza, iż pacjent ma prawo wskazać wybraną przez siebie osobę

⁹³ Zgodnie z § 8 ust. 1 pkt. 1) nowego Rozporządzenia RDM „(...) Oświadczenie pacjenta:

- 1) o wyrażeniu zgody na udzielanie informacji, o której mowa w art. 9 ust. 3 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, ze wskazaniem imienia i nazwiska osoby upoważnionej oraz danych umożliwiających kontakt z tą osobą,
- złożone w inny sposób niż za pośrednictwem Internetowego Konta Pacjenta, o którym mowa w art. 7a ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, zamieszcza się w dokumentacji indywidualnej wewnętrznej(...)

trzecią, względem, której wyraża zgodę na przekazywanie jej informacji o jakiejś mowa w art. 9 ust. 3 UoPPiRP.

W dokumentacji indywidualnej wewnętrznej zamieszcza się lub dołącza do niej oświadczenie pacjenta o upoważnieniu do dostępu do dokumentacji, ze wskazaniem imienia i nazwiska osoby upoważnionej⁹⁴, co oznacza, iż pacjent ma prawo wskazać wybraną przez siebie osobę trzecią, którą upoważnia do dostępu do swojej dokumentacji medycznej.

Podmiot informuje pacjenta, przed złożeniem przez niego oświadczeń o możliwości ich złożenia za pośrednictwem Internetowego Konta Pacjenta i skutkach ich złożenia.

W sytuacji kiedy pacjent, przedstawiciel ustawowy pacjenta składa w formie ustnej oświadczenie o upoważnieniu określonej osoby do uzyskiwania dokumentacji, osoba uprawniona po stronie jednostki utrzuwa ww. oświadczenie. Weryfikacja statusu upoważnionego możliwa jest także do dokonania na podstawie okazanego stosownego upoważnienia udzielonego przez pacjenta albo przedstawiciela ustawowego pacjenta. Należy jednak zasygnalizować, iż podmiot nie może żądać przedłożenia upoważnienia w postaci dokumentu urzędowo lub notarialnie potwierdzonego. W rzeczywistości przepisy prawa nie określają szczególnej formy dla oświadczenia zawierającego upoważnienie do dostępu do dokumentacji medycznej, zatem żądanie przedłożenia takiego upoważnienia jako dokumentu potwierdzonego urzędowo lub notarialnie jest niedopuszczalne.

Pacjent ma prawo, nie ma obowiązku wskazania, upoważniania jakiegokolwiek osoby trzeciej. Pamiętać jednak należy, że brak takiego upoważnienia nie jest już odnotowywany w dokumentacji medycznej pacjenta, Rozporządzenie RDM zniosło ten obowiązek.

Złożone oświadczenia zachowują swoją aktualność aż do czasu ich odwołania albo zmiany, nie zachodzi konieczność ponownego ich składania przy następnej wizycie.

⁹⁴ Zgodnie z § 8 ust. 1 pkt. 2) Rozporządzenia RDM „(...) Oświadczenie pacjenta: 1) o upoważnieniu do dostępu do dokumentacji, o którym mowa w art. 26 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, – złożone w inny sposób niż za pośrednictwem Internetowego Konta Pacjenta, o którym mowa w art. 7a ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, zamieszcza się w dokumentacji indywidualnej wewnętrznej (...)”.

Inne uprawnione podmioty.

Zwrócić należy uwagę na treści art. 26 ust. 3 UoPPiRP, który stanowi, iż podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną oprócz wyżej wymienionym osobom uprawnionym także opisanym w treści przepisu organom. Z tego względu jednostki medyczne powinny mieć nie tylko świadomość tego obowiązku udostępniania dokumentacji, ale i umiejętność zastosowania w praktyce przepisu. Niestety często jest zupełnie inaczej. Podmioty skłonne są do realizowania wniosków o udostępnienie dokumentacji bez jakiegokolwiek weryfikacji wnioskodawców, czy to podstaw prawnych do udostępnienia. Często popełniają błąd polegający na tym, iż wnioski składane przez instytucje, traktują tak, jakby nie wymagały one weryfikacji pod kątem ich poprawności.

Wykaz udostępnionej dokumentacji medycznej

Podkreślenia na wstępie wymaga to, iż nie jest prawem, a jest obowiązkiem podmiotu wykonującego działalność leczniczą prowadzić wykaz udostępnionej dokumentacji medycznej. Przepis art. 27 ust. 4 UoPPiRP nie tylko określa ten obowiązek, ale również wskazuje, jakie dane powinny zostać zamieszczone w prowadzonym wykazie.

Zgodnie z brzemieniem tego przepisu, podmiot udzielający świadczeń zdrowotnych prowadzi wykaz zawierający następujące informacje dotyczące udostępnianej dokumentacji medycznej:

- 1) imię (imiona) i nazwisko pacjenta, którego dotyczy dokumentacja medyczna;
- 2) sposób udostępnienia dokumentacji medycznej;
- 3) zakres udostępnionej dokumentacji medycznej;
- 4) imię (imiona) i nazwisko osoby innej niż pacjent, której została udostępniona dokumentacja medyczna, a w przypadkach, o których mowa w art. 26 ust. 3 i 4, także nazwę uprawnionego organu lub podmiotu;
- 5) imię (imiona) i nazwisko oraz podpis osoby, która udostępniła dokumentację medyczną;
- 6) datę udostępnienia dokumentacji medycznej.

Nie tylko udostępnianie dokumentacji medycznej jest obowiązkiem jednostki, ale także zobligowana ona została do prowa-

dzenia wykazu z informacjami dotyczącymi udostępnionej dokumentacji medycznej⁹⁵.

Imię (imiona) i nazwisko pacjenta, którego dotyczy dokumentacja medyczna

Odnotowanie danych identyfikujących pacjenta, którego dokumentacja została udostępniona w wykazie jedynie pozornie jest działaniem prostym. Warto bowiem zauważyć, iż możliwe są przypadki, kiedy mamy do czynienia w ramach jednego podmiotu z kilkoma osobami, które noszą to samo imię i takie samo nazwisko. Oznacza to, iż w takiej sytuacji, sprawdzając w wykazie, czy dokumentacja określonego pacjenta została udostępniona już wcześniej w danym zakresie, możemy dojść do błędnych ustaleń. Błędnych ustaleń, w zakresie tego, czyja, którego pacjenta dokumentacja medyczna została udostępniona. Takie błędne ustalenie, w kontekście udostępniania dokumentacji po raz pierwszy w danym zakresie nieodpłatnie, może wywoływać negatywne skutki. Możemy bowiem błędnie dojść do wniosku, iż w danym zakresie danemu pacjentowi udostępniona została już dokumentacja medyczna nieodpłatnie – a w rzeczywistości takie udostępnienie zrealizowane zostało na rzecz innego pacjenta, który nosi takie samo imię i nazwisko.

W mojej ocenie powyższe stanowi uzasadnienie dla tego, aby równolegle prowadzony był rejestr złożonych wniosków o udostępnienie dokumentacji medycznej. Wnioski bowiem zawierać muszą informacje pozwalające na identyfikację tożsamości pacjenta, którego dane będą udostępnione w następstwie jego złożenia, zatem zawierają one szerszy zakres danych, aniżeli ten ujęty w wykazie, co pozwala na wyeliminowanie problemu błędnego ustalenia tego, czy, kiedy i komu została udostępniona dokumentacja medyczna.

⁹⁵ Błędem powtarzającym się w praktyce jest odnotowywanie w ewidencji tylko i wyłącznie faktu udostępnienia papierowych kopii dokumentacji medycznej, z pominięciem innych form udostępnienia jakie zostały zrealizowane. Najczęściej pomija się odnotowywanie faktu udostępnienia dokumentacji do wglądu, albo wydawania wyników badań.

Sposób udostępnienia dokumentacji medycznej

Obowiązkiem podmiotu jest odnotowanie tego, w jaki sposób doszło do udostępnienia dokumentacji medycznej. Przepis art. 27 UoPPIRP określa sposoby udostępnienia dokumentacji medycznej. Aby w prawidłowo realizować wnioski o udostępnienie dokumentacji medycznej oraz rzetelnie prowadzić wykaz udostępnionej dokumentacji medycznej należy wyjaśnić sobie, jakie są prawem określone sposoby udostępniania dokumentacji medycznej.

Do wglądu

Dokumentacja medyczna może zostać udostępniona do wglądu, w tym także do baz danych w zakresie ochrony zdrowia, w miejscu udzielania świadczeń zdrowotnych, z wyłączeniem medycznych czynności ratunkowych, albo w siedzibie podmiotu udzielającego świadczeń zdrowotnych, z zapewnieniem pacjentowi lub innym uprawnionym organom lub podmiotom, możliwości sporządzenia notatek lub zdjęć. Należy dodać, iż ten sposób udostępnienia dokumentacji medycznej powinien być realizowany przy wykorzystaniu środków technicznych, osobowych gwarantujących zabezpieczenie dokumentacji medycznej.

W postaci wyciągu, odpisu, kopii, wydruku

Dokumentacja medyczna może być udostępniana także przez sporządzenie jej wyciągu, odpisu, kopii lub wydruku.

Wyciąg to skrótowy dokument zawierający wybrane informacje lub dane z całości dokumentacji medycznej.

Odpis to dokument wytworzony przez przepisanie tekstu z oryginału dokumentacji medycznej z wiernym zachowaniem zgodności co do treści z oryginałem.

Kopia to dokument wytworzony przez odwzorowanie oryginału dokumentacji medycznej, w formie kserokopii albo odwzorowania cyfrowego (skanu). Warto zauważyć iż zgodnie z definicją przez kopie rozumie się nie tylko kserokopię utrwaloną na papierze, ale też kopia może mieć postać cyfrowego odwzorowania tj. skanu dokumentu zapisanego w postaci elektronicznej.

Wydanie oryginału za potwierdzeniem odbioru

Dokumentacja medyczna może być także udostępniana przez wydanie oryginału za potwierdzeniem odbioru i z zastrzeżeniem zwrotu po wykorzystaniu, na żądanie organów władzy publicznej albo sądów powszechnych, a także w przypadku gdy zwłoka w wydaniu dokumentacji mogłaby spowodować zagrożenie życia lub zdrowia pacjenta.

Należy zasygnalizować, iż doszło do ograniczenia sytuacji, w których może mieć miejsce udostępnianie oryginału dokumentacji medycznej, względem uprzednio obowiązującej regulacji w tym zakresie⁹⁶. W obecnym stanie prawnym oryginał dokumentacji medycznej może być udostępniony wyłącznie w przypadku, gdy z wnioskiem wystąpi organ administracji publicznej albo sąd powszechny, oraz wyłącznie w przypadkach, gdy zwłoka w wydaniu dokumentacji medycznej w inny sposób, mogłaby spowodować zagrożenie życia lub zdrowia pacjenta. Właśnie ze względu na upływ czasu - z jednej strony i potrzebę konsultacji, czy rozpoznania historii choroby pacjenta, która możliwa będzie do wykonania w drodze analizy oryginału całej jego dokumentacji medycznej - z drugiej strony, zostało dopuszczone udostępnienie dokumentacji medycznej poprzez wydanie jej oryginału za potwierdzeniem odbioru i z zastrzeżeniem zwrotu. Jednostki muszą jednak pamiętać, o tym, iż w przypadku udostępnienia dokumentacji poprzez wydanie oryginału za potwierdzeniem odbioru, są zobowiązane do pozostawienia kopii tej dokumentacji lub jej pełnego odpisu w swoim posiadaniu. Takie rozwiązanie ma minimalizować negatywne skutki utraty dokumentacji, w związku z jej nie zwróceniem, przez podmiot któremu została udostępniona w oryginale. Na marginesie warto odnotować, iż zdjęcia rentgenowskie wykonane na kliszy, również podlegają udostępnieniu za potwierdzeniem odbioru z zastrzeżeniem ich zwrotu po wykorzystaniu

⁹⁶ Ustawa z dnia 23 marca 2017 r. o zmianie ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz niektórych innych ustaw (Dz. U. 2017 r., poz. 836), weszła w życie 11 maja 2017 r., i wprowadziła w art. 27 UoPPiRP całościową regulację, dotyczącą sposobów udostępniania dokumentacji medycznej. Jedną ze zmian było ograniczenie wydawania oryginałów dokumentacji medycznych oraz jednoznaczne i jak najbardziej precyzyjne określenie tych sytuacji, w jakich dopuszczalne jest udostępnienie dokumentacji poprzez wydanie jej oryginału. Przed ww. nowelizacją, każdy upoważniony podmiot mógł żądać wydania dokumentacji medycznej w oryginale.

Za pośrednictwem środków komunikacji elektronicznej. Na informatycznym nośniku danych Środki komunikacji elektronicznej

Dokumentacja medyczna może być udostępniana także za pośrednictwem środków komunikacji elektronicznej oraz na informatycznym nośniku danych.

Środki komunikacji elektronicznej to rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumiewanie się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi, a w szczególności poczta elektroniczna⁹⁷. Pod pojęciem środków komunikacji elektronicznej kryją się nie tylko rozwiązania techniczne w postaci poczty elektronicznej (e-mail) chociaż najbardziej popularnej, mogą to być także innego rodzaju komunikatory, czy rozwiązania programowe umożliwiające przy wykorzystaniu transmisji danych przekazywanie dokumentacji medycznej⁹⁸. Prawidłowym rozwiązaniem przy udostępnianiu dokumentacji medycznej będzie jej przesyłanie w postaci zaszyfrowanych plików zabezpieczonych hasłem z jednoczesnym dostarczeniem adresatowi samego

⁹⁷ Ustawa z 18 lipca 2002 r., o świadczeniu usług drogą elektroniczną (Dz. U. z 2002r., Nr 144, poz. 1204 ze zm.).

⁹⁸ Warto nadmienić, iż w sytuacji, w której podmiot zdecyduje się na udostępnianie dokumentacji medycznej za pośrednictwem środków komunikacji elektronicznej, z jednej strony zobligowany jest uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, z drugiej strony zmuszony jest do takiego ukształtowania swojego działania, aby nie narazić się na odpowiedzialność z tytułu stosowania niedozwolonych praktyk naruszających zbiorowe prawa pacjentów. Za wątpliwe zatem uznać należałoby rozwiązanie zakładające udostępnianie dokumentacji medycznej za pośrednictwem środków komunikacji elektronicznej, z ograniczeniem do stosowania tylko i wyłącznie w zakresie wymiany informacji z wykorzystaniem profilu ePUAP, a tym samym z ograniczeniem stosowania korespondencji w postaci elektronicznej (e-mail) w innej formie. Z tego względu za zasadne i celowe uznać należy, takie ukształtowanie zasad, aby z jednej strony nie stanowiło naruszenia praw zbiorowych pacjentów, a z drugiej gwarantowało bezpieczeństwo danych. Z tego względu każdy przypadek należy traktować indywidualnie, z należytą starannością i dokładnością, pamiętając o przesłankach koniecznych do spełnienia dla realizacji dyspozycji w zakresie udostępnienia dokumentacji medycznej.

hasła odrębnym kanałem informacyjnym. Dla przykładu wysyłamy plik zaszyfrowany zabezpieczony hasłem za pośrednictwem poczty email, ale hasło podajemy adresatowi bezpośrednio przesyłając je SMS na wskazany numer telefonu. Taką funkcjonalność zapewnia dla przykładu dostępny na rynku program RODO Sender⁹⁹.

Należy zastrzec jednak, iż dokumentacja medyczna prowadzona w postaci papierowej może być udostępniona przez sporządzenie kopii w formie odwzorowania cyfrowego (skanu) i następnie może być przekazana do wnioskodawcy z wykorzystaniem środków komunikacji elektronicznej, albo na informatycznym nośniku danych, jeżeli przewiduje to regulamin organizacyjny podmiotu udzielającego świadczeń zdrowotnych. Oznacza to, iż jednostka w regulaminie organizacyjnym musi wprost przewidywać taki sposób udostępniania dokumentacji medycznej prowadzonej w postaci papierowej, aby było to możliwe, aby można było od niej tego wymagać. Nie będzie zatem obowiązkiem jednostki udostępnianie dokumentacji medycznej prowadzonej w postaci papierowej, w postaci kopii w formie odwzorowania cyfrowego (skanu), jeśli jej regulamin organizacyjny, nie przewiduje takiej formy udostępniania dokumentacji medycznej, czyli za pośrednictwem środków komunikacji elektronicznej lub na informatycznym nośniku danych. Zapamiętać należy, iż udostępnianie dokumentacji medycznej prowadzonej w postaci papierowej za pośrednictwem środków komunikacji elektronicznej lub na informatycznym nośniku danych ma fakultatywny charakter dla podmiotu, który może a nie musi wprowadzić takiej możliwości w swoim regulaminie organizacyjnym.

Naturalnie w sytuacji prowadzenia dokumentacji medycznej w postaci elektronicznej, taka zależność nie obowiązuje. Obowiązek jej udostępniania występuje bez względu na zapisy dokonane w regulaminie organizacyjnym podmiotu.

Informatyczny nośnik danych.

Informatyczny nośnik danych jest to materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych

⁹⁹ Program do automatycznego szyfrowania załączników do email oraz przesyłania hasła dostępowego za pośrednictwem SMS do adresata. www.rodosender.pl

w postaci cyfrowej¹⁰⁰. Oznacza to, iż udostępniana dokumentacja medyczna, powinna zostać zapisana w formie cyfrowej na informatycznym nośniku danych, który oprócz funkcjonalności zapisu charakteryzować musi się także funkcjonalnością polegającą na zdolności przechowywania zapisanych danych oraz możliwością ich odczytywania. Przykładowymi informatycznymi nośnikami danych mogą być: pamięć komputera, pamięci dyskowe, urządzenia pamięciowe USB, płyty CD, DVD. Wraz z rozwojem technologii zmieniają się także rodzaje nośników danych, jedne zastępowane są innymi.

Zakres udostępnionej dokumentacji medycznej.

W wykazie udostępnionej dokumentacji medycznej odnotowuje się również zakres udostępnionej dokumentacji medycznej. Obowiązkiem jednostki jest odnotowanie tego, w jakim zakresie udostępniona została dokumentacja medyczna. Zakresem wniosku o udostępnienie dokumentacji, jak i zakresem, który odnotowany zostanie w wykazie, będą rodzajowo wskazane dokumenty zgromadzone w ramach dokumentacji medycznej, ale będą też dokumenty tworzące dokumentację medyczną powstałą w określonym czasie, lub utworzone przez wskazane np. poradnie, oddziały podmiotu udostępniającego. Precyzyjne określenie zakresu wymaga skrupulatności, ale jednocześnie daje nam możliwość weryfikowania, czy już poprzednio w danym zakresie dokumentacja była udostępniana nieodpłatnie – co z kolei otwierać będzie droga do naliczenia opłaty w przypadku ponownego udostępniania dokumentacji w tym samym zakresie.

Imię (imiona) i nazwisko osoby innej niż pacjent.

W wykazie zamieszcza się wpis wskazujący na imię (imiona) i nazwisko osoby innej niż pacjent, której została udostępniona dokumentacja medyczna, a w przypadkach, udostępnienia uprawnionemu organowi lub podmiotowi zamieszcza się informacje w postaci ich nazwy. Nie jest błędem, jeśli w wykazie umieszczone zostaną informacje nt. udostępnień realizowanych bezpośrednio na wniosek pacjenta i to jego imię (imiona) i nazwisko zostanie ujęte w wykazie,

¹⁰⁰ Ustawa z dnia 17 lutego 2005 r., o informatyzacji działalności podmiotów realizujących zadania publiczne (D z. U. z 2005r., Nr 64, poz. 565 ze zm.).

pomimo iż przepis tego nie przewiduje. Szerzej o tym pisać będziemy omawiając zagadnienie udostępniania dokumentacji medycznej nieodpłatnie po raz pierwszy w danym zakresie.

Imię (imiona) i nazwisko oraz podpis, osoby która udostępniła dokumentację medyczną

W wykazie zamieszcza się wpis wskazujący na imię (imiona) i nazwisko oraz podpis osoby, która udostępniła dokumentację medyczną. Odnotowuje się w wykazie nie tylko imię (imiona) i nazwisko osoby której udostępniono dokumentację wskazanego pacjenta, ale także zamieszcza się w nim imię (imiona) i nazwisko osoby, która udostępniła dokumentację medyczną oraz dodatkowo osoba taka składa swój własnoręczny podpis w wykazie prowadzonym w postaci papierowej. Podpis osoby, która udostępniła dokumentację medyczną, istotny jest z punktu widzenia dowodowego w przypadku konieczności rozstrzygnięcia ewentualnych kwestii spornych¹⁰¹.

Podpis może mieć charakter podpisu własnoręcznego złożonego w wykazie prowadzonym w postaci papierowej. Podpis jednak może mieć także postać podpisu składanego w postaci cyfrowej w przypadku prowadzenia wykazu w takiej właśnie formie. Złożenie podpisu, podpisanie wykazu, samo w sobie jest czynnością, którą należy odróżnić od czynności sprowadzającej się do wypełnienia wykazu określonymi w przepisie kategoriami danych. W mojej ocenie wymuszać to będzie takie skonstruowanie procedury składania podpisu w postaci cyfrowej, aby oprócz uzupełnienia wykazu o imię (imiona) i nazwisko udostępniającego dokumentację medyczną, dochodziło do zweryfikowania, uwierzytelnienia podpisu przy wykorzystaniu wewnętrznych mecha-

¹⁰¹ Jednostki skłonne są do uzupełniania wykazu o dodatkowe pola, które traktują jako obowiązkowe, np. nakazują uprawnionemu złożenie własnoręcznego podpisu potwierdzającego odbiór udostępnianej mu dokumentacji medycznej, warunkując tym jej wydanie. Jest to działanie, które nie znajduje swojego oparcia w przepisach i uznać należy je za niedopuszczalne. Takie wprowadzanie dodatkowego warunku dla udostępnienia dokumentacji medycznej jest bowiem niedopuszczalne. Warto także zasygnalizować, iż w sytuacji, kiedy złożenie podpisu nie jest warunkiem wydania dokumentacji, składający podpis kolejny odbierający dokumentację ma możliwości rozpoznania tego, kto przed nim odebrał lub po nim będzie odbierał przygotowaną dokumentację medyczną, co również przemawia za niedopuszczalnością takiego rozwiązania.

nizmów systemu teleinformatycznego podmiotu. Podpis zatem musi być możliwy do zweryfikowania przy wykorzystaniu wewnętrznych mechanizmów systemu teleinformatycznego podmiotu¹⁰².

Data udostępnienia dokumentacji medycznej

W wykazie zamieszcza się wpis wskazujący na datę udostępnienia dokumentacji medycznej. Takie adnotacje pozwolą na weryfikację poprawności realizacji procesu udostępniania dokumentacji medycznej w zakresie terminowości działania.

Praktyczne porady dotyczące

wykazu udostępnionej dokumentacji medycznej

Po raz pierwszy czy po raz kolejny udostępniono

Zgodnie z dyspozycją przepisu art. 28 ust. 2a UoPPiRP cyt.: „(...) opłaty (...) nie pobiera się w przypadku udostępnienia dokumentacji medycznej: (...) po raz pierwszy w żądanym zakresie (...)”, co oznacza, iż koniecznością stanie się dokonywanie weryfikacji tego, czy uprawniony po raz pierwszy, czy po raz już kolejny, występuje z wnioskiem o udostępnienie dokumentacji medycznej. Odnotowanie takiego udostępnienia, które realizowane jest po raz pierwszy w żądanym zakresie, pozwoli na pobranie opłaty, w sytuacji złożenia wniosku w analogicznym zakresie w późniejszym terminie. Aby było

¹⁰² Zgodnie z § 10 ust. 1 pkt 3 lit. 3 Rozporządzenia RDM cyt.: „(...) dokumentacja indywidualna, jeżeli przepisy rozporządzenia nie stanowią inaczej, zawiera (...) oznaczenie osoby udzielającej świadczeń zdrowotnych oraz osoby kierującej na badanie diagnostyczne, konsultację lub leczenie: (...) podpis (...)”. Zgodnie z § 10 ust. 2 Rozporządzenia RDM cyt.: „(...) w przypadku dokumentacji prowadzonej w postaci elektronicznej podpis, o którym mowa w ust. 1 pkt 3 lit. e, może być złożony oraz zweryfikowany przy wykorzystaniu wewnętrznych mechanizmów systemu teleinformatycznego, o którym mowa w § 80 (...)”. Przepis określa warunki, jakie powinny zostać spełnione przy składaniu podpisu w dokumentacji medycznej dopuszczając do wykonania ww. czynności wykorzystanie wewnętrznego systemu teleinformatycznego, który odpowiada określonym wymaganiom, jak i daje możliwość złożenia oraz zweryfikowania podpisu. Jeśli zatem ustawodawca dopuszcza taki mechanizm weryfikacji podpisu składanego jednak w dokumentacji medycznej to tym bardziej za uprawnione uznać należy posługiwanie się analogiczną metodologią w odniesieniu do podpisu, który znajdzie się w wykazie udostępnionej dokumentacji medycznej.

jednak możliwe dokonanie takiej oceny i zamieszczenie w wykazie takiej adnotacji warto jest dokonywać precyzyjnych zapisów określających zakres udostępnianej dokumentacji.

Skrupulatnie odnotowany zakres udostępnionej dokumentacji

Skrupulatne odnotowywania zakresów udostępnionej dokumentacji medycznej, służyć ma ustalaniu tego, czy wniosek w danym zakresie został już wcześniej zrealizowany, czy też nie. Innymi słowy, czy uprzednio doszło do udostępnienia dokumentacji medycznej bez opłaty w danym zakresie, czy jeszcze nie¹⁰³.

Ewidencja wniosków o udostępnienie dokumentacji medycznej

Wprowadzenie ewidencjonowania przyjmowanych i obsługiwanych wniosków o udostępnienie dokumentacji medycznej, jest również rozwiązaniem organizacyjnym, które usprawniać będzie proces udostępniania. Taka ewidencja wniosków uzupełniać będzie prowadzony wykaz udostępnionej dokumentacji. Naturalnie nie oznacza, to iż podmiot realizował będzie tylko te wnioski, które zostały zapisane przyjęte do ewidencji, nie może to być dodatkowy element warunkujący udostępnienie dokumentacji medycznej.

Osobiście odebrana dokumentacja medyczna

Z uwagi na fakt, iż nie pobiera się opłaty od pacjenta w przypadku udostępnienia dokumentacji medycznej po raz pierwszy w żądanym zakresie, warto jest odnotowywać w prowadzonym wykazie status takich udostępnień. Co prawda sam wykaz nie przewiduje konieczności odnotowywania faktu udostępnienia w nim dokumentacji medycznej pacjenta jemu samemu, jednak wprowadzenie powinności takiego odnotowywania pozwoli na dokonywanie weryfikacji, w sytuacji wystąpienia przez pacjenta z kolejnymi wnioskami, tego, czy jest to, czy też nie jest pierwszy wniosek o udostępnienie dokumentacji w danym zakresie.

¹⁰³ Wskazać jednak należy, iż w sytuacji podjęcia decyzji przez podmiot, iż w ogóle nie będzie on pobierał opłat za udostępnienie dokumentacji medycznej, nie zwalnia go to z obowiązku prowadzenia ewidencji (wykazu) udostępnionej dokumentacji z prawidłowo odnotowanym zakresem udostępnienia.

Kopia danych osobowych

Warto także zaprowadzić ewidencję wniosków złożonych w trybie art. 15 ust. 3 Rozporządzenia RODO oraz analogiczny wykaz udostępnień zrealizowanych na ich podstawie, co pozwoli na sprawne administrowanie wnioskami i udostępnianymi danymi.

Oплата za udostępnienie dokumentacji medycznej

Tytułem wprowadzenia warto przypomnieć, iż zgodnie z art. 28 ust. 1 UoPPiRP „(...) **za udostępnienie dokumentacji medycznej w sposób określony w art. 27 ust. 1 pkt 2 i 5 oraz w ust. 3 podmiot udzielający świadczeń zdrowotnych może pobierać opłatę (...)**” co oznacza tyle, iż podmiot realizujący swoje obowiązki w związku z uprawnieniami pacjentów, do dostępu do dokumentacji medycznej, może pobierać, nie musi, ale może pobierać opłatę:

- a) za udostępnienie dokumentacji medycznej przez sporządzenie jej wyciągu, odpisu, kopii, wydruku,
- b) za udostępnienie na informatycznym nośniku danych,
- c) za udostępnienie przez sporządzenie kopii w formie odwzorowania cyfrowego [skanu] i przekazanie za pośrednictwem środków komunikacji elektronicznej, albo na informatycznym nośniku danych.

Wysokość odpłatności, sposób określenia oraz podania do informacji w podmiocie

Opłatę za udostępnienie dokumentacji medycznej ustala podmiot udzielający świadczeń zdrowotnych¹⁰⁴ co oznacza, iż to na podmiocie udostępniający spoczywa obowiązek ustalenia wysokości opłaty, za udostępnienie dokumentacji medycznej. Maksymalna wysokość opłaty za:

- 1) jedną stronę wyciągu albo odpisu dokumentacji medycznej – nie może przekraczać 0,002,
- 2) jedną stronę kopii albo wydruku dokumentacji medycznej – nie może przekraczać 0,00007,

¹⁰⁴ Zgodnie z art. 27 ust. 3 UoPPiRP „(...) opłatę za udostępnienie dokumentacji medycznej (...) ustala podmiot udzielający świadczeń zdrowotnych (...)”

- 3) udostępnienie dokumentacji medycznej na informatycznym nośniku danych – nie może przekraczać 0,0004 – przeciętnego wyngrodzenia w poprzednim kwartale, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” na podstawie art. 20 pkt 2 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, począwszy od pierwszego dnia miesiąca następującego po miesiącu, w którym nastąpiło ogłoszenie.

Powyższe jednoznacznie wskazuje na brak dowolności jednostki przy określaniu maksymalnej wysokości stawek za udostępnienie dokumentacji medycznej. Jednostki bowiem zobowiązane są do stosowania ww. zasad¹⁰⁵

¹⁰⁵ Za nieprawidłową uznać należy praktykę, pobierania dodatkowych opłat za uwierzytelnianie tworzonych kopii, udostępnianej dokumentacji medycznej, czy jej odpisów, czyli za tzw. potwierdzanie jej „za zgodność z oryginałem”. Zgodnie z Wyrokiem z 31 stycznia 2018r. Wojewódzkiego Sądu Administracyjnego w Warszawie (VII SA/Wa 2720/17) cyt.: „(...) *poświadczenie za zgodność z oryginałem kopii dokumentacji medycznej, nie zmienia jej charakteru, bowiem w świetle zapisów ustawy, może być ona traktowana wyłącznie jako kopia. W ustawie nie przewidziano bowiem kopii poświadczonych za zgodność z oryginałem (...) w konsekwencji skarżący nie był uprawniony do pobrania opłat wyższych niż maksymalne kwoty określone w art. 28 ust 4 pkt 2 ustawy (...)*”. Podobnie za niedopuszczalne uznać należy pobieranie opłat dodatkowych za tzw. przygotowanie dokumentacji medycznej do udostępnienia, w praktyce czynności te nazywane są „czynnościami administracyjnymi”. W odniesieniu za pobieranie opłaty z tytułu wysyłki zgodnie z Wyrokiem Naczelnego Sądu Administracyjnego z dnia 04 grudnia 2018 r., (II OSK 3024/18) cyt.: „(...) *pobieranie opłaty za przesyłkę dokumentacji medycznej pocztą nie może przekraczać poniesionej opłaty ustalonej przez operatora pocztowego. Pobieranie wyższej opłaty jest działaniem bezprawnym (...)*”, co oznacza, iż naliczana wartość opłaty z tytułu realizacji wysyłki powinna być zindywidualizowana oraz stanowić ekwiwalent do poniesionych kosztów. Zgodnie z Wyrokiem Naczelnego Sądu Administracyjnego z dnia 10 kwietnia 2018 r. (II OSK 3194/17) cyt.: „(...) *wprowadzenie regulacji uzależniającej udostępnienie dokumentacji medycznej od uiszczenia opłaty przed wykonaniem czynności udostępnienia dokumentacji medycznej jest związane z ceną usługi, nie stanowi naruszenia praw pacjenta. Jest to związane z przyjęciem dopuszczalności obciążenia pacjentów kosztami tego rodzaju usług (...)*”, co oznacza, iż dopuszczalne wprowadzenie rozwiązania zakładającego udostępnienie dokumentacji medycznej dopiero po uzyskaniu płatności za tę czynność.

Obowiązek informowania o wysokości stawek opłat

Podmiot wykonujący działalność leczniczą, który podejmie decyzję o pobieraniu opłaty za udostępnianie dokumentacji medycznej zobowiązany jest do umieszczenia w swoim regulaminu organizacyjnego informacji o wysokości opłat za udostępnienie dokumentacji medycznej oraz po dokonaniu wyliczenia wartości konkretnych stawek do ich podania w widoczny sposób w miejscu udzielania świadczeń, na stronie internetowej i w Biuletynie Informacji Publicznej, w przypadku podmiotu obowiązany do jego prowadzenia¹⁰⁶.

Opłaty nie pobiera się za pierwszy wniosek w danym zakresie

Zwolnień z obowiązku ponoszenia odpłatności za udostępnienie dokumentacji jest kilka. Skupimy jednak swoją uwagę na ostatniej nowelizacji przepisów UoPPiRP. Jednostka nie może pobrać opłaty, za udostępnienie dokumentacji medycznej od pacjenta, przedstawiciela ustawowego pacjenta, od osoby upoważnionej przez pacjenta, czy przedstawiciela ustawowego pacjenta¹⁰⁷, udostępniając dokumentację

¹⁰⁶ Zgodnie z art. 24 ust. 1 pkt 9) Ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej „(...) w regulaminie organizacyjnym podmiotu wykonującego działalność leczniczą określa się w szczególności: (...) wysokość opłaty za udostępnienie dokumentacji medycznej ustalonej w sposób określony w art. 28 ust. 4 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (...)”

Zgodnie z art. 24 ust 2 Ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej „(...) aktualne informacje, o których mowa w ust. 1 pkt (...) 9 (...), podaje się do wiadomości pacjentów przez ich wywieszenie w widoczny sposób w miejscu udzielania świadczeń oraz na stronie internetowej podmiotu wykonującego działalność leczniczą i w Biuletynie Informacji Publicznej, w przypadku podmiotu obowiązany do jego prowadzenia (...)”.

¹⁰⁷ Literalne brzmienie treści przytoczonej normy prawnej prowadzi do konkluzji, iż ustawodawca dokonał zmiany kręgu uprawnionych do bezpłatnej dokumentacji medycznej, wykluczając z niego osoby upoważnione przez pacjenta i przedstawiciela ustawowego. Wywołało to dyskusję, które doprowadziły do rozbieżnych stanowisk w temacie. Mając na uwadze powyższe kontrowersje Ministerstwo Zdrowia zajęło stanowisko [Pismo z dnia 17 lipca 2019r. [EZP. 024.15.2019.EW] cyt.: „(...) w nawiązaniu do (...) korespondencji w sprawie dostępu do dokumentacji medycznej, uprzejmie informuję, iż z Rzecznikiem Praw Pacjenta została wypracowana wspólna interpretacja art. 28 ust. 2a pkt 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2019 r. poz. 1127, z późn.zm.). Upoważnienie do dokumentacji jest elementem prawa pacjenta do dokumentacji medycznej (...) przyjęta regulacja ma zagwarantować pacjentowi, że nie pobiera się od niego opłaty za pierwsze żądanie udostępnienia dokumentacji – bez względu na to, czy żądanie to kieruje do

medyczną pacjenta po raz pierwszy w żądanym przez uprawnione osoby zakresie przez sporządzenie jej wyciągu, odpisu, kopii, wydruku, na informatycznym nośniku danych, a w przypadku dokumentacji medycznej prowadzonej w postaci papierowej, przez sporządzenie kopii w postaci odwzorowania cyfrowego (skanu) i przekazanie za pośrednictwem środków komunikacji elektronicznej, albo na informatycznym nośniku danych¹⁰⁸.

Zwrócić należy uwagę, iż określony „sposób udostępnienia dokumentacji medycznej” to jest inne pojęcie niż „zakres udostępnionej dokumentacji medycznej”, przez co udostępnienie dokumentacji medycznej choćby, w jednym ze sposobów np. wydanie kopii, pozbawiać będzie wnioskodawcę prawa do ponownego pozyskania nieodpłatnie w opisywanym trybie, dokumentacji medycznej, w analogicznym zakresie a jedynie w inny niż uprzednio sposób, np. przez wydanie wydruku – albowiem w tym samym zakresie a jedynie w inny sposób dokumentacja wnioskodawcy została już udostępniona

Rzeczą naturalną jest, iż zakresy wnioskowanej do udostępnienia dokumentacji medycznej określane w kolejnych wnioskach przez wnioskodawcę, mogą ulegać zmianom. Jednak zmiana polegająca na zawężeniu zakresu, w kolejnym wniosku, względem wniosku już zrealizowanego, nie będzie oznaczać, iż wniosek traktować należy jako złożony po raz pierwszy w żądanym zakresie, de facto bowiem

podmiotu udzielającego świadczeń zdrowotnych sam, czy też przez osobę upoważnioną/ppełnomocnika. Tym bardziej bez znaczenia pozostaje fakt, czy osoba działająca w jego imieniu opiera się na upoważnieniu regulowanym w ustawie o prawach pacjenta czy na pełnomocnictwie regulowanym w kodeksie cywilnym. Odmienne interpretacja powodowałaby dla osób z niepełnosprawnościami czy osób niesamodzielnych, które nie zawsze mają przedstawiciela ustawowego, trudności w realizacji prawa do dokumentacji medycznej. Z wykonywaniem zaś tego prawa łączy się prawo upoważniania innych osób. Stąd też jedynym kryterium jest w tym przypadku to, czy pacjent korzysta z uprawnienia w przedmiocie dostępu do dokumentacji po raz pierwszy w żądanym zakresie oraz formie (...)” co oznacza tyle, iż wspólna interpretacja wyrażona w stanowisku RPP, wskazuje wprost, iż uprawnienie do zwolnienia z opłaty z tytułu udostępnienia dokumentacji medycznej w danym zakresie po raz pierwszy odnosi się także do osób pełnomocników, jak i do osób upoważnionych na gruncie UoPPiRP.

¹⁰⁸ Zgodnie z dyspozycją przepisu art. 28 ust. 2a pkt. 1) UoPPiRP, cyt.: „(...) *opłaty (...), nie pobiera się w przypadku udostępnienia dokumentacji medycznej: (...) pacjentowi albo jego przedstawicielowi ustawowemu po raz pierwszy w żądanym zakresie i w sposób, o którym mowa w art. 27 ust. 1 pkt 2 i 5 oraz ust. 3 (...)*”

taki żądany zakres dokumentacji medycznej został już udostępniony wnioskodawcy uprzednio bezpłatnie.

Wniosek o udostępnienie dokumentacji medycznej

Żądanie zgłoszone przez wnioskodawcę w zakresie udostępnienia dokumentacji medycznej uruchamia procedurę czynności ukierunkowanych na realizację obowiązków jednostki związanych z udostępnianiem dokumentacji. Z tego względu ważne jest, aby jednostka w sposób odpowiedzialny i rzetelny zarządzała procesem obsługi takich wniosków.

Forma wniosku o udostępnienie dokumentacji medycznej

Przepisy UoPPiRP nie określają, ani sposobu, ani formy, w jakiej żądanie udostępnienia dokumentacji medycznej powinno zostać wyrażone, aby było wiążące dla podmiotu, co oznacza, iż wniosek zawierający takie żądanie może być złożony zarówno:

- a) w formie pisemnej,
- b) w formie ustnej;
- c) w formie elektronicznej.

Prawidłową praktyką jest posługiwanie się wzorami wniosków o udostępnienie dokumentacji medycznej, jednak pełnią one rolę jedynie formularzy o charakterze pomocniczym i fakultatywnym¹⁰⁹. Stosowanie takiego formularza upraszcza uprawnionemu wyrażenie swojego oświadczenia woli i jednocześnie precyzuje jego zakres, co

¹⁰⁹ Zgodnie z Wyrokiem Naczelnego Sądu Administracyjnego z dnia 04 grudnia 2018 r. (II OSK 3024/18) cyt.: „(...) wprowadzenie regulacji formy złożenia żądania udostępnienia dokumentacji medycznej stanowi naruszenie zbiorowych praw pacjenta. Wybór formy żądania, w tym podstawowej – formy ustnej – należy do pacjenta (...), co oznacza iż podmiot udostępniający dokumentację medyczną nie może uzależnić realizacji swojego obowiązku od dochowania określonej i wskazanej formy wniosku. Zgodnie z Wyrokiem Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 01 września 2015 r. (VII SA/Wa 1189/14) cyt.: „(...) ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta nie uzależnia ważności lub skuteczności upoważnienia do dokumentacji medycznej od wymogu innej formy szczególnej, a nawet wymogu formy pisemnej. Oznacza to, że przedmiotowe upoważnienie może być udzielone nawet ustnie np. w obecności lekarza. Negowanie ważności pisemnego upoważnienia do dokumentacji medycznej i stawianie wymogu formy aktu notarialnego wbrew brzmieniu ustawy jest bezzasadne i niedopuszczalne (...)”.

ma istotne znaczenie z punktu widzenia realizacji takiego wniosku przez podmiot¹¹⁰.

W sytuacji złożenia żądania w formie ustnej, za zasadne i celowe uznać należy jego odnotowanie przez personel podmiotu, z uwzględnieniem wszystkich niezbędnych danych pozwalających na realizację żądania, oraz złożeniem adnotacji potwierdzającej fakt, dokonania odnotowania takiego żądania.

Dane zawarte we wniosku

Żądanie wnioskodawcy powinno umożliwiać jednoznaczne określenie:

- a) tożsamości wnioskodawcy;
- b) nazwy uprawnionego organu albo podmiotu wnioskującego;
- c) podstawy prawnej;
- d) tożsamości pacjenta którego dokumentacja medyczna ma zostać udostępniona;
- e) sposobu udostępnienia dokumentacji medycznej;
- f) zakresu udostępnienia dokumentacji medycznej;
- g) daty złożenia wniosku¹¹¹.

W sytuacji konieczności doprecyzowania, uzupełnienia wniosku, podmiot udostępniający uprawniony jest do wystąpienia do składającego żądanie ze stosownym zapytaniem, wnioskiem o doprecyzowanie swojego żądania, poprzez przekazanie oczekiwanych informacji¹¹².

¹¹⁰ Za nieuprawnione uznać należy praktyki sprowadzające się do ograniczania możliwości składania wniosków o udostępnienie dokumentacji medycznej do wyznaczonych godzin. Zgodnie z Wyrokiem Naczelnego Sądu Administracyjnego z dnia 04 grudnia 2018 r. (II OSK 3024/18) cyt.: „(...) podmiot udzielający świadczeń zdrowotnych obowiązany jest tak zorganizować swoją praktykę, aby pacjent mógł otrzymać dokumentację medyczną bez zbędnej zwłoki. W przypadkach szczególnych związanych z ochroną życia pacjenta, podmiot udzielający świadczeń zdrowotnych powinien stworzyć możliwość udostępnienia dokumentacji medycznej bez ograniczenia czasowego. Pozbawienie takiej możliwości narusza prawa pacjenta (...)”.

¹¹¹ Wskazać należy, iż obecnie obowiązujące przepisy nie dają możliwości warunkowania udostępnienia dokumentacji medycznej po uprzednim określeniu celu, w jakim żądanie zostało zgłoszone przez pacjenta, jego przedstawiciela ustawowego bądź osobę upoważnioną.

¹¹² Warto zwrócić tutaj uwagę na występujące w praktyce problemy związane z brakiem możliwości ustalenia tożsamości pacjenta, którego dokumentacja ma zostać udostępniona, czy też ustalenia tożsamości wnioskodawcy, których ustalenie jest

Wskazać należy, iż obecnie obowiązujące przepisy nie dają możliwości warunkowania udostępnienia dokumentacji medycznej od uprzedniego wskazania celu, w jakim żądanie udostępnienia zostało zgłoszone przez pacjenta, jego przedstawiciela ustawowego bądź osobę upoważnioną.

Ustalenie tożsamości jako warunek bezwzględny dla udostępnienia dokumentacji medycznej

Elementem koniecznym dla realizacji wniosku o udostępnienie dokumentacji medycznej, zgodnie z jego kierunkiem, jest bezwzględne ustalenie tożsamości, zarówno osoby pacjenta, którego dokumentacja dotyczy, jak i osoby wnioskodawcy. Za zabronione uznać należy udostępnianie dokumentacji medycznej osób, których tożsamości nie udało się potwierdzić bez wątpliwości, jak i osobom, których tożsamości a w konsekwencji uprawnienia do powyższego nie można zweryfikować.

Weryfikacji tożsamości dokonuje się poprzez kontrolę okazanego dokumentu tożsamość zawierającego co najmniej zdjęcie, imię i nazwisko oraz PESEL¹¹³ lub w przypadku jego braku inny numer jednoznacznie identyfikujący pacjenta. Dokumentem potwierdzającym tożsamość jest w szczególności:

- a) dowód osobisty;
- b) paszport;
- c) prawo jazdy;
- d) legitymacja szkolna;
- e) karta pobytu¹¹⁴;

warunkiem koniecznym realizacji wniosku, w następstwie ograniczenia się we wniosku do podawania przez wnioskodawców jedynie imienia i nazwiska, z pominięciem dodatkowych informacji. Bez doprecyzowania żądania poprzez uzupełnienie go przez wnioskodawcę o dane umożliwiające identyfikację tożsamości jego, czy też tożsamości pacjenta, udostępnienie dokumentacji jest niemożliwe i obarczone ryzykiem przekazania jej nieuprawnionemu.

¹¹³ Zgodnie z art. 15 ust. 2 Ustawy z 24 września 2010 r. o ewidencji ludności (Dz. U. z 2018 r. poz. 1382 ze zm.) cyt.: „(...) numer PESEL jest to jedenastocyfrowy symbol numeryczny, jednoznacznie identyfikujący osobę fizyczną, zawierający datę urodzenia, numer porządkowy, oznaczenie płci oraz liczbę kontrolną (...)”.

¹¹⁴ Karta pobytu, o której mowa w Ustawie z dnia 12 grudnia 2013 r. o cudzoziemcach (Dz. U. poz. 1650, ze zm.) – w przypadku osoby, która uzyskała

- f) dokument podróży¹¹⁵
g) lub inny dokument urzędowy ze zdjęciem.

Podmiot może utrwalić informację o dacie dokonania weryfikacji tożsamości oraz rodzaju dokumentu na podstawie którego została ona dokonana.

Jeśli okazanie dokumentu tożsamości jest niemożliwe lub utrudnione, bądź sytuacja stanu faktycznego stanowi uzasadnienie dla zmiany metody weryfikacji tożsamość, tożsamość ustalana jest poprzez wykorzystanie informacji będących w posiadaniu podmiotu w szczególności zawartych w dokumentacji medycznej pacjenta, które powinny być znane jedynie wnioskodawcy. Do tego celu należy wykorzystać metodę pytań bezpośrednich, w których wnioskodawca udziela poprawnych informacji w odpowiedzi na postawione mu pytania przez personel podmiot, bądź tożsamość ustalana jest poprzez dokonanie czynności weryfikacyjnych przy użyciu dostępnych podmiotowi oraz osobie zgłaszającej żądanie narzędzi.

Termin na udostępnienie dokumentacji medycznej

Podmiot zapewnia odpowiednie warunki zabezpieczające dokumentację przed zniszczeniem, uszkodzeniem lub utratą i dostępem osób nieuprawnionych, a także umożliwiające jej wykorzystanie bez zbędnej zwłoki. Dokumentację udostępnia się z zachowaniem jej inte-

w Rzeczypospolitej Polskiej status uchodźcy lub ochronę uzupełniającą, lub zezwolenie na pobyt czasowy udzielone w związku z okolicznością, o której mowa w art. 159 ust. 1 pkt 1 lit. c lub d ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach, posiadającej miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej.

¹¹⁵ Dokument podróży, o którym mowa w Ustawie z dnia 12 grudnia 2013 r. o cudzoziemcach (Dz. U. poz. 1650, ze zm.) – w przypadku osoby posiadającej miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, która uzyskała zezwolenie na pobyt czasowy udzielone w związku z okolicznością, o której mowa w art. 159 ust. 1 pkt 1 lit. c lub d ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach, albo dokument podróży przewidziany w Konwencji Genewskiej, o którym mowa w ustawie z dnia 13 czerwca 2003 r. o udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej Polskiej (Dz. U. z 2012 r. poz. 680, z późn. zm.) – w przypadku osoby posiadającej miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, która uzyskała w Rzeczypospolitej Polskiej status uchodźcy.

gralności, poufności oraz autentyczności, bez zbędnej zwłoki¹¹⁶. Wskazać należy, iż jakiekolwiek inne określenie terminu udostępnienia dokumentacji np. poprzez wskazanie konkretnego czasookresu jest ryzykowne, z punktu widzenia ww. sformułowania, iż dokumentacja powinna być udostępniana bez zbędnej zwłoki.

Odmowa udostępnienia dokumentacji medycznej

W przypadku gdy udostępnienie dokumentacji nie jest możliwe, odmowę przekazuje się w postaci papierowej lub elektronicznej, zgodnie z żądaniem uprawnionego organu lub podmiotu. W każdym przypadku wymagane jest podanie przyczyny odmowy¹¹⁷. Jednostka realizując obowiązek udostępnienia dokumentacji medycznej zobligowana została do weryfikacji, spełnienia się przesłanek uzasadniających udostępnienie dokumentacji medycznej. W praktyce jednak nie oznacza to, iż w przypadku spełnienia się przesłanek dla udostępnienia musi ona wydać jakąś decyzję na podstawie której udostępnienie dopiero zostanie zrealizowane. Wręcz przeciwnie. Wydawanie dodatkowo decyzji jeśli miałyby stanowić warunek konieczny dla udostępnienia dokumentacji jest działaniem nieprawidłowym. W sytuacji jednak, kiedy przeprowadzona analiza stanu faktycznego doprowadzi do dających się usunąć uchybień po stronie wnioskodawcy, najczęściej polegających na braku precyzyjności w zakresie formułowania żądania, podmiot powinien wystąpić ze stosownym wnioskiem o uzupełnienie żądania. Uwaga nie jest to jeszcze decyzja finalna ostateczna, kończąca postępowanie. Jeśli jednak uzupełnienie żądania nie nastąpiło, lub nie zostały spełnione przesłanki warunkujące dopuszczalność udostępnienia dokumentacji, wówczas to dopiero podmiot informuje wnioskodawcę o okolicznościach uzasadniających wydanie odmownej

¹¹⁶ Zgodnie z § 1 ust. 7 zw. z § 70 ust. 1 Rozporządzenia RDM cyt.: „(...) Dokumentację udostępnia się z zachowaniem jej integralności, poufności oraz autentyczności, bez zbędnej zwłoki. (...)” „(...) podmiot zapewnia odpowiednie warunki zabezpieczające dokumentację przed zniszczeniem, uszkodzeniem lub utratą i dostępem osób nieupoważnionych, a także umożliwiające jej wykorzystanie bez zbędnej zwłoki (...)”.

¹¹⁷ Zgodnie z § 71 Rozporządzenia RDM cyt.: „(...) W przypadku gdy udostępnienie dokumentacji nie jest możliwe, odmowę przekazuje się w postaci elektronicznej albo papierowej, zgodnie z żądaniem uprawnionego organu lub podmiotu. W każdym przypadku wymagane jest podanie przyczyny odmowy (...)”.

decyzji w zakresie udostępnienia mu dokumentacji medycznej, uzasadniając powyższe. Informacja przekazywana jest wnioskodawcy, zgodnie z jego żądaniem w formie papierowej albo elektronicznej.

Instrukcja udostępniania dokumentacji medycznej

1. CEL INSTRUKCJI

Celem Instrukcji jest ujednolicenie sposobu udostępniania dokumentacji medycznej: Pacjentom, osobom upoważnionym, przedstawicielom ustawowym Pacjenta oraz organom i podmiotom uprawnionym na podstawie obowiązujących przepisów prawa.

2. ZAKRES STOSOWANIA

Niniejsza Instrukcja obowiązuje w całej Jednostce.

3. DEFINICJE I TERMINY

- 1) **Pacjent** - osoba zwracająca się o udzielenie świadczeń zdrowotnych lub korzystająca ze świadczeń zdrowotnych udzielanych przez podmiot udzielający świadczeń zdrowotnych lub osobę wykonującą zawód medyczny.
- 2) **Jednostka** -
- 3) **Instrukcja** – niniejsza „Instrukcja udostępniania dokumentacji medycznej”.
- 4) **Ustawa / UoPPiRP** – Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta.
- 5) **Rozporządzenie / Rozporządzenie RDM** - Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania.
- 6) **Dokumentacja medyczna** - zbiór dokumentów medycznych, zawierających dane osobowe Pacjenta, informacje o udzielnych świadczeniach oraz inne informacje medyczne dotyczące stanu jego zdrowia, w związku z udzielanymi świadczeniami zdrowotnymi w Jednostce, gromadzonymi i udostępnionymi na zasadach określonych w Ustawie, Rozporządzeniu oraz innych przepisach.
- 7) **Przedstawiciel ustawowy pacjenta** - osoba, która z mocy przepisu prawa może działać w cudzym imieniu i ze skutkiem dla osoby, którą reprezentuje. Czynności dokonane przez przedstawiciela ustawowego wywołują bezpośrednie skutki dla reprezentowanego. Przedstawicielem ustawowym są: rodzice małoletnich dzieci¹¹⁸, ustanowiony przez sąd opiekun¹¹⁹.
- 8) **Wyciąg** - skrótowy dokument zawierający wybrane informacje lub dane z całości dokumentacji medycznej.
- 9) **Odpis** - dokument wytworzony przez przepisanie tekstu z oryginału dokumentacji medycznej z wiernym zachowaniem zgodności co do treści z oryginałem.
- 10) **Kopia** - dokument wytworzony przez odwzorowanie oryginału dokumentacji medycznej, w formie kserokopii albo odwzorowania cyfrowego (skanu).
- 11) **Opiekun faktyczny** - osobę sprawującą, bez obowiązku ustawowego, stałą

¹¹⁸ Art. 98. § 1. Kodeks rodzinny i opiekuńczy

Rodzice są przedstawicielami ustawowymi dziecka pozostającego pod ich władzą rodzicielską. Jeżeli dziecko pozostaje pod władzą rodzicielską obojga rodziców, każde z nich może działać samodzielnie jako przedstawiciel ustawowy dziecka.

¹¹⁹ Art. 155. § 1 i 2 Kodeks rodzinny i opiekuńczy

§ 1. Opiekun sprawuje pieczę nad osobą i majątkiem pozostającego pod opieką; podlega przy tym nadzorowi sądu opiekuńczego.

§ 2. Do sprawowania opieki stosuje się odpowiednio przepisy o władzy rodzicielskiej z zachowaniem przepisów poniższych.

opiekę nad Pacjentem, który ze względu na wiek, stan zdrowia albo stan psychiczny opieki takiej wymaga.

- 12) **Osoba bliska** - małżonka, krewnego do drugiego stopnia lub powinowatego do drugiego stopnia w linii prostej, przedstawiciela ustawowego, osobę pozostającą we wspólnym pożyciu lub osobę wskazaną przez Pacjenta / Przedstawiciela ustawowego Pacjenta.

4. ODPOWIEDZIALNOŚĆ

Odpowiedzialnym za:

- 1) wprowadzenie do stosowania Instrukcji oraz nadzór nad poprawnością jej stosowania **jest**
- 2) weryfikację poprawności przygotowanej do udostępnienia dokumentacji medycznej zgodnie z kierunkiem wniosku o udostępnienie dokumentacji medycznej, **jest**
- 3) zapewnienie adekwatnych do ryzyk warunków organizacyjno – technicznych w związku z udostępnieniem dokumentacji medycznej do wglądu, **jest**
- 4) prowadzenie wykazu udostępnionej dokumentacji medycznej, **jest**
- 5) realizację wysyłki udostępnianej dokumentacji medycznej, **jest**
- 6) ustalanie wysokości stawek opłat za udostępnienie dokumentacji medycznej, oraz podawanie ich do wiadomości w sposób określony przepisami prawa, **jest**
- 7) udostępnienie dokumentacji medycznej w postaci oryginału, **jest**

5. ZASADY UDOSTĘPNIANIA DOKUMENTACJI MEDYCZNEJ

1. W Jednostce zabronione jest udostępnianie dokumentacji medycznej osobom, których tożsamości a w konsekwencji uprawnienia do powyższego nie można zweryfikować w sposób jednoznaczny.
2. Weryfikacji tożsamości dokonuje się poprzez kontrolę okazanego dokumentu tożsamość zawierającego co najmniej zdjęcie, imię i nazwisko oraz PESEL lub w przypadku jego braku inny numer jednoznacznie identyfikujący Pacjenta. Dokumentem potwierdzającym tożsamość jest w szczególności:
 - a) dowód osobisty;
 - b) paszport;
 - c) prawo jazdy;
 - d) legitymacja szkolna;
 - e) karta pobytu¹²⁰;
 - f) dokument podróży¹²¹

¹²⁰ Karta pobytu, o której mowa w ustawie z dnia 12 grudnia 2013 r. o cudzoziemcach (Dz. U. poz. 1650, z późn. zm.) – w przypadku osoby, która uzyskała w Rzeczypospolitej Polskiej status uchodźcy lub ochronę uzupełniającą, lub zezwolenie na pobyt czasowy udzielone w związku z okolicznościami, o których mowa w art. 159 ust. 1 pkt 1 lit. c lub d ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach, posiadającej miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej.

¹²¹ Dokument podróży, o którym mowa w ustawie z dnia 12 grudnia 2013 r. o cudzoziemcach – w przypadku osoby posiadającej miejsce zamieszkania na terytorium

- g) lub inny dokument urzędowy ze zdjęciem.
3. Jednostka może utrwalić informację o:
 - a) dacie dokonania weryfikacji tożsamości; oraz
 - b) rodzaju dokumentu, na podstawie którego została ona dokonana.
 4. Jeśli okazanie dokumentu tożsamości jest niemożliwe lub utrudnione, bądź sytuacja stanu faktycznego stanowi uzasadnienie dla zmiany metody weryfikacji tożsamość:
 - a) tożsamość ustalana jest poprzez wykorzystanie informacji będących w posiadaniu Jednostki w szczególności zawartych w dokumentacji medycznej pacjenta, które powinny być znane jedynie wnioskodawcy. Do tego celu należy wykorzystać metodę pytań bezpośrednich, w których wnioskodawca udziela poprawnych informacji w co najmniej zapytaniach.
 - b) tożsamość ustalana jest poprzez dokonanie czynności weryfikacyjnych przy użyciu dostępnych Jednostce oraz osobie zgłaszającej żądanie narzędzi,
 5. W Jednostce niedopuszczalne jest udostępnianie dokumentacji medycznej podmiotom, instytucjom czy też organom, które nie mogą wykazać swojego uprawnienia umocowanego właściwą podstawą prawną.
- 5.1 Dokumentacja medyczna udostępniana jest:**
1. Pacjentowi, którego dokumentacja medyczna dotyczy po potwierdzeniu jego tożsamości;
 2. Przedstawicielowi ustawowemu pacjenta którego dokumentacja medyczna dotyczy:
 - po potwierdzeniu tożsamość Pacjenta,
 - po potwierdzeniu tożsamość przedstawiciela ustawowego Pacjenta i potwierdzeniu jego statusu;
 - a) w przypadku rodzica dokumentem potwierdzającym status może być akt urodzenia dziecka, jeśli weryfikacja nie jest możliwa do dokonania w oparciu o posiadane przez Jednostkę informacje w szczególności zawarte w dokumentacji medycznej Pacjenta,
 - b) w przypadku opiekuna ustanowionego przez sąd bądź kuratora działającego w roli przedstawiciela ustawowego – dokumentem potwierdzającym status jest stosowne postanowienie sądu.
 3. Osobie upoważnionej przez Pacjenta / osobie upoważnionej przez przedstawiciela ustawowego Pacjenta, którego dokumentacja medyczna

Rzeczypospolitej Polskiej, która uzyskała zezwolenie na pobyt czasowy udzielone w związku z okolicznością, o której mowa w art. 159 ust. 1 pkt 1 lit. c lub d ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach, albo dokument podróży przewidziany w Konwencji Genewskiej, o którym mowa w ustawie z dnia 13 czerwca 2003 r. o udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej Polskiej (Dz. U. z 2012 r. poz. 680, z późn. zm.) – w przypadku osoby posiadającej miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, która uzyskała w Rzeczypospolitej Polskiej status uchodźcy.

dotyczy:

- po potwierdzeniu tożsamość pacjenta,
- po potwierdzeniu tożsamość osoby upoważnionej i potwierdzeniu jej statusu;
 - a) potwierdzenie statusu osoby upoważnionej dokonywane jest poprzez weryfikację treści oświadczenia o upoważnieniu do dostępu do dokumentacji medycznej złożonego za pośrednictwem Internetowego Konta Pacjenta,
 - b) potwierdzenie statusu osoby upoważnionej dokonywane jest poprzez weryfikację treści oświadczenia zamieszczonego w dokumentacji indywidualnej wewnętrznej pacjenta, w przypadku złożenia takiego oświadczenia o upoważnieniu do dostępu do dokumentacji medycznej, w inny sposób niż za pośrednictwem Internetowego Konta Pacjenta,
 - c) potwierdzenie statusu osoby upoważnionej jest także możliwe na podstawie okazanego stosownego upoważnienia udzielonego przez Pacjenta albo przedstawiciela ustawowego Pacjenta.
- 4. Po śmierci Pacjenta dokumentacja medyczna jest udostępniana:
 - a) osobie upoważnionej przez Pacjenta za życia;
 - b) lub osobie, która w chwili zgonu Pacjenta była jego przedstawicielem ustawowym;
 - c) osobie bliskiej, chyba że udostępnieniu sprzeciwi się inna osoba bliska lub sprzeciwił się temu pacjent za życia, z zastrzeżeniem przepisów art. 26 ust. 2 a i 2b UoPPiRP.
- 5. Innym podmiotom wymienione w art. 26 ust. 3 UoPPiRP:
 - a) podmiotom udzielającym świadczeń zdrowotnych, jeżeli dokumentacja ta jest niezbędna do zapewnienia ciągłości świadczeń zdrowotnych;
 - b) organom władzy publicznej, w tym Rzecznikowi Praw Pacjenta, Narodowemu Funduszowi Zdrowia, organom samorządu zawodów medycznych oraz konsultantom w ochronie zdrowia, a także Rzecznikowi Praw Pacjenta Szpitala Psychiatrycznego, w zakresie niezbędnym do wykonywania przez te podmioty ich zadań, w szczególności nadzoru i kontroli;
 - c) podmiotom, o których mowa w art. 119 ust. 1 i 2 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej, w zakresie niezbędnym do przeprowadzenia kontroli na zlecenie ministra właściwego do spraw zdrowia;
 - d) upoważnionym przez podmiot, o którym mowa w art. 121 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej, osobom wykonującym zawód medyczny, w zakresie niezbędnym do sprawowania nadzoru nad podmiotem leczniczym niebędącym przedsiębiorcą;
 - e) Agencji Oceny Technologii Medycznych i Taryfikacji, w zakresie niezbędnym do wykonywania przez nią zadań określonych w art. 31n ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2019 r. poz. 1373, ze. zm.);
 - f) Agencji Badań Medycznych w zakresie określonym ustawą z dnia 21 lutego 2019 r. o Agencji Badań Medycznych (Dz. U. poz. 447 oraz z 2020 r. poz. 567);
 - g) ministrowi właściwemu do spraw zdrowia, sądom, w tym sądom dyscyplinarnym, prokuraturom, lekarzom sądowym i rzecznikom odpowiedzialności zawodowej, w związku z prowadzonym postępowaniem;
 - h) uprawnionym na mocy odrębnych ustaw organom i instytucjom, jeżeli

- badanie zostało przeprowadzone na ich wniosek;
- i) organom rentowym oraz zespołom do spraw orzekania o niepełnosprawności, w związku z prowadzonym przez nie postępowaniem;
 - j) podmiotom prowadzącym rejestry usług medycznych, w zakresie niezbędnym do prowadzenia rejestrów;
 - k) zakładom ubezpieczeń, za zgodą Pacjenta;
 - l) komisjom lekarskim podległym ministrowi właściwemu do spraw wewnętrznych, wojskowym komisjom lekarskim oraz komisjom lekarskim Agencji Bezpieczeństwa Wewnętrznego lub Agencji Wywiadu, podległym Szefom właściwych Agencji;
 - m) osobom wykonującym zawód medyczny, w związku z prowadzeniem procedury oceniającej podmiot udzielający świadczeń zdrowotnych na podstawie przepisów o akredytacji w ochronie zdrowia albo procedury uzyskiwania innych certyfikatów jakości, w zakresie niezbędnym do ich przeprowadzenia;
 - n) wojewódzkiej komisji do spraw orzekania o zdarzeniach medycznych, o której mowa w art. 67e ust. 1 Ustawy, w zakresie prowadzonego postępowania;
 - o) spadkobiercom w zakresie prowadzonego postępowania przed wojewódzką komisją do spraw orzekania o zdarzeniach medycznych, o której mowa w art. 67e ust. 1 Ustawy,
 - p) osobom wykonującym czynności kontrolne na podstawie art. 39 ust. 1 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, w zakresie niezbędnym do ich przeprowadzenia;
 - q) członkom zespołów kontroli zakażeń szpitalnych, o których mowa w art. 14 ustawy z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (Dz. U. z 2019 r. poz. 1239 i 1495 oraz z 2020 r. poz. 284, 322, 374 i 567), w zakresie niezbędnym do wykonywania ich zadań.
 - r) poz. 284, 322, 374 i 567), w zakresie niezbędnym do wykonywania ich zadań.
 - s) Dokumentacja medyczna podmiotów leczniczych, o których mowa w art. 89 ust. 1 i 3 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej, instytutów badawczych, o których mowa w art. 3 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2016 r. poz. 371, 1079, 1311 i 2260 oraz z 2017 r. poz. 202), i innych podmiotów udzielających świadczeń zdrowotnych uczestniczących w przygotowaniu osób do wykonywania zawodu medycznego i kształceniu osób wykonujących zawód medyczny jest udostępniana tym osobom wyłącznie w zakresie niezbędnym do realizacji celów dydaktycznych.
 - t) Dokumentacja medyczna może być udostępniona także szkole wyższej lub instytutowi badawczemu do wykorzystania w celach naukowych, bez ujawniania nazwiska i innych danych umożliwiających identyfikację osoby, której dokumentacja dotyczy.

5.2 Formy udostępnienia dokumentacji

Dokumentacja medyczna jest udostępniana:

1. Do wglądu, w tym także do baz danych w zakresie ochrony zdrowia, w siedzibie Jednostki, z zapewnieniem Pacjentowi lub innym uprawnionym organom lub podmiotom możliwości sporządzenia notatek lub zdjęć. Udostępnienie dokumentacji do wglądu następuje na miejscu w

- w obecności: lekarza prowadzącego lub pracownika upoważnionego (dotyczy to zarówno dokumentacji papierowej, jak i prowadzonej w formie elektronicznej).
2. Poprzez sporządzenie jej wyciągów, odpisów, kopii oraz wydruku.
 3. Przez wydanie oryginału za potwierdzeniem odbioru i z zastrzeżeniem zwrotu po wykorzystaniu, na żądanie organów władzy publicznej albo sądów powszechnych, a także w przypadku gdy zwłoka w wydaniu dokumentacji mogłaby spowodować zagrożenie życia lub zdrowia pacjenta.
 4. Na informatycznym nośniku danych.
 5. Za pośrednictwem środków komunikacji elektronicznej.
 6. Dokumentacja medyczna prowadzona w postaci papierowej może być udostępniona przez sporządzenie kopii w formie odwzorowania cyfrowego (skanu) i przekazanie w sposób określony w ppkt. 4 i 5, na żądanie Pacjenta lub innych uprawnionych organów lub podmiotów, jeżeli przewiduje to regulamin organizacyjny Jednostki.
 7. W przypadku gdy dokumentacja jest udostępniana w formie wydruku, osoba upoważniona przez podmiot potwierdza jego zgodność z dokumentacją i opatruje swoim oznaczeniem, zawierającym imię (imiona), nazwisko, stanowisko i podpis. Wydruk sporządza się w sposób umożliwiający identyfikację osoby udzielającej świadczeń zdrowotnych, zgodnie z § 10 pkt 3 Rozporządzenia RDM.
 8. W przypadku udostępnienia dokumentacji w postaci papierowej w sposób określony w art. 27 ust. 1 pkt 3 UoPPiRP tj. przez wydanie oryginału za potwierdzeniem odbioru i z zastrzeżeniem zwrotu po wykorzystaniu, na żądanie organów władzy publicznej albo sądów powszechnych, a także w przypadku gdy zwłoka w wydaniu dokumentacji mogłaby spowodować zagrożenie życia lub zdrowia pacjenta, pozostawia się kopię lub pełny odpis wydanej dokumentacji.
 9. W przypadku udostępnienia dokumentacji w sposób określony w art. 27 ust. 1 pkt 4 UoPPiRP tj. za pośrednictwem środków komunikacji elektronicznej oraz w art. 27 ust. 3 UoPPiRP tj. gdy dokumentacja medyczna prowadzona w postaci papierowej jest udostępniona przez sporządzenie kopii w formie odwzorowania cyfrowego (skanu) i przekazywana jest za pośrednictwem środków komunikacji elektronicznej albowiem taką ewentualność przewiduje regulamin organizacyjny Jednostki – udostępnienie realizowane jest z wykorzystaniem adresu poczty elektronicznej lub elektronicznej skrzynki podawczej pacjenta, wskazanego jako takiego i zamieszczonego w jego dokumentacji medycznej indywidualnej, zgodnie z § 10 ust. 6 Rozporządzenia RDM.

5.3 Zasady udostępnienia dokumentacji medycznej

1. W celu uzyskania dokumentacji medycznej osoby, podmioty, organy, wymienione w pkt. 5.1 Instrukcji występują z wnioskiem o jej udostępnienie w dowolnej formie.
2. W przypadku formy pisemnej zaleca się wykorzystanie wzoru wniosku o udostępnienie dokumentacji medycznej, stanowiącego **Załącznik nr 1** do niniejszej Instrukcji.
3. Wnioski, o których mowa w ppkt 1 można pobrać w
..... w godzinach albo ze strony internetowej Jednostki

4. Wniosek o udostępnienie dokumentacji medycznej można składać:
 - a) Osobiście.
 - b) Telefonicznie.
 - c) Listownie – przysyłając go na adres
 - d) za pośrednictwem środków komunikacji elektronicznej poprzez przesłanie na email:
5. W przypadku, o którym mowa w ppkt 5a wydaje się wniosek stanowiący Załącznik nr 1 do niniejszej Instrukcji, w celu wypełnienia **pkt 1-4**. Jednocześnie zaznajamia się ww. osobę z zasadami udostępniania dokumentacji medycznej. Wypełniony wniosek następnie przekazywany jest według właściwości w celu przygotowania dokumentacji medycznej do udostępniania, zgodnie z informacjami zawartymi we wniosku. Wyjątkowo przyjęcie wniosku w trybie ppkt 4a może zostać zrealizowane według zapisów ppkt 4b Instrukcji, jeśli znajduje to uzasadnienie w stanie faktycznym, uwzględniając przede wszystkim dobro Pacjenta.
6. W przypadku, o którym mowa w ppkt 5b, pracownik uzyskuje informacje od wnioskodawcy, aby móc wypełnić **pkt 1-3** wniosku, stanowiącego **Załącznik nr 1** do niniejszej Instrukcji. Wypełniony wniosek zostaje odczytany w obecności składającego oświadczenie a następnie przekazywany jest według właściwości w celu przygotowania dokumentacji medycznej do udostępniania, zgodnie z informacjami zawartymi we wniosku (np. sporządzenia kserokopii i potwierdzenia jej za zgodność z oryginałem).
7. Dokumentacja medyczna udostępniana jest bez zbędnej zwłoki.
8. Dokumentacja medyczna wydawana jest po dokonaniu opłaty¹²², o której mowa w pkt 6.1. Opłaty można dokonać w lub przelewem na wskazany rachunek bankowy
9. Każde udostępnienie dokumentacji medycznej, należy zgłaszać do pracownika prowadzącego wykaz udostępnionej dokumentacji medycznej. Zgłoszenia dokonuje osoba udostępniająca dokumentację medyczną.
10. Wyznaczony pracownik prowadzi wykaz dotyczący udostępnionej dokumentacji medycznej zawierający następujące informacje:
 - a) imię (imiona) i nazwisko Pacjenta, którego dotyczy dokumentacja medyczna;
 - b) sposób udostępnienia dokumentacji medycznej;
 - c) zakres udostępnionej dokumentacji medycznej;
 - d) imię (imiona) i nazwisko osoby innej niż Pacjent, której została udostępniona dokumentacja medyczna, a w przypadkach, o których mowa w art. 26 ust. 3 i 4 UoPPiRP, także nazwę uprawnionego organu lub podmiotu;
 - e) imię (imiona) i nazwisko oraz podpis osoby, która udostępniła dokumentację medyczną;
 - f) datę udostępnienia dokumentacji medycznej.
11. Na wniosek zainteresowanego dokumentacja medyczna zostaje wysłana

¹²² Wyrok NSA w Warszawie z dnia 10 kwietnia 2018 r. II OSK 3194/17

wraz z dokumentem księgowym za udostępnienie dokumentacji medycznej korespondencją poleconą za zwrotnym potwierdzeniem odbioru.

12. W przypadku gdy udostępnienie dokumentacji nie jest możliwe, odmowę przekazuje się w postaci elektronicznej albo papierowej, zgodnie z żądaniem uprawnionego organu lub podmiotu. W każdym przypadku wymagane jest podanie przyczyny odmowy. W miarę możliwości decyzja o odmowie udostępnienia dokumentacji medycznej powinna być poprzedzona działaniami ukierunkowanymi na usunięcie przeszkody uniemożliwiającej udostępnienie dokumentacji medycznej.

6. OPŁATY ZA UDOSTĘPNIENIE DOKUMENTACJI MEDYCZNEJ

- 6.1. Wysokość opłaty za udostępnienie dokumentacji medycznej w sposób, o którym mowa w pkt. 5.2 ppkt. 2, 4 i 6 Instrukcji określa podmiot udzielający świadczeń zdrowotnych.
- 6.2. Opłaty, o której mowa w pkt 6.1 nie pobiera się za udostępnienie dokumentacji medycznej:
 1. na potrzeby organów rentowych;
 2. w związku z postępowaniem przed wojewódzką komisją do spraw orzekania o zdarzeniach medycznych, o której mowa w art. 67e ust. 1 UoPPiRP
 3. w przypadku udostępniania dokumentacji medycznej Agencji Oceny Technologii Medycznych i Taryfikacji.
 4. gdy wnioskodawca będący osobą fizyczną wykaże, że nie jest w stanie ponieść opłaty bez uszczerbku dla siebie i rodziny w zakresie utrzymania, po uzyskaniu decyzji Jednostki o zwolnieniu z uiszczenie opłaty.
- 6.3. Opłaty, o której mowa w ust. 6.1, nie pobiera się w przypadku udostępnienia dokumentacji medycznej pacjentowi albo jego przedstawicielowi ustawowemu, albo osobie upoważnionej przez Pacjenta, albo upoważnionej przez przedstawiciela ustawowego Pacjenta, po raz pierwszy w żądanym zakresie i w sposób, o którym mowa w pkt. 5.2 ppkt. 2, 4 i 6

7. PRZECHOWYWANIE DOKUMENTACJI MEDYCZNEJ

- 7.1. Jednostka przechowuje dokumentację medyczną przez okres 20 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu, z wyjątkiem:
 1. dokumentacji medycznej w przypadku zgonu Pacjenta na skutek uszkodzenia ciała lub zatrucia, która jest przechowywana przez okres 30 lat, licząc od końca roku kalendarzowego, w którym nastąpił zgon;
 2. dokumentacji medycznej zawierającej dane niezbędne do monitorowania losów krwi i jej składników, która jest przechowywana przez okres 30 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu;
 3. zdjęć rentgenowskich przechowywanych poza dokumentacją medyczną Pacjenta, które są przechowywane przez okres 10 lat, licząc od końca roku kalendarzowego, w którym wykonano zdjęcie;
 4. skierowań na badania lub zleceń lekarza, które są przechowywane przez okres:
 - a. 5 lat, licząc od końca roku kalendarzowego, w którym udzielono świadczenia zdrowotnego będącego przedmiotem skierowania lub zlecenia lekarza,
 - b. 2 lat, licząc od końca roku kalendarzowego, w którym wystawiono skierowanie – w przypadku gdy świadczenie zdrowotne nie zostało udzielone z powodu niezgłoszenia się

Pacjenta w ustalonym terminie, chyba że Pacjent odebrał skierowanie;

5. dokumentacji medycznej dotyczącej dzieci do ukończenia 2. roku życia, która jest przechowywana przez okres 22 lat.

7.2. Po upływie okresów wymienionych w ppkt. 7.1 Jednostka niszczy dokumentację medyczną w sposób uniemożliwiający identyfikację Pacjenta, którego dotyczyła. Dokumentacja medyczna przeznaczona do zniszczenia może być wydana Pacjentowi, jego przedstawicielowi ustawowemu lub osobie upoważnionej przez Pacjenta.

7.3. Po upływie okresów, o których mowa w ppkt. 7.1, do postępowania z dokumentacją medyczną będącą materiałem archiwalnym w rozumieniu przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2016 r. poz. 1506 i 1948 oraz z 2017 r. poz. 1086), stosuje się przepisy wydane na podstawie art. 5 ust. 2 i 2b tej UoPPiRP.

WNIOSEK O UDOSTĘPNIENIE DOKUMENTACJI MEDYCZNEJ

Dane identyfikujące tożsamości <u>WNIOSKODAWCY</u>: (proszę wypełnić czytelnie)	
Imię (imiona) wnioskodawcy / Nazwa podmiotu wnioskującego	
Adres zamieszkania wnioskodawcy / Adres siedziby podmiotu wnioskującego	
PESEL wnioskodawcy	
Numer telefonu kontaktowego wnioskodawcy	

Status wnioskodawcy: (proszę określić, kto występuje z wnioskiem o udostępnienie dokumentacji medycznej, proszę zaznaczyć „X” właściwą kolumnę)				
Pacjent	Osoba upoważniona przez Pacjenta / przez przedstawiciela ustawowego	Przedstawiciel ustawowy Pacjenta	Osoba bliska	Podmiot wskazany w art. 26 ust. 3 / 3a / 4 UoPIRP ¹²³
				Proszę określić podstawę prawną:

¹²³ Ustawa z dnia 06 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta.

(1) Wnoszę o udostępnienie dokumentacji medycznej

a) w formie:							
1. do wglądu	2. kopii	3. odpisu	4. wyciągu	5. wydruku	6. na informatycznym nośniku danych	7. oryginału z obowiąz- kiem zwrotu ¹²⁴	8. za pośrednictwem środków komunikacji elektronicznej
a) w zakresie: dokumentacja medyczna z							
(proszę określić nazwę komórki organizacyjnej / albo wskazać rodzaj dokumentacji wnioskowanej)							
b) za okres:							
(oddo..... / data udzielenia świadczenia)							

(2) Dane identyfikujące PACJENTA, którego dokumentacja dotyczy:

Imię (imiona) Pacjenta	
Nazwisko Pacjenta	
Adres zamieszkania Pacjenta	
PESEL Pacjenta / w przypadku noworodka PESEL matki.	

(3) Sposób odbioru dokumentacji, w przypadku jej wydania:

ODBIERAJĄCY:	Odbiór osobisty	
Pacjent którego dokumentacja dotyczy	Wysyłka	
ODBIERAJĄCY:	Odbiór osobisty	
Osoba upoważniona	Wysyłka	
ODBIERAJĄCY:	Odbiór osobisty	
Przedstawiciel ustawowy Pacjenta	Wysyłka	

¹²⁴ Art. 27 ust. 3 Ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta

Dokumentacja medyczna jest udostępniana przez wydanie oryginału za potwierdzeniem odbioru i z zastrzeżeniem zwrotu po wykorzystaniu, na żądanie organów władzy publicznej albo sądów powszechnych, a także w przypadku gdy zwłoka w wydaniu dokumentacji mogłaby spowodować zagrożenie życia lub zdrowia pacjenta;

(4) Oświadczenie wnioskodawcy:

Oświadczam, że zapoznałem/am się z zasadami udostępniania dokumentacji medycznej w Jednostce, rozumiem i akceptuję określony nimi tryb oraz mam świadomość obowiązku pokrycia kosztów jej wydania, jeśli nie dotyczą mnie sytuacji zwalniające z tego obowiązku.	
W przypadku wniosku o jakim mowa w pkt. (1) lit a. ppkt 7. oświadczam, iż zwłoka w wydaniu dokumentacji w innej formie niż w oryginale mogłaby spowodować zagrożenie życia lub zdrowia Pacjenta, jednocześnie zobowiązuję się do jej zwrotu po wykorzystaniu.	

(5) Tożsamość i status wnioskodawcy ustalono w oparciu o:*(wypełnia upoważniony pracownik Jednostki)*

Dokument tożsamości wnioskodawcy:	Nazwa:
Metodą pytań bezpośrednich	
Inne czynności weryfikacyjne:	
Dokumentację przedłożoną do wniosku:	Upoważnienie Potwierdzające zagrożenie życia, zdrowia

Miejsce i data	Podpis wnioskodawcy / W przypadku odnotowania wniosku za wnioskodawcę imię i nazwisko pracownika Jednostki z adnotacją, przyjęcia wniosku w innej formie niż ustna do realizacji	Data i podpis przyjmującego

(6) Potwierdzenie udostępnienia dokumentacji medycznej:

Oplata	tytułem	Ilość stron	Kwota	Uregulowano
udostępniania				
Pierwszy wniosek o udostępnienie dokumentacji medycznej w danym zakresie:				
Zwolnienie z opłaty:				
Podpis i data osoby udostępniającej w sposób zgodny z treścią wniosku:			Podpis:	
			Data.	
Podpis i data osoby odbierające			Podpis:	
			Data.	

(7) Potwierdzenie zwrotu udostępnionej w oryginale dokumentacji medycznej:

Podpis osoby odbierającej zwracaną dokumentację medyczną	Podpis:	
	Data.	
Potwierdzam kompletność zwracanej dokumentacji medycznej	Kompletna	Wybrakowana

**OŚWIADCZENIE O UPOWAŻNIENIU DO DOSTĘPU DO
DOKUMENTACJI MEDYCZNEJ**

Miejscowość:		
Data:		
Oświadczenie Pacjenta / Przedstawiciela ustawowego Pacjenta o upoważnieniu do dostępu do dokumentacji medycznej Pacjenta złożone w formie ustnej w obecności personelu Jednostki podlega odnotowaniu przez personel Jednostki, z wykorzystaniem niniejszego formularza.		
Imię i nazwisko osoby odnotowującej oświadczenie Pacjenta / Przedstawiciela ustawowego Pacjenta	Imię i nazwisko	Stanowisko

Dane identyfikujące Pacjenta: (A) (proszę podać dane umożliwiające identyfikację tożsamości Pacjenta)	
Imię (imiona) Pacjenta	
Nazwisko Pacjenta	
Adres zamieszkania Pacjenta	
PESEL Pacjenta	
W przypadku noworodka – numer PESEL matki.	
Data i miejsce urodzenia w przypadku cudzoziemca	

Składający oświadczenie (B) (proszę wpisać osobę która składa oświadczenie)				
	Pacjent	Przedstawiciel ustawowy Pacjenta	Osoba upoważniona przez Przedstawiciela ustawowego Pacjenta	Opiekun prawny Pacjenta pozostającego pod jego opieką / kurator
Składający oświadczenie:				

Działając, jako uprawniony na podstawie art. 26 ust. 1 Ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta składam oświadczenie o upoważnieniu do dostępu do dokumentacji medycznej przez nw. osobę:	
Imię (imiona) upoważnionego	
Nazwisko upoważnionego	
PESEL upoważnionego	
Nr telefonu upoważnionego	
Data i miejsce urodzenia w przypadku cudzoziemca	
Zakres udzielonego upoważnienia:	
	do dokumentacji w pełnym zakresie
	do dokumentacji w ograniczonym zakresie
	do dokumentacji powstałej jedynie w niniejszej Jednostce
	do dokumentacji powstałej w niniejszej Jednostce oraz w pozostałych Jednostkach.
	do dokumentacji także po śmierci Pacjenta bez względu na Jednostkę ją tworzącą

Miejscowość i data	Podpis udzielającego upoważnienia	Data i podpis przyjmującego

**Upoważnienie
do przetwarzania danych
osobowych**

Upoważnienie

do przetwarzania danych osobowych

Nie można w sposób jednoznaczny powiedzieć, że obowiązek¹²⁵ nadania upoważnienia do przetwarzania danych osobowych wynika z art. 29 RODO i/lub z art. 32 ust. 4 RODO.¹²⁶ Co prawda w polskiej wersji językowej art. 29 RODO nosi tytuł: „Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego”, to jednak w angielskiej wersji językowej, ten sam tytuł brzmi: „Processing under the authority of the controller or processor”. Analiza treści przepisu prowadzi do podobnych obserwacji. W polskiej wersji językowej w art. 29 widnieje: „Podmiot przetwarzający oraz każda osoba **działająca z upoważnienia administratora lub podmiotu przetwarzającego** i mająca dostęp do danych osobowych **przetwarzają je wyłącznie na polecenie administratora**, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.”. W angielskiej wersji językowej, w art. 29 widnieje: „The processor and any person **acting under the authority of the controller or of the processor**, who has access to personal data, **shall not process those data except on instructions from the controller**, unless required to do so by Union or Member State law.”.

Niezależnie od wersji językowej uprawnienie do przetwarzania danych osobowych jest dwuetapowe. Pierwszy etap to: „**działająca**

¹²⁵ M. Krzysztofek twierdzi: „Upoważnienie powinno być odrębnym oświadczeniem administratora lub processora” (sic!), „nie można domniemywać jego zakresu lub treści z umowy o pracę lub z zakresu obowiązków pracownika”. M. Krzysztofek. *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*. Warszawa 2016. s. 215. Pogląd ten cytują P. Litwiński, P. Barta, M. Kawecki w swoim Komentarzu. P. Litwiński, P. Barta, M. Kawecki. w: P. Litwiński (red.) P. Barta, M. Kawecki. *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*. Warszawa 2018. s. 489. W komentarzu tych autorów zdaje się być jednak widać pewien dystans do poglądu M. Krzysztofka. Moje stanowisko na temat upoważnień wynika z dalszej części wyводу głównego i nie ma go tu sensu streszczać.

¹²⁶ Źródło obowiązku znajdujące się równolegle w dwóch przepisach stanowi piękną ilustrację zjawiska superfluum. Por. M. Kłodawski. *Superfluum i nadwyżki znaczeniowe jako przykłady redundancji tekstu prawnego*. Archiwum Filozofii Prawa i Filozofii Społecznej 2013/2. s. 38–51.

z upoważnienia administratora ” – „acting under the authority of the controller or of the processor”, drugi etap to: „przetwarzają je wyłącznie na polecenie administratora” – „shall not process those data except on instructions from the controller”.

Należy zrealizować oba etapy. Można nadać pisemne upoważnienia i nadać/ wydać pisemne polecenia i skorzystać przy tym z dokumentów, których wzory zaproponowane są poniżej.

Obowiązek dwuetapowego uprawniania do przetwarzania danych osobowych można też zrealizować inaczej niż wydając upoważnienia i polecenia. Poniżej zamieszczono zestawienie kilku możliwości realizacji tego obowiązku.

1 etap ¹²⁷	2 etap
upoważnienie	polecenie przetwarzania
umowa o pracę	zakres czynności służbowych ¹²⁸
umowa o pracę z zakresem czynności służbowych	polecenie przetwarzania
umowa o pracę z zakresem czynności służbowych	upoważnienie
umowa o pracę z zakresem czynności służbowych	dostęp do systemu informatycznego/teleinformatycznego
umowa cywilno–prawna	polecenie przetwarzania
umowa cywilno–prawna	upoważnienie
umowa cywilno–prawna + upoważnienie	polecenie przetwarzania
upoważnienia tylko w rejestrze upoważnień	polecenia tylko w rejestrze poleceń
umowa cywilno–prawna	upoważnienia tylko w rejestrze upoważnień
umowa cywilno–prawna	polecenia tylko w rejestrze poleceń

¹²⁷ Tabela ta stanowi rozwinięcie tabeli zamieszczonej w: J. Rzymowski *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*. Kraków 2019. s. 93.

¹²⁸ Jako zwolennika rozwiązania, które znajduje się w tym wierszu tabeli identyfikuję pana Piotra Wojczyśa. Nie jestem w stanie wskazać źródła pisanego, ponieważ pogląd P. Wojczyśa znam wskutek internetowej wymiany uwag z Nim na ten temat.

Niezależnie od tego, które podejście stosujemy, należy w Polityce ochrony sprawę opisać, wskazując przy tym co uważamy za pierwszy etap – upoważnienie, co uważamy za drugi etap – polecenie.

Trafnie o zjawisku upoważnień, pisze K. Wygoda¹²⁹. Autor ten zwraca uwagę na fakt, że na gruncie RODO konieczne jest rozdzielanie „fazy umocowania”, czyli fazy „określenia ogólnego, potencjalnego zakresu działania” osób, które są lub będą dopuszczone do przetwarzania, od „późniejszej, stałej aktywności związanej” z¹³⁰ „wydawaniem poleceń (instrukcji) co do konkretnego przetwarzania (niezależnie od trybu ich wydania oraz formy, jaką przybiorą).¹³¹

W kontekście uprawnienia do przetwarzania danych osobowych należy pamiętać o tym, że z art. 5 ust 1 lit f RODO wynika zasada integralności i zasada poufności. Zasady te, realizowane są głównie właśnie dzięki systemowi upoważnień i poleceń. To, że przetwarzać dane osobowe powinny wyłącznie osoby, wobec których zaistniało dwuetapowe uprawnienie do przetwarzania danych osobowych wynika z art. 29 RODO i z art. 32 ust. 4 RODO.

Można do sprawy podejść w sposób ryzykancki i uznać, że osoby pracujące w PWDL są z mocy prawa upoważnione czy uprawnione do przetwarzania danych osobowych, danych medycznych. Pogląd taki można wyprowadzić z art. 24 ust. 2 UoPPiRPP.

Z przepisu tego wynika, że:

- **do przetwarzania** danych zawartych w dokumentacji medycznej
- **w celu ochrony zdrowia**, w celu udzielania oraz zarządzania udzielaniem świadczeń zdrowotnych, w celu utrzymania systemu telein-

¹²⁹ K. Wygoda w: M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre. *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*. Warszawa 2018. s. 332.

¹³⁰ Dziwna przerwa w cytacie spowodowane jest prawdopodobnym błędem drukarskim w cytowanym Komentarzu, błąd usunęłam, cytując, poprzez zamianę oryginalnego: „w” na „z”.

¹³¹ Rozważania prowadzone w niniejszym rozdziale, od jego początku, do miejsca umieszczenia tego przypisu są częściowo cytatem, częściowo skrótem a częściowo (tabela) rozwinięciem rozważań prowadzonych w: J. Rzymowski RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora. Kraków 2019. s. 92-94.

formatycznego, w którym przetwarzana jest dokumentacja medyczna, i zapewnienia bezpieczeństwa tego systemu

- są uprawnione dwie kategorie osób.

Pierwsza kategoria to osoby wykonujące zawód medyczny. Osoby te są uprawnione do przetwarzania danych bez żadnych dodatkowych warunków.

Druga kategoria to inne osoby wykonujące czynności pomocnicze przy udzielaniu świadczeń zdrowotnych, a także czynności związane z utrzymaniem systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna, i zapewnieniem bezpieczeństwa tego systemu. Osoby te są uprawnione do przetwarzania danych na podstawie upoważnienia administratora danych.

Mając na uwadze powyższe, można uznać, że skoro druga kategoria osób jest uprawniona na podstawie upoważnienia, to pierwsza (osoby wykonujące zawód medyczny) są uprawnione do przetwarzania danych bez upoważnienia. Można tak uznać, ale:

- przepis UoPPiRPP stanowi o danych zawartych w dokumentacji, faktem jest, że w PWDL występują głównie takie dane, jednak nie tylko takie; jeżeli udostępniane są informacje o stanie zdrowia, to nie można z całą pewnością powiedzieć, że są to dane „zawarte w dokumentacji”, one w niej zawarte były, ale już nie są;
- przepis UoPPiRPP stanowi o upoważnieniu ADO czyli o jednym z etapów uprawnienia do przetwarzania, o drugim zapomniano, jednak UoPPiRPP ma rangę niższą niż RODO, więc drugi etap (jakkolwiek rozumiany) powinien mieć miejsce;
- pracownicy medyczni są uprawnieni, ale nie wiadomo czy to jedno-etapowe uprawnienie zastępuje dwuetapowe uprawnienie z RODO.

Mając w pamięci art. 24 ust. 3 UoPPiRPP można prowadzić takie rozważania, jednak nieliczne (w czasie pisania książki) ale drażniące kary nakładane przez PUODO nakazują być ostrożnym. Innymi słowy, rozważania prowadzić można jednak nienadawanie upoważnień, a lepiej jeszcze upoważnień wraz z czymś jeszcze jest nieroztropnym ryzykanctwem.

Należy zwrócić uwagę, że PUODO przejawia na oficjalnej stronie skłonność do koncepcji, zgodnie z którą upoważnienia nadawać należy. Jednocześnie, jeśli chodzi o formę upoważnień, o której pisze-

my niżej, PUODO sygnalizuje, że „W świetle zasady rozliczalności jakakolwiek postać, w tym elektroniczna, która pozwala na udokumentowanie spełnienia obowiązków celem wykazania przestrzegania przepisów, a w tym przypadku wykonania obowiązku wynikającego z art. 29 RODO”¹³² może być uznana za prawidłową. należy uznać za prawidłową. Uważam, że już tu konieczne jest poczynienie pewnych uwag. Jeśli chodzi o formę upoważnienia wymaganą przez RODO, to rzeczywiście wynika ona jedynie z zasady rozliczalności. W związku z tym forma ta może być dowolna. Papier. Dokument elektroniczny bez podpisu elektronicznego. Dokument elektroniczny z podpisem elektronicznym. Wiadomość poczty elektronicznej zawierająca. Wszystkie te sposoby wydania upoważnienia wydają się być właściwe na gruncie RODO, ale... Ale uważamy, że w przewidywaniu ewentualnej kontroli dobrze jest mieć konkretny substrat upoważnienia, czyli dokument sporządzony najlepiej w wersji papierowej. Zwracamy też uwagę, że rozważania takie mogą być prowadzone na gruncie RODO. Na gruncie Ustawy 730 (wyjaśniamy niżej) rozważania takie są nieuprawnione. Na gruncie tej ustawy konieczna jest forma pisemna w rozumieniu prawa polskiego, bo ustawa ta w Polsce została wydana, więc odnosi się do polskich zjawisk języka prawnego. Piszemy o tym również niżej i zastrzegamy, że Ustawa 730, w tym zakresie na szczęście PWDLi nie dotyczy.

Forma upoważnień

Z prowadzonych wyżej rozważań wynika, że wydawanie upoważnień nie jest obowiązkiem. Kwestia skonstruowania uprawnienia do przetwarzania danych osobowych może być załatwiona inaczej niż z wykorzystaniem upoważnień. Kiedy jednak upoważnienia się wydaje, to należy zdecydować w jakiej formie.

O formie upoważnień decydują 3 czynniki:

- forma przewidziana w RODO
- zasada rozliczalności (art. 5 ust. 2 RODO)
- forma przewidziana w Ustawie 730.¹³³

¹³² <https://uodo.gov.pl/pl/225/1278>

¹³³ Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związ-

Jeśli chodzi o **formę przewidzianą przez RODO**, to RODO żadnej szczególnej formy nie przewiduje.

Jeśli chodzi o **formę wynikającą z zasady rozliczalności**, to forma pisemna, czyli z podpisem odręcznym lub z podpisem kwalifikowanym nie jest konieczna, należy jednak pamiętać, że forma pisemna stanowi idealny dowód w ujęciu procesowym. Upoważnienie (polecenie) nadane w postaci uprawnień do systemu jest równie dobre jak upoważnienie pisemne, nadający musi jednak pamiętać, że pewnego dnia może zostać zapytany o to czy to upoważnienie nadał. O dowód, że nadał. Przez pracowników PUODO. Przez sąd. Jeżeli administrator nadaje upoważnienia, to zapytany o nie, musi być w stanie wykazać, że je nadał. Może pokazać papierowe upoważnienia, wydruki uprawnień do systemu itd. Wystarczająca wydaje się też forma dokumentowa.

Jeśli chodzi o **formę wynikającą z Ustawy 730**, to zachodzi tu pewien fascynujący splot zjawisk.

- W ustawie 730 nałożono na wiele podmiotów, obowiązek nadawania upoważnień pisemnych. Na szczęście na PWDLe nie nałożono takiego obowiązku.
- Pisemne upoważnienie to upoważnienie z podpisem odręcznym. Te same skutki prawne co podpis odręczny wywołuje również podpis elektroniczny kwalifikowany.
- PUODO twierdzi, że „Nadawanie upoważnień w postaci elektronicznej należy uznać za wykonanie obowiązku nadania upoważnień w formie pisemnej.”¹³⁴. Z tym się zgadzamy. Przypominamy jednak, że postać elektroniczna to postać z podpisem elektronicznym kwalifikowanym.¹³⁵ Czy anonimowy pracownik PUODO, którego wypowiedź cytujemy, był tego świadom – nie wiemy, jednak napisał co napisał. Treść ta obecna jest na stronie www PUODO. W takim razie należy sądzić, że PUODO twierdzi iż upoważnienia można nadawać z podpisem odręcznym lub z podpisem elektronicznym kwalifikowanym.

ku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Dz.U. 2019 poz. 730 (Dalej: Ustawa 730).

¹³⁴ <https://uodo.gov.pl/pl/225/1278> (2.01. 2020).

¹³⁵ Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny. ze zm. t.j. Dz. U. 2019 poz. 1145. ze zm. art. 781.

- PUODO twierdzi dalej, że „W świetle zasady rozliczalności jakakolwiek postać, w tym elektroniczna, która pozwala na udokumentowanie spełnienia obowiązków celem wykazania przestrzegania przepisów, a w tym przypadku wykonania obowiązku wynikającego z art. 29 RODO należy uznać za prawidłową.”¹³⁶.
- Prawdą jest, że jakakolwiek postać, która „pozwała na udokumentowanie spełnienia obowiązków celem wykazania przestrzegania przepisów” realizuje zasadę rozliczalności, o czym jednak PUODO nie pisze.
- Prawdą jest, że z art. 29 RODO wynika obowiązek, jednak nie jest to obowiązek nadawania upoważnień, na co mogłoby wskazywać pierwsze z cytowanych zdań. Obowiązek dbałości o to by dane przetwarzały jedynie osoby dwuetapowo uprawnione wynika z art. 29 RODO, jednak nie ma konieczności realizacji tego obowiązku, na drodze wydawania upoważnień. Obowiązek nadawania upoważnień można zrealizować w formie pisemnej lub elektronicznej, jednak nie wynika on z RODO.
- Obowiązek wynikający z art. 29 RODO można zrealizować z wykorzystaniem formy pisemnej, formy elektronicznej, lub bez zachowania tych form, na przykład z wykorzystaniem formy dokumentowej¹³⁷. W realiach systemu informatycznego, warunki dla takiej formy spełniłoby uprawnienie do dostępu do obszarów systemu, o ile dokładnie byłoby wiadomo kto je, w sensie technicznym, sporządził.
- Obowiązki nadawania pisemnych upoważnień, wynikające z Ustawy 730 mogą zostać bezpiecznie zrealizowane z wykorzystaniem podpisu odręcznego lub podpisu elektronicznego kwalifikowanego. Wykorzystanie formy dokumentowej jest pewnym ryzykiem, ale ryzykiem na gruncie Ustawy 730, nie na gruncie RODO.

Podsumowując

Upoważnienia na gruncie RODO mogą nie być nadawane w ogóle, można je zastąpić innymi aktami, innymi dokumentami. Piszemy o tym na początku rozdziału. Upoważnienia na gruncie

¹³⁶ <https://uodo.gov.pl/pl/225/1278> (2.01. 2020).

¹³⁷ Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny. ze zm. t.j. Dz. U. 2019 poz. 1145. ze zm. art. 772.

Ustawy 730 należy nadawać w konkretnych formach (forma pisemna, forma elektroniczna, ryzykownie – forma dokumentowa), jednak ograniczenie to nie dotyczy PWDL.

W realiach medycznych upoważnienia i polecenia, o ile są nadawane, to można nadawać je w dowolnej formie.
Należy dbać o to by móc wykazać, że upoważnienia, o ile są nadawane, zostały wydane, co wynika z zasady rozliczalności.

Upoważnienie i polecenie, administrator danych i podmiot przetwarzający¹³⁸

Przy okazji rozważań o upoważnieniach i zjawiskach im podobnych należy zwrócić uwagę na jeszcze jedno. Otóż upoważnienia nadaje na gruncie RODO odpowiednio administrator lub podmiot przetwarzający, jednak polecenie ma być wydane wyłącznie przez administratora, co wynika z art. 29 RODO.

Przetwarzanie przez ADO z upoważnienia ADO i na polecenie ADO nie jest problemem. Problemem jest przetwarzanie przez podmiot przetwarzający. Podmiot przetwarzający upoważnia swoich pracowników, jednak konieczność przetwarzania z polecenia ADO jest pewną niedogodnością.

Jeżeli przetwarzanie ma miejsce w organizacji administratora, to przetwarzanie wyłącznie na jego polecenie nie jest problemem. Jeżeli przetwarzanie ma jednak miejsce w organizacji podmiotu przetwarzającego dane osobowe, to przetwarzanie wyłącznie na polecenie administratora jawi się jako bardziej skomplikowane.

Podmiot przetwarzający upoważnia do przetwarzania danych osobowych, których przetwarzanie mu powierzono, trudno jednak powiedzieć, czy może również polecić w imieniu ADO. Uważam, że jest to dopuszczalne, jeżeli ADO przewidzi to w umowie powierzenia przetwarzania.

Sugerujemy by obowiązek dbałości o to by dane osobowe były przetwarzane przez osoby upoważnione realizować w sposób tradycyjny, czyli z użyciem dokumentów papierowych, są one idealne z punktu widzenia zasady rozliczalności i równie idealnie nadają się

¹³⁸ Podrozdział ten jest fragmentem mojego artykułu „Upoważnienia do przetwarzania danych w RODO”, opublikowanego w numerze 7/2017 It w administracji.

jako dowody w postępowaniu przed sądem administracyjnym, po ukaraniu ADO karą administracyjną. Lepiej je mieć niż ich nie mieć.

Upoważnienia można sformułować w oparciu o RCPD, można je sformułować z odniesieniem do umów o pracę lub innych umów zawartych z osobą upoważnioną.

Treść dokumentu

„Dla rozważań na temat upoważnień do przetwarzania danych osobowych istotne jest, że w rejestrze czynności przetwarzania danych osobowych, prowadzonym przez ADO, należy odnotowywać między innymi opis kategorii osób, których dane dotyczą. W takim razie dobrze by było, gdyby kategorie osób, których dane dotyczą, które odnotowane są w rejestrze, znalazły się w upoważnieniach do przetwarzania danych osobowych. Skoro ADO przetwarza dane osobowe osób należących do kategorii wymienionych w rejestrze, to dobrze by było gdyby było wiadomo kto, kto w ramach struktury ADO, przetwarza informacje o osobach należących do tych kategorii. Dowiemy się o tym z upoważnienia, jeśli w upoważnieniu informacje o kategoriach osób umieścimy.

W rejestrze czynności przetwarzania prowadzonym przez administratora danych należy umieścić kategorie czynności przetwarzania.¹³⁹ Sytuacja z umieszczeniem w upoważnieniu kategorii czynności przetwarzania lub czynności przetwarzania jest analogiczna do sytuacji związanej z umieszczeniem w upoważnieniu kategorii danych osobowych. Dobrze by było, gdyby czynności przetwarzania danych osobowych lub kategorie czynności przetwarzania danych osobowych, które odnotowane są w rejestrze, znalazły się w upoważnieniach do przetwarzania danych osobowych, skoro bowiem te czynności przetwarzania danych osobowych lub kategorie czynności przetwarzania danych osobowych mają miejsce (o czym dowiadujemy się z rejestru), to dobrze by było, gdyby było wiadomo, kto dane czynności przetwarzania danych osobowych lub kategorie czynności przetwa-

¹³⁹ Artykuł 30 RODO jest skonstruowany błędnie. Po szersze informacje odsyłam do rozdziału niniejszej publikacji, poświęconego rejestrowi czynności przetwarzania prowadzonemu przez ADO.

rzania danych osobowych wykonuje, o czym dowiemy się z upoważnienia, jeśli w upoważnieniu informacje o tym ADO umieści.”¹⁴⁰

Upoważnienie może wyglądać w sposób wskazany na następnej stronie. Upoważnienie, którego wzór wskazano na następnej stronie mieści w sobie zarówno etap upoważnienia jak i etap polecenia.

¹⁴⁰ J. Rzymowski. *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*. Kraków 2019. s. 58-59.

....., dn.

UPOWAŻNIENIE

Numer:

Na podstawie art. 29 w zw. z 32 ust. 4, 30 ust. 1 art. 5 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych (Dz. Urz. 2016.119.1), jako administrator danych osobowych **upoważniam** Panią / Pana:

.....

(imię i nazwisko pracownika)

.....

(stanowisko służbowe)

zatrudnioną / zatrudnionego w

do przetwarzania danych osobowych na polecenie i w zakresie wynikającym z powierzonych do wykonywania czynności służbowych / zlecenia wykonywania zadań zleconych*, określonych treścią umowy z dnia w odniesieniu do następujących kategorii danych osobowych, **zgodnie z poleceniami** określonymi treścią ww. aktów:

Ciąg dalszy upoważnienia, ewentualnie jego druga strona znajduje się na kolejnej stronie.

Rodzaj czynności przetwarzania	Upoważniam / Nie upoważniam	Nazwa programu informatycznego / Nadany indywidualny login:
a) Czynności przetwarzania danych utrwalonych w postaci papierowej – odnoszące się do Pacjentów		Nie dotyczy
b) Czynności przetwarzania danych w systemie teleinformatycznym – odnoszące się do Pacjentów		
c) Czynności przetwarzania danych utrwalonych w postaci papierowej – odnoszące się do Pracowników / Kandydatów/ Innych podmiotów		Nie dotyczy
d) Czynności przetwarzania danych w systemie teleinformatycznym – odnoszące się do Pracowników / Kandydatów/ Innych podmiotów		
Upoważnienie obowiązuje od dnia do dnia / do odwołania* Niniejsze upoważnienie zastępuje / nie zastępuje upoważnienia wydane uprzednio* /data i podpis administratora danych / osoby upoważnionej/ , dn.		

Jeżeli upoważnienie nie jest już konieczne, to należy je wycofać, uchylić, w każdym razie zadbać by nie obowiązywało.

Wzór dokumentu wycofania upoważnienia.

....., dn.

**COFNIĘCIE
UPOWAŻNIENIA**

Numer:

Na podstawie art. 29 w zw. z 32 ust. 4, 30 ust. 1 art. 5 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych (Dz. Urz. 2016.119.1), jako administrator danych osobowych **cofam upoważnienie wydane** Pani / Panu:

.....

(imię i nazwisko osoby upoważnionej)

.....

(stanowisko służbowe)

.....

(numer upoważnienia)

Upoważnienie cofa się od dnia

.....

/data i podpis administratora danych / osoby upoważnionej/

Upoważnienie w formie listy

„Upoważnienie do przetwarzania danych osobowych może mieć zupełnie inną postać niż zamieszczony powyżej wzór¹⁴¹. ADO może nadawać upoważnienia niejako hurtowo. Możliwe i jak najbardziej realizujące nieliczne w tej mierze wymogi RODO, jest nadanie upoważnienia w postaci wskazanej poniżej. W takim upoważnieniu ADO określa jego zakres, po czym wymienia listę osób, którym owo upoważnienie nadaje.”¹⁴²

W realiach medycznych upoważnienia takie można nadawać całym grupom osób, które przetwarzają dane osobowe w ten sam sposób, na przykład studentom. Osoba nadająca upoważnienia może określić zakres upoważnienia i wskazać, że dotyczy ono „studentów roku takiego to a takiego studiów medycznych, wymienionych na załączonej do upoważnienia liście”, albo, jeśli nadający upoważnienia lubi jałową pracę, może wskazać on, że upoważnienie dotyczy „studentów grupy dziekańskiej takiej to a takiej”.

¹⁴¹ P. Litwiński, P. Barta, M. Kawecki. Zwracają słuszną uwagę, że: „Rozporządzenie nie przesądza, czy upoważnienie powinno być nadawane indywidualnie, czy też może przyjąć formę zbiorczej listy obejmującej wykaz upoważnianych osób”. P. Litwiński, P. Barta, M. Kawecki. w P. Litwiński (red.) P. Barta, M. Kawecki. *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*. Warszawa 2018. s. 489. Zgadzam się w pełni z tym poglądem, a cytuję go dlatego, że w mojej pracy spotkałem się ze zjawiskiem, że stawiana przeze mnie propozycja nadawania upoważnień w formie listy spotykała się co najmniej z protestem a zwykle z zaskoczeniem. Upoważnienie zwykle wyobrażane jest jako karteczka, na której ADO upoważnia jedną osobę do przetwarzania danych osobowych. Na karteczce tej ADO pisze też o odpowiedzialności i odbiera pokwitowanie od osoby, którą upoważnił. Upoważnienie takie wygląda mniej więcej tak, jak pierwszy z proponowanych przeze mnie wzorów. Oczywiście i pod rządami poprzednich przepisów, i teraz może to tak wyglądać, ale zdecydowanie nie musi. Ufam, że nazwiska P. Litwińskiego i P. Barty przekonają nieprzekonanych Czytelników.

¹⁴² J. Rzymowski. *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*. Kraków 2019. s. 65

Upoważnienie do przetwarzania danych osobowych

numer upoważnienia (numer nie jest konieczny, jednak ogromnie ułatwia zarządzanie upoważnieniami).

Administrator danych (słowa: „administrator danych mogą być zastąpione pełną nazwą administratora danych”, lub pełna nazwa administratora zostaje dodana do słów: „administrator danych”).

upoważnia wymienione poniżej osoby do przetwarzania danych osobowych w następującym zakresie:

czynności przetwarzania, do wykonywania których administrator nadaje upoważnienie:

lub

kategorie czynności przetwarzania, do wykonywania których administrator nadaje upoważnienie:

kategorie osób, których dane osobowe są objęte upoważnieniem:

kategorie danych osobowych, które są objęte upoważnieniem:

cel przetwarzania:

upoważnienie ma charakter jednorazowy i obowiązuje w dniu:

lub

upoważnienie zostaje wydane na czas nieokreślony.

lub

upoważnienie obowiązuje od dnia: do dnia:

Osoby którym nadawane jest upoważnienie:

1)

2)

3)

...) (w kolejnych pozycjach należy podać imiona i nazwiska osób, którym nadawane jest upoważnienie, ilość pozycji jest nieograniczona, o ile zakres nadawanego upoważnienia jest ten sam.).

Data : (data pozornie nie jest konieczna, jednak jej umieszczenie daje właściwie postępującemu administratorowi danych osobowych lepszą pozycję w ewentualnym sporze).

Podpis osoby reprezentującej administratora danych:

(podpis nie jest konieczny, w upoważnieniu mającym formę nadania uprawnień do systemu umieszczenie podpisu jest niemożliwe, w upoważnieniu papierowym, z ostrożności lepiej jest umieścić podpis).

Druga faza nadawania uprawnienia do przetwarzania danych osobowych może zostać (a tak przynajmniej uważają zgodnie obaj autorzy tej książki) zrealizowana przez nadanie loginu do systemu informatycznego.

Stosowne wzory związane z loginem proponujemy na kolejnych stronach. Dobrą praktyką jest usystematyzowanie procesu nadawania, cofania, aktualizowania loginów dostępowych, przyznawanych poszczególnym upoważnionym. Ważne jest również, aby zakres uprawnień w ramach danego systemu teleinformatycznego odpowiadał rzeczywistemu zakresowi upoważnienia. Przekazanie osobie odpowiedzialnej informacji w tym zakresie w sposób precyzyjny pozwoli na poprawne wypełnienie obowiązku nadania login, a co za tym idzie i uprawnień w adekwatnym zakresie do upoważnienia¹⁴³.

¹⁴³ Rzeczywistość pokazuje, iż w praktyce spotkać można się z licznymi praktykami, których stosowanie uznać należy za nieprawidłowe. Dla przykładu można wymienić tutaj praktykę polegającą na posługiwaniu się przez kilku pracowników upoważnionych do przetwarzania danych w systemie teleinformatycznym tym samym, czyli jednym loginem dostępowym, który jest im znany, tak samo, jak jest im znane hasło zabezpieczające, w rzeczywistości jednak login przypisany jest tylko do jednego konkretnego pracownika. Wskazać także należy na inny przykład nieprawidłowych praktyk, przejawiający się w tym, iż za upoważnionego pracownika, któremu przyznany został login dostępowy, zmianę haseł zabezpieczających dokonuje osoba trzecia. Błędną praktyką także jest posługiwanie się przez upoważnionych pracowników jednym i tym samym hasłem dla swoich loginów, które jest powszechnie znane. Warto także wspomnieć, iż odnotowywanie haseł zabezpieczających na kartkach umieszczanych np. pod klawiaturą komputera, na monitorach, czy na tablicach wewnątrz pomieszczeń jest niedopuszczalne. Za nieprawidłową również uznać należy praktykę przypisywania do wielu kont użytkowników danego systemu teleinformatycznym uprawnień realizowanych z wykorzystaniem innego użytkownika, korzystającego z innego konta systemu teleinformatycznego. Prowadzi to do tego, że wielu uprawnionych użytkowników korzysta wspólnie z jednego konta innego uprawnionego, dla realizacji określonego zadania. W praktyce występować może takie zjawisko przy systemie eWUŚ Elektroniczna Weryfikacja Uprawnień Świadczeniobiorców. Zdarza się, iż aplikacje gabinetowe konfigurowane są w taki sposób, iż uprawnienia jednego użytkownika eWUŚ wykorzystywane są przez kilku użytkowników aplikacji gabinetowej. Od strony jednak systemu eWUŚ nadal widoczne jest, iż to wyłącznie osoba użytkownika po jego stronie uprawnionego korzysta z systemu, a nie kilku użytkowników uprawnionych tylko po stronie aplikacji gabinetowej. (Przypis: D.S.)

....., dn.

**WNIOSEK O NADANIE LOGIN(u)
DO SYSTEMU INFORMATYCZNEGO**

Numer:

Działając na podstawie Polityki Bezpieczeństwa obowiązującej
w: wnoszę o przyznanie uprawnień względem nw.
użytkownika w określonym zakresie:

.....

(imię i nazwisko użytkownika)

.....

(stanowisko służbowe / numer prawa wykonywania zawody – jeśli wymagane)

Informacje ADO	
Numer stanowiska komputerowego według wykazu – jeśli możliwe do wskazania.	
Oznaczenie lokalizacji stanowiska komputerowego – jeśli możliwe do wskazania.	
Czy sprzęt wykorzystywany będzie poza obszarem przetwarzania określonym jako siedziba jednostki:	
Bezpośredni przełożony użytkownika:	
Okres udzielenia upoważnienia, określający okres na jaki należy nadać uprawnienia użytkownika do systemu informatycznego.	
Powierzono sprzęt komputerowy przenośny (laptop), tablet, telefon: numer seryjny, marka, rodzaj, opis identyfikujący.	
Potrzebne oprogramowanie (nazwy programów/systemów, do których upoważniony ma mieć dostęp w związku z wykonywaniem powierzonych czynności, zadań	
..... /data i podpis administratora danych / osoby upoważnionej/	

**POTWIERDZENIE REALIZACJI WNIOSKU
O NADANIE LOGIN(u)
DO SYSTEMU INFORMATYCZNEGO**

Dnia utworzono konto użytkownik
ze zdefiniowanymi rolami, adekwatnie do. danych wskazanych we wniosku:

Nazwa oprogramowania (nazwy programów/systemów, do których upoważniony ma mieć dostęp w związku z wykonywaniem powierzonych czynności, zadań	Login użytkownika
1.	1.
2.	2.
3.	3.
4.	4.
5.	5.
Dnia skonfigurowano i sprawdzono sprzęt.	
Powierzono sprzęt komputerowy przenośny (laptop), tablet, telefon: numer seryjny, marka, rodzaj, opis identyfikujący.	
Przyznano dostęp do służbowej poczty elektronicznej email.	@.....
Podpis ASI	

Praktyka pokazuje, iż sytuacje, w których następuje faktyczny brak dostępu do systemu informatycznego spowodowany działaniami / zaniechaniami upoważnionych pracowników nie należy do rzadkości. O ile taki brak dostępu jest spowodowany tym, że pracownik zapomniał swojego hasła to, taką sytuację należy zakwalifikować, jako wymagająca prostej interwencji. Jednak jeśli, taki brak dostępu stanowi następstwo tego, iż zagubiono np. kartkę na której zostały zapisane hasła dostępowe, taka sytuacja wymaga innej już reakcji ze strony administratora. Należy mieć także na uwadze sytuacje, które pozornie mogą wyglądać na nieskomplikowane. Nie zawsze informacja o braku możliwości wykonania autoryzowanego logowania w związku z zapomnieniem hasła, oznacza iż użytkownik faktycznie hasło zapomniał. Nie można bowiem wykluczyć, iż w takiej sytuacji mogło np. dojść do zmiany hasła przez osobę nieuprawnioną, która uprzednio weszła w posiadanie danych umożliwiających jej dostęp do systemu, które użytkownik wskazuje, iż zapomniał. Ponadto częstym zjawiskiem jest informowanie przez użytkowników np. telefonicznie, czy ustnie o braku możliwości dokonania autoryzowanego logowania do pionów IT swoich jednostek bez jednoczesnego informowania o przyczynach wystąpienia takiego stanu. Warto jest przeanalizować w jednostce częstotliwość występowania takich zjawisk i podjąć stosowne kroki mogące im zapobiegać. Z tego względu przygotowaliśmy procedurę, która opisuje zasady postępowania w wyżej opisanych przypadkach.

PROCEDURA RESETOWANIA HASŁA I NADAWANIA NOWEGO HASŁA STARTOWEGO DO SYSTEMU CELEM PRZYWRÓCENIA DOSTĘPU

1. **[Podstawa prawna]** Działając na podstawie Polityki Bezpieczeństwa wprowadza się Procedurę resetowania i ustanawiania powtórnego hasel dostępowych dla Użytkowników do elementów składowych systemu informatycznego Jednostki.
2. **[Zakres stosowania]** Procedura niniejsza określa sposób postępowania Użytkownika oraz Jednostki w sytuacji konieczności zresetowania dotychczasowego hasła Użytkownika do elementu systemu informatycznego w związku z jego zapomnieniem oraz ustanowienia nowego hasła.
3. **[Definicja hasła]** Zgodnie z Polityką Bezpieczeństwa hasło to ciąg znaków literowych, cyfrowych lub innych, przypisany do Identyfikatora Użytkownika, znane jedynie osobie uprawnionej do pracy w Systemie Informatycznym.
4. **[Nadawanie i zmiana uprawnień]** W zakresie nadawania uprawnień po raz pierwszy do przetwarzania danych osobowych w systemie informatycznym stosuje się Procedurę określoną w Polityce Bezpieczeństwa.
5. **[Procedura – resetowania hasła]** W przypadku kiedy nie jest możliwe zalogowanie się Użytkownika do danego elementu systemu informatycznego w związku z zapomnieniem przez niego przyznanego mu hasła, bądź utrata jego ważności na skutek nie dokonania zmiany, zobowiązany jest on do bezzwłocznego poinformowania o powyższym Administratora Danych Osobowych, bądź bezpośredniego przełożonego. W przypadku podjęcia decyzji przez Administratora Danych Osobowych o zasadności zresetowania hasła i ustanowienia nowego hasła startowego dla Użytkownika sporządza on „**Wniosek o reset hasła i nadanie nowego hasła startowego do systemu celem przywrócenia dostępu**” i przekazuje go służbom właściwym, jako dokument podpisany w postaci papierowej. Służby uprawnione po spełnieniu dyspozycji wniosku przekazują bezpośrednio Użytkownikowi uprawnionemu nowe hasło, tak gdzie system informatyczny nie posiada funkcjonalności wymuszającej zmianę hasła startowego przy pierwszym logowaniu.
6. **[Procedura – zagubiony nośnik z zanotowanym hasłem]** W przypadku, kiedy nie jest możliwe zalogowanie się Użytkownika do danego elementu systemu informatycznego, w związku z zagubieniem nośnika na którym zanotowane było hasło, stosuje się procedurę określającą zasady postępowania w przypadku naruszenia ochrony danych osobowych oraz odpowiednio procedurę resetowania hasła.
7. **[Obowiązek informowania]** Każdy Użytkownik zobowiązany jest do niezwłocznego informowania Administratora Danych Osobowych, albo Inspektora Ochrony Danych, albo swojego bezpośredniego przełożonego o stanach faktycznych uzasadniających zastosowanie procedury określającej zasady postępowania w przypadku naruszenia ochrony danych osobowych..

8. **[Weryfikacja możliwości wykorzystania login / hasła]** Jeśli jest to technicznie możliwe służby uprawnione przed zresetowaniem hasła i ustanowieniem nowego, podejmują czynności weryfikujące polegające na sprawdzeniu, czy po dacie wskazanej przez Użytkownika w jego oświadczeniu, dokonywane było skuteczne logowanie do elementu systemu informatycznego z wykorzystaniem login Użytkownika. W sytuacji stwierdzenia faktu skutecznych logowań wszczyna się procedurę określającą zasady postępowania w przypadku naruszenia ochrony danych osobowych.
9. **[Obowiązek zapoznania się z Procedurą]** Każda z osób posługująca się indywidualnym login pozwalającym na autoryzowane logowanie do elementów systemu informatycznego, zobowiązana jest do zapoznania się z treścią niniejszej procedury oraz do jej bezwzględnego stosowania.

.....

/ i podpis administratora danych / osoby upoważnionej/

WNIOSEK O RESET HASŁA I NADANIE NOWEGO HASŁA STARTOWEGO DO SYSTEMU CELEM PRZYWRÓCENIA DOSTĘPU

Działając na podstawie pkt. 5 Procedury resetowania i ustanawiania hasła do elementów systemu informatycznego, składam wniosek o zresetowanie hasła nw. Użytkownika i ustanowienie nowego hasła dostępowego do wskazanego elementu systemu informatycznego:

Dane Użytkownika

Imię i nazwisko Użytkownika	
Stanowisko	

Dane elementy systemu informatycznego

Login Użytkownika:	
Nazwa oprogramowania / systemu do którego nadany był login:	
Usytuowanie stanowiska komputerowego:	

.....
/data i podpis administratora danych / osoby upoważnionej/

OŚWIADCZENIE UŻYTKOWNIKA

Ja niżej podpisana/y, oświadczam, iż w związku z **zapomnieniem hasła*** / **zgubieniem nośnika na którym było hasło zapisane*** do ww. elementu systemu informatycznego, nie mam możliwości dokonania autoryzowanego logowania, jednocześnie oświadczam, iż brak możliwości logowania stwierdziłam/em w dniu:

.....

.....
/data i podpis Użytkownika/

ADNOTACJA DOTYCZĄCA WYKONANIA RESETU HASŁA

ADNOTACJA DOTYCZĄCA WNIOSKU O RESET HASŁA I NADANIE NOWEGO HASŁA STARTOWEGO DO SYSTEMU CELEM PRZYWRÓCENIA DOSTĘPU

Dnia wykonano reset hasła zgodnie z ww. wnioskiem oraz przekazano hasło dostępne bezpośrednio Użytkownikowi.

Wykonano* / **nie wykonano z uwagi na brak możliwości technicznych*** czynności sprawdzające oraz **nie stwierdzono*** / **stwierdzono*** fakt logowania się do elementu systemu informatycznego z wykorzystaniem login Użytkownika po dacie wskazanej przez niego w oświadczeniu.

Poinformowano ADO* dnia o nieuprawnionych logowaniach / prawdopodobieństwie ich wystąpienia.

Uwagi:

.....

.....

.....

.....
/data i podpis służb uprawnionych/

* niepotrzebne skreślić

Administrator musi mieć świadomość tego, iż wprowadzanie procedur opisujących modele postępowań związane jest z dodatkowymi czynnościami, które personel odpowiedzialny, ale i zobowiązany będą wykonywali. Odpowiednio do sytuacji należy adekwatnie reagować, czy to poprzez organizację spotkań informacyjno-edukacyjnych, czy

też poprzez zintensyfikowane monitorowanie stosowania procedury, zwłaszcza w początkowym okresie po jej wdrożeniu. Przede wszystkim personelu musi posiadać wiedzę na temat tego, jak ma realizować swoje nowe obowiązki oraz świadomość tego, w związku z czym kolejne procedury postępowania są wdrażane przez Administratora.

Proces zarządzania uprawnieniami do systemów wymaga przemyślenia i dokładnego rozplanowania

Zagadnieniem wymagającym pochylenia się nad nim i wypracowania adekwatnych metod działania w jednostce, jest proces obsługi nadawania, cofania upoważnień oraz z tym związany proces obsługi tych zadań. Z praktycznie każdą decyzją powodująca ruch kadrowy nierozzerwalnie związane będą działania administratora. Niestety dla wielu administratorów w praktyce nadawanie upoważnień, ich aktualizacja, czy cofanie, zarządzanie dokumentacją uzupełniającą, w początkowej fazie może być problematyczne. Z tego względu, aby ułatwić personelowi odpowiedzialnemu za obsługę zadania, warto jest opracować określone zasady a następnie przeszkolić personel w posługiwaniu się przygotowaną dokumentacją.

Po wprowadzeniu w życie natomiast nowych zasad, należy skrupulatnie weryfikować działania podejmowane na ich podstawie, tak aby mieć możliwość dokonania oceny poprawności zaproponowanych rozwiązań i wprowadzenia ewentualnych zmian porządkujących. Należy w szczególności interweniować w sytuacji, kiedy to personel odpowiedzialny, z opóźnieniem tworzy dokumentację związaną z upoważnieniami, albo z opóźnieniem bądź wcale jej nie aktualizuje pomimo zmiany np. sytuacji pracownika.

Należy w sposób precyzyjny wyznaczyć osoby / komórki odpowiedzialne za przygotowywanie i egzekwowanie dokumentacji. Należy mieć świadomość tego, iż z wydaniem upoważnienia wiązać będą się też inne czynności towarzyszące. Trzeba będzie przekazać jego treść upoważnionej osobie, zapoznać ją z przepisami traktującymi o ochronie danych osobowych w jednostce, odebrać od niej stosowne oświadczenie dotyczące zachowania tajemnicy, przeszkolić osobę upoważnioną w zakresie ochrony danych osobowych adekwatnie do

powierzonych jej zadań, udokumentować powyższe czynności i zabezpieczyć zgromadzoną w następstwie opisanych działań dokumentację.

W realiach medycznych upoważniony personel korzysta często z różnorodnych aplikacji informatycznych. Wymaga to wprowadzenia i stosowania sprawnego systemu zarządzania przyznanymi uprawnieniami. Najczęściej osobami odpowiedzialnymi za powyższe będą służby informatyczne jednostki działające w ramach jej struktury, bądź wyznaczone osoby, albo też personel zewnętrznego podmiotu informatycznego. W każdym z opisanych przypadków należy opracować adekwatną metodę przepływu informacji i podejmowania decyzji w zakresie działań zmierzających do nadania, cofnięcia czy aktualizacji uprawnień użytkownika w ramach aplikacji. Bez wątpienia przyznawanie uprawnień użytkowników nie może być oderwane od zakresu upoważnienia do przetwarzania danych osobowych, jeśli w danych systemie teleinformatycznych faktycznie przetwarzane są dane osobowe. To samo dotyczy ich cofnięcia, czy zmiany zakresu. Na marginesie należy zwrócić uwagę na element, jakim jest konieczność dostosowania zakresu uprawnień użytkownika w danej aplikacji do zakresu upoważnienia. Przyznanie zatem adekwatnych uprawnień użytkownikowi w ramach tworzonego dla niego dostępu do systemu uznać należy za element realizujący nadane mu upoważnienie do przetwarzania danych. Wymusza to na osobach odpowiedzialnych za realizację tych zadań skrupulatne weryfikowanie zakresu upoważnienia i adekwatne przyznawanie uprawnień w systemie względem każdego upoważnionego. Warto wybiegając w przyszłość zorganizować także w sposób prawidłowy i przemyślany procedurę postępowania w związku z koniecznością zmiany hasła dostępowego względem konta danego użytkownika. Kierując się doświadczeniem przyjąć należy, iż będą mieć miejsce sytuacje polegające na tym, że upoważniony personel zapomni hasła dostępowego, zablokuje konto, bądź, co gorsza, zgubi hasło, jakie samodzielnie zanotował.

Problematycznym okazać może się wypracowanie prawidłowych praktyk personelu polegających na samodzielnym zgłaszaniu tego faktu wskazanym służbom informatycznym. Personel, bądź bagatelizuje takie sytuacje, bądź stara się je ukryć i odroczyć w czasie fakt zgłoszenia braku możliwości zalogowania się do systemu aplikacyjnego. Należy rozróżnić przyczyny powstania braku takiej możliwości i stosować adekwatne środki naprawcze. Najgroźniejszą z pun-

ktu widzenia możliwości wystąpienia naruszenia ochrony zasad bezpieczeństwa będzie sytuacja zagubienia zanotowanych haseł dostępowych, czy to na papierze, czy to na nośniku elektronicznym np. w telefonie, który został skradziony zgubiony.

Nadanie uprawnień do nadawania upoważnień do przetwarzania danych osobowych

Jeżeli upoważnienie do przetwarzania danych osobowych nie zostaje podpisane przez osobę kierującą podmiotem, dyrektora szpitala, przychodni, rektora uczelni medycznej, to należy się spodziewać, że podmiot kontrolujący zażąda przedstawienia dokumentu z którego wynika, że osoba podpisująca upoważnienie, osoba nadająca upoważnienie ma prawo ten dokument skutecznie podpisać, że osoba ta ma prawo nadać upoważnienie w imieniu ADO. Dokument ten może mieć charakter polecenia służbowego, upoważnienia do nadawania i podpisywania upoważnień do przetwarzania danych osobowych itp. Dokument ten należy przechowywać tak długo jak upoważnienie do przetwarzania danych osobowych.

Dokument nadania uprawnień do nadawania upoważnień do przetwarzania danych osobowych

Kierujący ADO: (tu należy podać imię i nazwisko osoby kierującej ADO – wójta, dyrektora, prezesa)

poleca

panu/pani: (tu należy podać imię i nazwisko osoby, która nadaje i podpisuje upoważnienia)

nadawanie upoważnień do przetwarzania danych osobowych w :
... .. (tu należy podać nazwę ADO)

Polecenie obowiązuje od dnia: do dnia:

Data: (data pozornie nie jest konieczna, jednak jej umieszczenie daje właściwie postępującemu administratorowi danych, lepszą pozycję w ewentualnym sporze).

Podpis osoby kierującej ADO: (podpis nie jest konieczny, z ostrożności lepiej jest go umieścić).

Uwaga

Nadawać i uchylać upoważnienia, nadawać i uchylać polecenia może ta sama osoba, zatem uprawnienia do tych czynności nie muszą być nadawane przez kierującego podmiotem, w osobnych dokumentach, wystarczy jeden.

Osoba nadająca upoważnienia

Z RODO nie wynika, kto ma nadawać upoważnienia i kto ma wydawać polecenia. Art. 29 RODO zatytułowany jest „Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego”, zaś sam art. 29 RODO stanowi w istotnym dla prowadzonych rozważań zakresie: „(...) każda osoba działająca z upoważnienia administratora (...)”. Pozornie wynika z tego, że upoważnienia nadaje administrator. Niestety, z punktu widzenia praktyki, nic to nie wyjaśnia. Jeżeli przyjmujemy, że administratorem jest szpital, przychodnia, uczelnia, to nadal nie wiadomo kto, tak naprawdę, ma upoważnienie nadać. Która osoba. Pierwsze nasuwające się rozwiązanie jest takie, że upoważnienie powinna nadawać osoba kierująca ADO. Nadanie upoważnienia przez osobę kierującą ADO – w imieniu ADO jest tylko częściowym rozwiązaniem, jeżeli bowiem jest konieczność nadania dużej (cokolwiek to znaczy) liczby upoważnień, to nadawanie przez kierującego ADO osobiście po prostu kłóci się z rozumem. ADO powinien to nadawanie komuś polecić. Patrząc przez pryzmat RODO, nie sposób uczciwie powiedzieć, komu nadawanie upoważnień można polecić, a komu nie. W zasadzie można to polecić każdemu.

Poza tym niebezpieczne dla dyrektora jest osobiste realizowanie obowiązków administratora danych, bo porcesowo daje mu to złą pozycję. PUODO może uznać, że jest on administratorem i nałożyć na niego karę. Najbezpieczniej jest uznawać za administratorem danych jest szpital, uczelnia, przychodnia. Gorzej – osoba kierująca. Najgorzej – osoba kierująca wymieniona z nazwiska i imienia.

Nadawanie upoważnień do przetwarzania danych osobowych przez inspektora ochrony danych

Z moich obserwacji wynika, że osoby, które zajmują się ochroną danych osobowych, często zadają sobie pytanie o to, czy IOD może nadawać upoważnienia do przetwarzania danych osobowych.

Uważam, że na gruncie RODO nie ma przepisu, którego przyzwoita wykładnia prowadziłaby do wniosku, że osoba, która jest IODem, nie może nadawać upoważnień. Uważam, że z samego faktu bycia wyznaczonym na IODa, na podstawie art. 37 RODO, nie wynika dla osoby wyznaczonej na IODa uprawnienie do nadawania upoważnień do przetwarzania danych osobowych. Jeżeli ktoś ma nadawać, czy wycofywać upoważnienia do przetwarzania danych osobowych, to należy mu to polecić, nieistotne jest tu, czy osoba ta jest IODem, czy nie.

By nie pozostawić niedosytu Czytelnikom, należy się jeszcze zastanowić, czy nic w RODO nie stoi na przeszkodzie, by osobie, którą wyznaczono na IODa polecać nadawanie upoważnień do przetwarzania danych osobowych.

Z art. 38 ust. 3 RODO wynika, że ADO ma obowiązek zapewnić, by IOD nie otrzymywał instrukcji dotyczących wykonywania swoich zadań. Przepis ten następuje jednak po art. 38 ust. 2 RODO, który stanowi o zadaniach IODa, „o których mowa w art. 39”, z kolei wspomniany wyżej art. 38 ust 3 RODO zakazuje wydawania IODowi instrukcji „dotyczących wykonywania tych zadań”, „tych” czyli wskazanych w art. 38 ust 2 RODO, czyli wymienionych w art. 39 RODO. Z omówionej płataniny przepisów nie wynika jednak by osobie, która jest IODem, nie wolno było wydawać poleceń w zakresie innych zadań. Idąc dalej, należy stwierdzić, że jeżeli ADO poleca osobie, która jest IODem, nadawanie upoważnień do przetwarzania danych osobowych, to nie jest to sprzeczne z wnioskami wynikającymi z art. 38 ust 3 RODO w zw. z art. 38 ust. 2 RODO w zw. z art. 39 RODO. Artykuł 38 ust. 6 RODO stanowi: „Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator danych lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.”. Niestety przepis ten jedynie z pozoru zawiera treść, kiedy bowiem staramy się zrozumieć, co ten przepis tak naprawdę nakazuje, czego zakazuje, jakie uprawnienie lub obowiązek opisuje, to okazuje się, że dopuszczalność wykonywania innych zadań przez IODa uzależniono od tego, czy powodowałyby one konflikt interesów, czyli nie wiadomo od czego. Pragnąc uzasadnić racjonalność postępowania prawodawcy, należy stwierdzić, że w art. 38 ust. 6 RODO umieszczono kryterium ocenne, od którego uzależniono jakie obowiązki może wykonywać IOD. Brzmi to lepiej, jednak nadal nie wiadomo jakie obowiązki może wykonywać osoba, która jest IODem. Analiza art. 39 ust 1 RODO, wskazuje, że jeżeli

chcemy uzasadnić, że IOD nie może nadawać upoważnień, to należy to uzasadnić treścią art. 39 ust 1 lit. b RODO, z którego wynika, że obowiązkiem IODa jest m.in. monitorowanie przestrzegania RODO i innych przepisów, oraz prowadzenie audytów. Można stwierdzić, że jeżeli IOD nada upoważnienie, a prócz tego musi monitorować, czy zostało ono nadane i przeprowadzić audyt nadanych upoważnień, to skutkuje to konfliktem interesów, zatem IOD nie może nadawać upoważnień. Rozumowanie zostało świadomie przeprowadzone tak by dowieść założonej tezy, że IOD upoważnień nadawać nie może. Zostało ono zatem przeprowadzone tu przeze mnie celowo nieuczciwie.

Uważam, że z omówionych wyżej pokrótce przepisów RODO nie wynika, że osoba, która jest IOD nie może nadawać upoważnień. Również „Wytyczne dotyczące inspektorów ochrony danych”¹⁴⁴, autorstwa Grupy Roboczej art. 29 ds. ochrony danych, nie są przesądzające w tej mierze. Mimo poprowadzonych tu rozważań, należy się liczyć z tym, że kontrolujący ADO pracownicy organu ochrony danych będą chcieli, podczas przeprowadzanych kontroli, wykazać naruszenia przepisów RODO. Tak po prostu jest, że taka jest często praktyka pracowników organów kontroli i nadzoru. Jeżeli u kontrolowanego ADO, nadał upoważnienia IOD, to kontrolerzy mogą przeprowadzić zaprezentowane powyżej rozumowanie, które określiłem jako celowo nieuczciwe, aby wykazać, że ADO prawo naruszył¹⁴⁵. Jaka będzie praktyka kontrolowania przestrzegania RODO, tego w momencie pisania tej książki, z racji czasu jej pisania nie wiem, ni wiedzieć nie mogę. Mając na uwadze przeprowadzone powyżej rozważania, uważam, że lepiej by IOD nie nadawał upoważnień do przetwarzania danych osobowych. Wniosek ten nie wpływa z argumentów merytorycznych, a jedynie z ostrożności.

¹⁴⁴ Korzystałem z wersji dostępnej ze strony: <https://giodo.gov.pl/pl/1520285/9740> (dostęp 10.11.2018 godz. 00.34.)

¹⁴⁵ Popelniał przy tym błąd aprioryzmu.

**Uchylenie/ustanie upoważnienia
do przetwarzania danych osobowych, dokument:
uchylenia, odebrania, wycofania, stwierdzenia nieważności
upoważnienia do przetwarzania danych osobowych**

Upoważnienia i polecenia, które już nie są potrzebne, należy dla porządku wycofać i zachować na papierze dowód tego wycofania. Można to robić z użyciem wskazanych niżej dokumentów.

Dokument uchylenia upoważnienia do przetwarzania danych osobowych, (inaczej dokument: *ustania, odebrania, wycofania, stwierdzenia nieważności upoważnienia do przetwarzania danych osobowych*)

Dokument odnosi się do upoważnienia nr:

nadanego pani/panu:

Administrator danych: (słowa: „administrator danych” mogą być zastąpione pełną nazwą administratora danych, lub pełna nazwa administratora zostaje dodana do słów: „administrator danych”).

uchyla upoważnienie do przetwarzania danych osobowych wskazane wyżej.

Data: (data pozornie nie jest konieczna, jednak jej umieszczenie daje właściwie postępującemu administratorowi danych lepszą pozycję w ewentualnym sporze).

Podpis osoby reprezentującej administratora danych osobowych: (podpis nie jest konieczny, w upoważnieniu mającym formę nadania uprawnień do systemu umieszczenie podpisu jest niemożliwe, w upoważnieniu papierowym, z ostrożności lepiej jest umieścić podpis).

**Uprawnienie do uchylenia upoważnień
do przetwarzania danych osobowych**

Jeżeli dokument uchylenia upoważnienia do przetwarzania danych osobowych nie zostaje podpisany przez osobę kierującą podmiotem, jeżeli uchylenia upoważnienia do przetwarzania danych osobowych nie wykonuje osobiście osoba kierująca podmiotem, to należy się spodziewać, że podmiot kontrolujący zażąda przedstawienia dokumentu, z którego wynika, że osoba podpisująca dokument uchylający upoważnienie, osoba uchylająca upoważnienie, ma prawo ten

dokument skutecznie podpisać, że osoba ta ma prawo uchylić upoważnienie w imieniu ADO.

Dokument nadania uprawnień do uchylania upoważnień do przetwarzania danych osobowych

Kierujący ADO *(tu podajemy imię i nazwisko osoby kierującej ADO – wójta, dyrektora, prezesa)*

poleca

panu/pani *(tu podajemy imię i nazwisko osoby, która nadaje i podpisuje upoważnienia)*

uchylanie *(odbieranie, wycofywanie itd.)* upoważnień do przetwarzania danych osobowych w *(tu podajemy nazwę ADO).*

Polecenie obowiązuje od dnia do dnia

Data *(data pozornie nie jest konieczna, jednak jej umieszczenie daje właściwie postępującemu ADO, lepszą pozycję w ewentualnym sporze).*

Podpis osoby kierującej ADO..... *(podpis nie jest konieczny, z ostrożności lepiej jest go umieścić).*

Dokumentowi można nadać wszelkie cechy formalne dokumentu wewnętrznego, nadawane takim dokumentów w danym ADO.

Możliwe błędy

Błędem jest brak upoważnień. (Chyba, że ADO uznaje, że upoważnienia są niepotrzebne, a sprawę dwuetapowego uprawnienia do przetwarzania danych osobowych załatwia inaczej niż za pomocą systemu upoważnień i poleceń.)

Błędem jest brak upoważnień i jednocześnie zastępowanie ich za pomocą innych dokumentów, na przykład za pomocą klauzuli w umowie o pracę, za pomocą polecenia przetwarzania danych osobowych lub za pomocą jeszcze innych dokumentów.

Błędem jest, jeżeli zakres upoważnień nie pokrywa się z zakresem przetwarzania danych osobowych przez konkretne upoważnione osoby.

Błędem jest nadawanie upoważnień nieimiennych, upoważnień dla osób wskazanych rodzajowo.

Błędem jest nadawanie upoważnień przez osoby, które nie posiadają uprawnień do nadawania upoważnień do przetwarzania danych osobowych, uprawnienia te nadaje kierujący jednostką.

Błędem jest nadawanie upoważnień wyłącznie w systemie informatycznym, jeżeli w podmiocie wykonywane są również czynności poza tym systemem.

Uwaga

Nadawanie i uchylanie upoważnień można zlecić tej samej osobie, w związku z czym również uprawnienie do nadawania upoważnień i uprawnienie do uchylania upoważnień mogą być nadawane na podstawie jednego dokumentu, wystarczy wtedy miast oddzielnego tworzenia dwóch dokumentów: dokumentu nadania uprawnień do nadawania upoważnień do przetwarzania danych osobowych i dokumentu nadania uprawnień do uchylania upoważnień do przetwarzania danych osobowych stworzyć jeden dokument, a to: dokument nadania uprawnień do nadawania i uchylania upoważnień do przetwarzania danych osobowych.

Polecenie przetwarzania danych osobowych¹⁴⁶

Źródło obowiązku

Obowiązek nadania polecenia przetwarzania danych osobowych wynika z art. 29 RODO. Obowiązek nadania polecenia przetwarzania danych osobowych wynika również z art. 32 ust. 4 RODO.

Art. 29 RODO ustanawia nowe zjawisko, nową instytucję – przetwarzanie danych osobowych wyłącznie na polecenie administratora. Osobom, które upoważniono do przetwarzania danych osobowych i które mają dostęp do tych danych, wolno przetwarzać dane osobowe wyłącznie na polecenie administratora. W realiach codziennej pracy administratora nie sposób wyobrazić sobie, że każda czynność przetwarzania danych osobowych poprzedzona będzie poleceniem wykonania tej czynności – poleceniem przetwarzania. Trudno sobie wyobrazić, tym niemniej nie sposób nie zauważyć pojawienia się opisywanego, nowego obowiązku. Uważam, że najlepszym sposobem realizacji tego obowiązku jest sporządzenie przez administratora danych odpowiednich dokumentów, w których administrator poleca przetwarzanie danych osobowych lub kategorii danych osobowych.

Na gruncie RODO ustanowiono więc nie tylko obowiązek nadawania upoważnień do przetwarzania danych osobowych, ale ustanowiono również obowiązek wydawania poleceń przetwarzania danych osobowych. Uważam, że obydwa te obowiązki można zrealizować w jednym dokumencie, w którym administrator danych upoważnia do przetwarzania konkretnych kategorii danych i w którym administrator poleca osobie upoważnionej przetwarzanie tych kategorii danych. Oczywiście nic nie stoi na przeszkodzie, by wydawać dwa osobne dokumenty.¹⁴⁷

¹⁴⁶ Obowiązek wydawania polecenia przetwarzania danych osobowych jest analogiczny do obowiązku nadawania upoważnienia do przetwarzania danych osobowych, z tego m.in. względu lwią część rozważań prowadzonych w niniejszym rozdziale została skopiowana z rozdziału poświęconego upoważnieniom, uczulam Czytelników, że między upoważnieniem a poleceniem pewne różnice zachodzą, warto więc obydwa rozdziały czytać uważnie, z racji tych właśnie różnic.

¹⁴⁷ Tekst zawiera fragmenty mojego (J. Rz.) artykułu *Upoważnienia do przetwarzania danych w RODO*, opublikowanego w numerze 7/2017 It w administracji.

Dokument polecenia przetwarzania może wyglądać tak samo jak dokument upoważnienia tyle że administrator w dokumencie tym nie upoważnia do przetwarzania danych a poleca by dane przetwarzano. Wyżej, na początku rozdziału: „Upoważnienie do przetwarzania danych osobowych” wyjaśniamy, że nadawanie pisemnych upoważnień i wydawanie pisemnych poleceń nie jest obowiązkiem, który wynika z RODO, rozważań tych nie powtarzamy. Zwracamy tu jedynie uwagę na pozornie prosty fakt, że co prawda upoważnień nie trzeba nadawać, poleceń nie trzeba wydawać, jednak sprawę upoważnienia i polecenia trzeba jakoś załatwić. Załatwić i udokumentować.

Wskazanie osób uprawnionych do odwrócenia pseudonimizacji

Źródło obowiązku

Obowiązek wskazania osób uprawnionych do odwrócenia pseudonimizacji wynika z mot. 29 Preambuły RODO. Przepis ten zachęca do stosowania pseudonimizacji, jednak pseudonimizacji, która korzysta ze środków pseudonimizacyjnych umożliwiających ogólną analizę. Przepis nie wyjaśnia niestety, czym jest owa ogólna analiza, wydaje się jednak że to analiza danych niespseudonimizowanych. Jednocześnie przepis dopuszcza stosowanie takiej odwracalnej pseudonimizacji pod dwoma warunkami. Pierwszy z nich jest taki, że RODO ma być wdrożone w zakresie danego przetwarzania, zapewne twórcy przepisu chcieli wyrazić, że dana czynność ma być chroniona na mocy RODO, czyli na przykład ujęta w rejestrze czynności przetwarzania, ktoś ma być upoważniony do jej wykonywania itd. Drugi warunek jest taki, że dodatkowe informacje pozwalające przypisać dane osobowe konkretnej osobie, której dane dotyczą, mają być przechowywane osobno. Ponadto, co jest szczególnie istotne dla celu niniejszego wywodu, przepis zawiera zdanie: „Administrator przetwarzający dane osobowe powinien wskazać osoby uprawnione.”. Zapewne mowa tu o osobach uprawnionych do odwrócenia pseudonimizacji.

Sama pseudonimizacja zdefiniowana jest w art. 4 pkt 5 RODO. Pseudonimizacja oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami

technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Możliwość odwrócenia pseudonimizacji jest o tyle istotna, że jeżeli danych nie można przypisać konkretnej osobie fizycznej, to nie są to dane osobowe, jeżeli zaś, co wynika z mot. 26 Preambuły RODO, spseudonimizowane dane osobowe można przypisać osobie fizycznej przy użyciu dodatkowych informacji, to dane te są danymi osobowymi.

Pojęcie odwrócenia pseudonimizacji zawarte jest w mot. 75 Preambuły RODO i w mot. 85 Preambuły RODO. W obu tych przepisach mowa jest m.in. o nieuprawnionym odwróceniu pseudonimizacji, rozumianym jako szkoda (raczej niemajątkowa) u osoby fizycznej. Przypominam, że zaistnienie szkody niemajątkowej u osoby fizycznej może skutkować możliwością uzyskania od administratora lub podmiotu przetwarzającego odszkodowania za poniesioną szkodę, co wynika z artykułu 82 RODO. Z tego m.in. względu nie należy lekceważyć obowiązku sporządzenia dokumentu wskazania osoby uprawnionej do odwrócenia pseudonimizacji. Odwracanie pseudonimizacji jako czynność wykonywana wobec danych osobowych jest czynnością przetwarzania danych osobowych, a tym samym teoretycznie możliwe jest ujęcie odwracania pseudonimizacji w upoważnieniu do przetwarzania danych osobowych. Jest ono możliwe i uważam, że jeżeli ktoś zostanie w swoim upoważnieniu do przetwarzania danych osobowych upoważniony do odwracania pseudonimizacji, to wygra przed sądem ewentualny spór, ponieważ różnica między upoważnieniem do dokonania odwrócenia pseudonimizacji a wskazaniem osoby uprawnionej do dokonania odwrócenia pseudonimizacji jest, moim zdaniem, pomijalna. Mimo tego uważam, że z ostrożności należy wskazywać osoby uprawnione do odwracania pseudonimizacji, jeżeli zjawisko odwracania pseudonimizacji w podmiocie zachodzi.

Polityka ochrony

Polityka ochrony

Źródło obowiązku

Z RODO nie wynika obowiązek posiadania polityki ochrony, jednak jest o niej mowa w tym akcie prawnym. Niżej wskazujemy dlaczego warto politykę ochrony posiadać, wskazujemy również jedną z możliwości jej stworzenia.

Artykuł 24 RODO, zatytułowany: „Obowiązki administratora”, stanowi:

- „1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądowi i uaktualniane.
2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.”

Z przepisu wynika, że administrator ma obowiązek uwzględnić „charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia”. Dalej przepisie czytamy o celu działania administratora celem jest zatem: „aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać”. Z przepisu wynika, że administrator ma obowiązek wdrożenia środków, technicznych i organizacyjnych i obowiązek wykazania, że administrator te środki wdrożył. Że wdrożył środki, za pomocą których wykaże, że przetwarzanie danych osobowych w organizacji odbywa się zgodnie z RODO.

Polityka ochrony jako narzędzie rozliczalności

Najlepszym sposobem wykazania realizacji technicznej strony obowiązku jest przeprowadzenie ocen ryzyka i sporządzenie ogólnego opisu technicznych i organizacyjnych środków bezpieczeństwa.

Dokument ten jednak zwykle nie zapewnia realizacji obowiązku wykazania realizacji zasad z art. 5 ust. 1 RODO. Przypominam, że z art. 5 ust. 2 RODO wynika, że realizację zasad wykazać trzeba. Należy przy tym pamiętać, że zasady można zrealizować jedynie dzięki realizacji odpowiadających im przepisów szczególnych RODO. Administrator realizuje przepisy szczególne RODO i tym samym realizuje zasady, to jednak nie wystarczy. Oprócz realizacji zasad administrator musi wykazać, że je realizuje. Wynika to z art. 5 ust. 2 RODO. Ponieważ, jak piszę wyżej, zasady są realizowane przez realizację przepisów szczególnych, jedynym sposobem wykazania, że zasady są realizowane jest wykazanie realizacji tych właśnie przepisów szczególnych. Innej drogi nie ma. Najlepszym, z kolei, sposobem wykazania, że przepisy szczególne są realizowane jest drobiazgowo opisanie tego, jak dany administrator przepisy realizuje i jednocześnie wskazanie, realizacja którego przepisu służy realizacji której zasady.

Brak wykazania realizacji zasad zagrożony jest karą administracyjną. Najlepszym dokumentem do opisanie realizacji zasad jest polityka ochrony danych. Najlepszym dlatego, że jest to dokument występujący w RODO. Realizację zasad można też opisać w innych, stworzonych przez administratora dokumentach, o jednym należy jednak pamiętać, a mianowicie o tym, że posiadanie sposobu wykazania realizacji zasad jest obowiązkiem każdego administratora.

Polityka ochrony

jako narzędzie odwrócenia ciężaru dowodu

Polityka ochrony jest nie tylko narzędziem rozliczalności. Polityka ochrony jest również niezwykle wygodnym narzędziem odwrócenia ciężaru dowodu, w sytuacji kontrolnej. Na pytanie kontrolera o to czy i jak administrator realizuje ten czy inny przepis, administrator może po prostu wskazać odpowiedni fragment polityki ochrony, lub innego dokumentu, w którym administrator opisuje jak dany przepis realizuje. W takiej sytuacji kontroler może oczywiście sprawdzać, czy to co administrator napisał jest prawdą i doszukiwać się tych sfer działalności administratora, w których narusza on RODO. I o to właśnie chodzi, by odwrócić ciężar dowodu i zmusić kontrolera do odszukania ewentualnego naruszenia.

Dla łatwiejszego zrozumienia poszczególnych elementów polityki umieszczono w niej krótkie charakterystyki poszczególnych zasad, zaczerpnięte z książki¹⁴⁸ J. Rzymowskiego. W konkretnej polityce ochrony dobrze jest je pozostawić. Treść poszczególnych zasad nie jest czasem oczywista, więc taki element polityki może pomóc w ewentualnych sporach z kontrolerem, czy nawet tylko z pracownikami własnej organizacji administratora.

Sporządzenie polityki ochrony jest dość prostym, choć żmudnym zajęciem.

Sporządzić politykę ochrony należy w opisany poniżej sposób.

- a) Najpierw należy wypisać po kolei zasady z art. 5 ust. 1 RODO, na przykład na kolejnych stronach papieru. Można posłużyć się przy tym listą zasad zaproponowaną przeze poniżej.

„Zasada zgodności z prawem.

Zasada rzetelności.

Zasada przejrzystości.

Zasada ograniczenia celu.

Zasada minimalizacji danych.

Zasada prawidłowości.

Zasada ograniczenia przechowywania.

Zasada integralności

Zasada poufności.”

- b) Następnie pod każdą wypisaną zasadą należy wypisać przepisy, które tę zasadę realizują. Przepisy te są w niniejszym wzorze wymienione, wraz z krótkimi opisami. Odpowiednie przepisy wypisujemy poniżej.

- c) Następnie należy przy każdym odnotowanym przepisie dokładnie opisać jak przepis ten jest przez danego administratora realizowany. Ten element pozostawiamy niewypełniony, każdy administrator musi wypełnić go sam. Przy realizacji tego etapu istotne jest by opis realizacji przepisów nie był fantazją administratora, ale by dokładnie oddawał to jak administrator przepisy realizuje.

¹⁴⁸ J. Rzymowski. *RODO – GDPR. Zasady dotyczące przetwarzania danych osobowych. Zgodność przetwarzania danych osobowych z prawem*. Łódź. 2020.

Punkty „b” i „c” realizujemy w tabelach oznaczonych: „I poziom”.

- d) Następnie możliwy jest jeszcze jeden etap, a mianowicie administrator może wypisać przepisy wymienione i opisane przez nas w tabelach oznaczonych jako: „II poziom”. Są to przepisy, które nie tyle konkretyzują odpowiednie zasady ile raczej potwierdzają realizację zasad czy też jej sprzyjają. Etap ten można pominąć, mając jednak świadomość, że uczyni to politykę nieco mniej doskonałą.
- e) Następnie i tu należy przy każdym odnotowanym przepisie dokładnie opisać jak przepis ten jest przez danego administratora realizowany.

Ważne jest, by polityka ochrony oddawała rzeczywisty stan realizacji obowiązków wynikających z RODO w danym podmiocie, by była aktualna i aktualizowana. Nieaktualna polityka może być łatwo podważony jako dowód.

Dodatkowe narzędzia rozliczalności

Poza polityką ochrony, administrator może i powinien może gromadzić też wszelkie inne dowody na realizację przepisów i zasad. Realizacja wielu przepisów łączy się z tworzeniem dokumentów, dokumenty te administrator powinien gromadzić. Gromadzić, zachowując świadomość jakie przepisy szczególne i jakie zasady za pomocą konkretnych dokumentów realizuje.

Administrator może również dysponować innymi dowodami na realizację obowiązków, kopiami maili, pokwitowaniami np. przy realizacji art. 13 RODO itd. Wszystkie te dowody należy gromadzić zawczasu gdyż na etapie kontroli lub postępowania sądowego mogą być przydatne w dowodzeniu, że racja i prawo stoją po stronie administratora, nie zaś PUODO lub powoda.

Polityka ochrony

Podstawę prawną dla niniejszego dokumentu stanowi art. 24 ust. 2 RODO w zw. z przepisami powołanymi w treści dokumentu.¹⁴⁹

Administratorem danych jest:

Zasada odpowiedzialności (administratora danych)

„Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).”

Rozporządzenie RODO

Art. 5 ust. 2

Obowiązek

Art. 5 ust. 2 RODO, w zakresie zasady odpowiedzialności, nakłada na administratora obowiązek realizacji zasad wynikających z art. 5 ust. 1 RODO a co z tego wynika obowiązek realizacji przepisów RODO.

Uprawnienie

Art. 5 ust. 2 RODO, w zakresie zasady odpowiedzialności, przyznaje osobom, które dane dotyczą uprawnienie polegające na tym, że mogą oczekiwać, że administrator zrealizuje obowiązek realizacji zasad wynikających z art. 5 ust. 1 RODO a co z tego wynika obowiązek realizacji przepisów RODO.

Dokumentacja wewnętrzna potwierdzająca realizację zasady a w tym przepisów ja konkretyzujących

Zasada odpowiedzialności administratora oznacza, że administrator ma obowiązek przestrzegać zasad z art. 5 ust. 1 RODO. Zasady z art. 5 ust. 1 RODO są realizowane przez przepisy szczegółowe RODO czyli zasada odpowiedzialności administratora oznacza, że administrator ma obowiązek przestrzegać przepisów RODO.

¹⁴⁹ Treść i układ tabel: J. Rz, pomysł i układ tabel: D.S.

Zasada rozliczalności (administratora danych)
„Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”). ”
Rozporządzenie RODO
Art. 5 ust. 2
Obowiązek
Art. 5 ust. 2 RODO nakłada, w zakresie zasady rozliczalności, na administratora obowiązek wykazania przestrzegania zasad wynikających z art. 5 ust. 1 RODO.
Uprawnienie
Art. 5 ust. 2 RODO przyznaje, w zakresie zasady rozliczalności, osobom, które dane dotyczą uprawnienie polegające na tym, że mogą oczekiwać, że administrator zrealizuje obowiązek wykazania przestrzegania zasad wynikających z art. 5 ust. 1 RODO.
Dokumentacja wewnętrzna potwierdzająca realizację zasady a w tym przepisów ja konkretyzujących

Zasada rozliczalności oznacza, że administrator ma obowiązek wykazania przestrzegania zasad wynikających z art. 5 ust. 1 RODO. Zasady z art. 5 ust. 1 RODO są realizowane przez przepisy szczegółowe RODO czyli obowiązek wykazania przestrzegania zasada oznacza obowiązek wykazania przestrzegania przepisów szczegółowych RODO.

Zasada zgodności z prawem
„Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”). ”
Rozporządzenie RODO
Art. 5 ust. 1 lit. a)
Obowiązek
Art. 5 ust. 1 lit. a RODO nakłada na administratora obowiązek przetwarzania danych osobowych w sposób zgodny z prawem, czyli w zgodzie odpowiednio z art. 6 RODO lub z art. 6 RODO i z art. 9 RODO lub z art. 6 RODO i z art. 10 RODO.
Uprawnienie
Art. 5 ust. 1 lit. a RODO ustanawia uprawnienie, które przysługuje każdej osobie której dane dotyczą, polegające na tym, że osoba której dane dotyczą ma prawo oczekiwać, że jej dane osobowe są lub będą przetwarzane w zgodzie odpowiednio z art. 6 RODO lub z art. 6 RODO i z art. 9 RODO lub z art. 6 RODO i z art. 10 RODO.
Dokumentacja wewnętrzna potwierdzająca realizację zasady a w tym przepisów ja konkretyzujących

Zasada zgodności z prawem oznacza obowiązek przetwarzania danych osobowych zgodnie z art. 6 RODO lub zgodnie z art. 6 RODO i z art. 9 RODO lub zgodnie z art. 6 RODO i z art. 10 RODO.

Przetwarzanie danych osobowych zgodnie z zasadą zgodności z prawem zapisaną w art. 5 ust. 1 lit a RODO to przetwarzanie zgodne z art. 6 RODO lub zgodne z art. 6 RODO i z art. 9 RODO lub zgodne z art. 6 RODO i z art. 10 RODO¹⁵⁰, jednocześnie przetwarzanie zgodne z prawem to przetwarzanie zgodne ze wskazanymi w pierwszej części zdania przepisami RODO i zgodne z wszelkimi innymi przepisami, które dotyczą przetwarzania danych osobowych, zarówno przepisami RODO jak i przepisami innych niż RODO aktów prawnych.

¹⁵⁰ Podobnie: M. Gumularz. *Ochrona danych osobowych w sektorze publicznym. Rozdział IV. FILARY RODO. ZASADY OGÓLNE. 2. Zasady. 2.1. Zgodność z prawem, rzetelność i przejrzystość.* Warszawa 2018. Lex.

I poziom

Zasada zgodności z prawem skonkretyzowana jest przez wymienione poniżej przepisy:	Sposób realizacji przepisu konkretyzującego zasadę:
Art. 6 RODO – „Zgodność przetwarzania z prawem” – dane wolno przetwarzać przy spełnieniu jednego z warunków zawartych w art. 6 ust. 1 RODO.	
Art. 9 RODO - „Przetwarzanie szczególnych kategorii danych osobowych” – dane wolno przetwarzać przy spełnieniu jednego z warunków zawartych w art. 9 ust. 2 RODO.	
Art. 10 RODO - „Przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa” dane wymienione w przepisie, są przetwarzane zgodnie z prawem przy spełnieniu warunków zawartych w przepisie.	
Art. 29 RODO - „Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego” – istota autoryzowanego dostępu.	
Art. 32 RODO, zwłaszcza art. 32 ust. 4 RODO – „Bezpieczeństwo przetwarzania”, a w art. 32 ust. 4 RODO mowa jest o konieczności autoryzowanych działań.	
Art. 24 ust. 1 RODO – wdrożenie odpowiednich środków technicznych i organizacyjnych powinno zapewniać autoryzowane przetwarzanie a co za tym idzie, poszanowanie zasady integralności.	
Art. 32 ust. 1 lit. b – „zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania” – jako jeden z elementów technicznego zabezpieczenia danych, którego opis powinien znaleźć się w OOTiOŚB.	
Art. 28 RODO – „Podmiot przetwarzający” – przetwarzanie przez ten podmiot jest istotne w kontekście poszanowania zasady integralności, PP zwykle przetwarza w sposób autoryzowany, ale gdy jest jednoosobowy, gdy PP ma strukturę, a zwykle ma, to skutkuje to pojawieniem się zagrożeń.	

II poziom

Zasada zgodności z prawem skonkretyzowana jest również przez wymienione poniżej przepisy:	Sposób realizacji przepisu konkretyzującego zasadę:
Art. 7 RODO w zw. z art. 4 pkt 11 RODO – przy przetwarzaniu danych osobowych za zgodą.	
Art. 8 RODO – „Warunki wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego” – jeżeli Ma miejsce to przepis ten jest uzupełnieniem art. 6 ust. 1 lit a RODO.	
Art. 13 ust. 1 lit. c RODO – „Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą”, w zakresie informowania o podstawie prawnej przetwarzania, umożliwia osobom, których dane dotyczą, składanie żądań z tym związanych, co może sprzyjać realizacji zasady.	
Art. 14 ust. 1 lit. c RODO – „Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą”, w zakresie informowania o podstawie prawnej przetwarzania, umożliwia osobom, których dane dotyczą, składanie żądań z tym związanych, co może sprzyjać realizacji zasady.	
Art. 17 RODO – „Prawo do usunięcia danych („prawo do bycia zapomnianym”)” sprzyja zgodności z prawem. Usuwane zainicjowane na gruncie tego przepisu może doprowadzić do usunięcia danych, których ADO nie powinien przetwarzać.	
Art. 18 RODO – „Prawo do ograniczenia przetwarzania” – może sprzyjać zgodności z prawem.	
Art. 19 RODO – „Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania” jeżeli ADO informuje odbiorcę o usunięciu danych, lub o ograniczeniu przetwarzania, które ma na celu usunięcie danych, których przetwarzanie jest niezgodne z prawem	

Art. 20 RODO – „Prawo do przenoszenia danych” prawo do przenoszenia danych pozwala osobie, której dane dotyczą na dokładne zapoznanie się z danymi, jakie przetwarza ADO, a tym samym na skorzystanie z uprawnień, które mogą skutkować zmniejszeniem zakresu przetwarzania.	
Art. 21 RODO – „Prawo do sprzeciwu”- prawo do sprzeciwu wobec przetwarzania danych osobowych sprzyja realizacji zasady.	
Art. 25 ust. 2 RODO – „Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych”- sprzyjają realizacji zasady, ponieważ „Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.(...)”	
Art. 26 RODO – „Współadministratorzy” – ustalenia dotyczące współadministrowania mogą sprzyjać realizacji zasady, poprzez umożliwienie osobom, których dane dotyczą, składania żądań, mogących skutkować usunięciem danych przetwarzanych niezgodnie z prawem. Związek art., 26 RODO z zasadą zgodności z prawem jest daleki i pośredni, ale jednak jest.	
Art. 28 RODO – „Podmiot przetwarzający” – podpisanie umowy powierzenia przetwarzania legalizuje przetwarzanie w imieniu ADO.	
Art. 30 ust. 1 lit b RODO – „Rejestrowanie czynności przetwarzania” – o ile w pozycji „cele przetwarzania” ADO wpisuje również podstawę prawną przetwarzania. Jest to dopuszczalne, ponieważ realizację podstawy prawnej można uznać za cel przetwarzania.	
Art. 33 RODO – „Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorcemu” – sprzyja realizacji zasady ponieważ ocena naruszenia może	

doprowadzić do zmian w przetwarzania, skutkujących podniesieniem poziomu zgodności z prawem w zakresie przetwarzania danych osobowych. Również kontrola, mogąca być efektem zgłoszenia sprzyja realizacji zasady”.	
Art. 34 RODO – „Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych” - może skutkować podjęciem przez tę osobę decyzji o skorzystaniu z uprawnień, które mogą skutkować zmniejszeniem zakresu przetwarzania.	
Art. 35 ust. 7 lit. b RODO - „Ocena skutków dla ochrony danych” – ocena, „czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów” może skłonić ADO do kontroli czy dane są przetwarzane w sposób zgodny z prawem.	
Art. 36 ust. 3 lit. b RODO – „Uprzednie konsultacje” – mogą doprowadzić do stanu zgodnego z prawem, w zakresie przetwarzania.	

Zasada rzetelności
1. Dane osobowe muszą być: a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”)
Rozporządzenie RODO
Art. 5 ust. 1 lit. a)
Obowiązek
Art. 5 ust. 1 lit. a RODO nakłada na administratora obowiązek przetwarzania danych osobowych w sposób rzetelny, czyli tak by osoba, której dane dotyczą wiedziała że dany administrator je przetwarza.
Uprawnienie
Art. 5 ust. 1 lit. a RODO ustanawia uprawnienie, które przysługuje każdej osobie której dane dotyczą, polegające na tym, że osoba której dane dotyczą ma prawo wiedzieć, że dotyczące jej dane osobowe są przetwarzane przez danego administratora.
Dokumentacja wewnętrzna potwierdzająca realizację zasady a w tym przepisów ja konkretyzujących

Przetwarzanie danych osobowych w sposób rzetelny to przetwarzanie w taki sposób, że osoba, której dane dotyczą wie, że dotyczące jej dane są przetwarzane przez danego administratora.

Przetwarzanie danych osobowych w sposób rzetelny to przetwarzanie w taki sposób, że osoba, której dane dotyczą wie, że dotyczące jej dane są przetwarzane przez danego administratora.

I poziom

Zasada rzetelności konkretyzowana jest przez wymienione poniżej przepisy:	Sposób realizacji przepisu konkretyzującego zasadę:
Art. 6 ust. 1 RODO lub art. 9 ust. 1 RODO (w zw. z art. 7 RODO w zw. z art. 4 pkt 11 RODO) – osoba, która wyraża zgodę na przetwarzanie dotyczących jej danych osobowych, tym samym zdaje sobie sprawę z faktu, że jej dane przetwarzane będą.	
Art. 12 ust. 1 RODO – „Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą” – Ado informuje o fakcie przetwarzania.	
Art. 13 ust. 2 lit a RODO – Informacja podawana w przypadku zbierania danych od osoby, której dane dotyczą - informacja o okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu.	
Art. 14 ust. 2 lit a RODO – informacja podawana w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą – informacja o okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu.	
Art. 15 ust. 1 lit d RODO – informacja podawana jeżeli Osoba, której dane dotyczą korzysta z przysługującego jej prawa dostępu do informacji – informacja o (w miarę możliwości) planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu.	
Art. 17 RODO – Prawo do usunięcia danych („prawo do bycia zapomnianym”)	
Art. 18 RODO – Prawo do ograniczenia przetwarzania jeżeli ograniczenie przetwarzania danych osobowych w przyszłości oznacza żądanie usunięcia danych w przyszłości.	
Art. 19 RODO – Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania jeżeli ADO informuje odbiorcę o usunięciu danych lub o ograniczeniu przetwarzania jeżeli takowe w przyszłości oznacza żądanie usunięcia danych w przyszłości.	

II poziom

Zasada rzetelności konkretyzowana jest przez wymienione poniżej przepisy:	Sposób realizacji przepisu konkretyzującego zasadę:
Art. 7 RODO w zw. z art. 4 pkt 11 RODO – jeżeli w zgodzie skonkretyzowano czas, na jaki zgody udzielono (ew. w zw. z art. 8 RODO - Warunki wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego	
Art. 7 RODO w zw. z art. 4 pkt 11 RODO w zw. z art. 8 RODO – jeżeli w zgodzie skonkretyzowano czas, na jaki zgody udzielono i chodzi o zgodę wyrażoną przez dziecko w przypadku usług społeczeństwa informacyjnego	
Art. 20 RODO – Prawo do przenoszenia danych. Pozwala osobie, której dane dotyczą na dokładne zapoznanie się z danymi, jakie przetwarza ADO, a tym samym na skorzystanie z uprawnień, które mogą skutkować usunięciem danych.	
Art. 21 RODO – Prawo do sprzeciwu. Może skutkować usunięciem danych	
Artykuł 23 – Ograniczenia. „Prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw.” „W szczególności akt prawny (...) musi zawierać szczegółowe przepisy przynajmniej – w stosownym przypadku – o: (...) okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania	
Art. 25 ust. 1 RODO – „Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych”, o ile projektowanie systemu ma przyczynić się do ograniczenia przechowywania danych.	
Art. 30 ust. 1 lit. f RODO – „Rejestrowanie czynności przetwarzania”. RCPD ma zawierać „jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych”.	
Art. 34 RODO – „Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych” może skutkować podjęciem przez tę osobę decyzji o skorzystaniu z uprawnień, które mogą skutkować usunięciem danych.	
Art. 35 RODO, zwłaszcza art. 35 ust. 7 RODO – „Ocena skutków dla ochrony danych” opis operacji przetwarzania i ocena ich niezbędności, mogą skłonić ADO do usunięcia.	

Zasada przejrzystości
1. Dane osobowe muszą być: a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”)
Rozporządzenie RODO
Art. 5 ust. 1 lit. a)
Obowiązek
Art. 5 ust. 1 lit. a RODO nakłada na administratora obowiązek przetwarzania danych osobowych w sposób rzetelny, czyli tak by osoba, której dane dotyczą wiedziała że dany administrator je przetwarza.
Uprawnienie
Art. 5 ust. 1 lit. a RODO ustanawia uprawnienie, które przysługuje każdej osobie której dane dotyczą, polegające na tym, że osoba której dane dotyczą ma prawo wiedzieć, że dotyczące jej dane osobowe są przetwarzane przez danego administratora.
Dokumentacja wewnętrzna potwierdzająca realizację zasady a w tym przepisów ja konkretyzujących

Zasada przejrzystości oznacza obowiązek przetwarzania danych osobowych w taki sposób, że osoba, której dane dotyczą zna szczegóły przetwarzania dotyczących jej danych, wymienione odpowiednio w art. 13 RODO, art. 14 RODO, art. 15 RODO.

I poziom

Zasada przejrzystości konkretyzowana jest przez wymienione poniżej przepisy:	Sposób realizacji przepisu konkretyzującego zasadę:
Art. 12 ust. 1 RODO – „Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą” – ADO informuje o fakcie przetwarzania. W ten sposób osoby, których dane dotyczą poznają szczegóły przetwarzania danych.	
Art. 13 ust. 1 i 2 RODO – „Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą” – jest to istota zasady przejrzystości.	
Art. 14 ust. 1 i 2 RODO – „Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą” – drugi z przepisów, których celem jest konkretyzacja zasady przejrzystości.	
Art. 15 ust. RODO – „Prawo dostępu przysługujące osobie, której dane dotyczą” - informacja podawana jeżeli osoba, której dane dotyczą korzysta z przysługującego jej prawa dostępu do informacji, dowiaduje się wtedy o szczegółach przetwarzania danych	

II poziom

Zasada przejrzystości konkretyzowana jest przez wymienione poniżej przepisy:	Sposób realizacji przepisu konkretyzującego zasadę:
Art. 19 RODO – Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania – sprzyja realizacji zasady przejrzystości.	
Art. 34 RODO – „Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych” - sprzyja realizacji zasady przejrzystości.	

Zasada ograniczenia celu
1. Dane osobowe muszą być: (...) b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu”)
Rozporządzenie RODO
Art. 5 ust. 1 lit. b)
Obowiązek
Art. 6 ust. 1 lit. b RODO nakłada na administratora obowiązek przetwarzania danych osobowych w zgodzie z zasadą ograniczenia celu czyli tak by dane osobowe były przetwarzane przez administratora zgodnie z celami określonymi w rejestrze czynności przetwarzania danych osobowych i o których, na podstawie (odpowiednio) art. 13 RODO lub art. 14 RODO lub art. 15 RODO poinformowano osobę, której dane dotyczą.
Uprawnienie
Art. 6 ust. 1 lit. b RODO ustanawia uprawnienie, które przysługuje każdej osobie której dane dotyczą, polegające na tym, że osoba której dane dotyczą ma prawo oczekiwać, iżby administrator przetwarzał dotyczące jej dane wyłącznie w celach określonych w rejestrze czynności przetwarzania danych osobowych i o których poinformował tę osobę, na podstawie (odpowiednio) art. 13 RODO lub art. 14 RODO lub art. 15 RODO.
Dokumentacja wewnętrzna potwierdzająca realizację zasady a w tym przepisów ją konkretyzujących

Przetwarzanie danych osobowych zgodne z zasadą ograniczenia celu, to przetwarzanie w taki sposób, że administrator przetwarza dane w celach określonych odpowiednio w rejestrze czynności przetwarzania danych osobowych, oraz na gruncie art. 13 RODO lub 14 RODO lub 15 RODO.

Po wygaśnięciu wskazanych wyżej celów, administrator może, nie naruszając zasady ograniczenia celu, przetwarzać dane osobowe przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych.

I poziom

Zasada ograniczenia celu konkretyzowana jest przez wymienione poniżej przepisy:	Sposób realizacji przepisu konkretyzującego zasadę:
Art. 13 ust. 1 lit. c RODO w zw. z art. 12 RODO w zw. z art. 4 pkt 7 RODO – „Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą”. Informowanie osoby, której dane dotyczą o celach przetwarzania danych osobowych umożliwia tej osobie podjęcie kroków, mogących doprowadzić do przetwarzania w mniejszym zakresie.	
Art. 13 ust. 3 RODO – „Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2.” – informowanie osoby, której dane dotyczą o zmienionym celu przetwarzania danych osobowych umożliwia tej osobie podjęcie kroków, mogących doprowadzić do przetwarzania w mniejszym zakresie.	
Art. 14 ust. 1 lit. c RODO w zw. z art. 14 ust. 5 lit. b RODO w zw. z art. 12 RODO w zw. z art. 4 pkt 7 RODO – „Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą” – informowanie osoby, której dane dotyczą o celach przetwarzania danych osobowych umożliwia tej osobie podjęcie kroków, mogących doprowadzić do przetwarzania w mniejszym zakresie.	
Art. 14 ust. 4 RODO – „Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2. ” – informowanie osoby, której dane dotyczą o zmienionym celu przetwarzania danych osobowych umożliwia tej osobie podjęcie kroków, mogących doprowadzić do przetwarzania w mniejszym zakresie.	
Art. 6 ust. 3 RODO, art. 6 ust. 4 RODO, Art. 6 ust. 1 RODO – litera odpowiednia do podstawy prawnej – przetwarzanie w oparciu o odpowiednią podstawę wynikającą z art. 6 RODO, oznacza przetwarzanie w celu realizacji konkretnego celu, z taką przesłanką	

związanego.	
Art. 9 ust. 1 RODO w zw. z art. 9 ust. 2 RODO – litera odpowiednia do podstawy prawnej – przetwarzanie w oparciu o odpowiednią podstawę wynikającą z art. 6 RODO, oznacza przetwarzanie w celu realizacji konkretnego celu, z taką przesłanką związanego.	
Art. 30 ust. 1 lit. b RODO (RCPD) – „Rejestrowanie czynności przetwarzania” – umieszczenie w RCPD pozycji „cele przetwarzania” jest jednym z kluczowych momentów realizacji zasady. Cel przetwarzania danych to cel, o którym ADO informuję w oparciu o art. 12 RODO i który to cel ma wskazany w RCPD (oczywiście o ile ma RCPD).	
Art. 30 ust. 1 lit. d RODO (RCPD - odbiorcy), „Rejestrowanie czynności przetwarzania” – umieszczenie w RCPD pozycji „odbiorcy” przyczynia się do realizacji zasady. Odbiorca to ktoś kto otrzymuje dane od ADO, ale przetwarza je w oparciu o własną podstawę prawną, we własnym celu, cel ten jest, do pewnego stopnia możliwy do skontrolowania przez pierwotnego ADO – ADO może po prostu danych nie udostępnić odbiorcy, o ile prawo mu na to pozwala.	

II poziom

Zasada ograniczenia celu konkretyzowana jest przez wymienione poniżej przepisy:	Sposób realizacji przepisu konkretyzującego zasadę:
Art. 11 ust. 1 RODO – „Przetwarzanie niewymagające identyfikacji” – przetwarzanie w celu niewymagającym identyfikacji, przetwarzanie bez identyfikacji, sprzyja realizacji zasady.	
Art. 15 ust. 1 lit. a RODO – „Prawo dostępu przysługujące osobie, której dane dotyczą” – informowanie osoby, której dane dotyczą o celach przetwarzania, sprzyja realizacji zasady.	
Art. 16 RODO – „Prawo do sprostowania danych” – realizacja prawa do sprostowania danych może mieć dobry wpływ na realizację zasady u ADO.	
Art. 16 RODO w zw. z art. 19 RODO – „Prawo do sprostowania danych” w zw. z „Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania” – realizacja prawa do sprostowania danych i obowiązku powiadomienia o sprostowaniu danych może mieć dobry wpływ na realizację zasady u odbiorców.	
Art. 17 ust. 1 odpowiednio (lit a RODO lub lit. d RODO) – „Prawo do usunięcia danych („prawo do bycia zapomnianym”)”- może mieć dobry wpływ na realizację zasady u ADO dzięki usunięciu danych, co do których cel przetwarzania już ustał.	
Art. 17 ust. 1 odpowiednio (lit a RODO lub lit. d RODO) w zw. z art. 19 RODO – „Prawo do usunięcia danych („prawo do bycia zapomnianym”)” w zw. z „Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania” – realizacja prawa do sprostowania danych i obowiązku powiadomienia o sprostowaniu danych może mieć dobry wpływ na realizację zasady u odbiorców dzięki usunięciu u odbiorców, danych, co do których cel przetwarzania już ustał.	
Art. 18 ust. 1 lit. c RODO – „Prawo do ograniczenia przetwarzania” gdy „administrator nie potrzebuje już danych osobowych do celów przetwarzania (...)”,- może wpłynąć zrazu na ograniczenie przetwarzania danych, potem na usunięcie i przyczynić się w ten sposób do realizacji zasady u ADO.	
Art. 18 ust. 1 lit. c RODO w zw. z art. 19 RODO, - „Prawo do ograniczenia przetwarzania” gdy	

„administrator nie potrzebuje już danych osobowych do celów przetwarzania (...),- może wpłynąć zrazu na ograniczenie przetwarzania danych, potem na usunięcie i przyczynić się w ten sposób do realizacji zasady u ADO i „Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania” po poinformowaniu odbiorcy może przyczynić się do usunięcia danych i wpłynąć pozytywnie na poszanowanie zasady u odbiorcy.	
Art. 21 ust. 3 RODO – „Prawo do sprzeciwu” – „Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów” – co sprzyja realizacji zasady.	
Art. 21 ust. 6 RODO – „Prawo do sprzeciwu”, „Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.”	
Art. 23 ust. 1 lit e RODO w zw. z art. 23 ust. 2 lit a RODO w zw. z art. 23 ust. 2 lit f RODO (w zw. z ewentualnymi przepisami krajowymi) – ograniczenia wprowadzone przepisami krajowymi Mogą sprzyjać realizacji zasady.	
Art. 24 ust. 1 RODO w zw. z art. 25 ust. 1 RODO w zw. z RCPD „Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne (...)” – uwzględnienie celów przetwarzania podczas wdrażania zabezpieczeń, sprzyja realizacji zasady.	
Art. 25 ust. 2 RODO – „Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych” – „Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. (...)”- wdrożenie	

środków technicznych i organizacyjnych dla osiągnięcia celu przetwarzania sprzyja realizacji zasady.	
Art. 26 ust. 1 RODO (jeżeli zachodzi współadministrowanie) – „Współadministratorzy”, „Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami.” – określanie celów przetwarzania przez więcej niż jednego ADO może mieć wpływ na realizację zasady.	
Art. 27 ust. 2 lit. a RODO (Przedstawiciele administratorów lub podmiotów przetwarzających niemających jednostki organizacyjnej w Unii) – „Przedstawiciele administratorów lub podmiotów przetwarzających niemających jednostki organizacyjnej w Unii”, „1. Jeżeli zastosowanie ma art. 3 ust. 2, administrator lub podmiot przetwarzający na piśmie wyznacza swojego przedstawiciela w Unii. Obowiązek ustanowiony w ust. 1 niniejszego artykułu nie ma zastosowania w przypadku: (...)i jest mało prawdopodobne, by ze względu na swój charakter, kontekst, zakres i cele powodowało ryzyko naruszenia praw lub wolności osób fizycznych”. – niewyznaczenie przedstawiciela jeżeli nie jest ono konieczne z uwagi na cel przetwarzania ma, daleki bo daleki, ale jednak, związek z realizacją zasady.	
Art. 28 ust. 3 (w przypadku powierzenia przetwarzania) - zawarcie umowy powierzenia przetwarzania może sprzyjać realizacji zasady	
Art. 35 ust. 1 RODO w zw. z art. 35 ust. 7 RODO – „Ocena skutków dla ochrony danych” – podczas dokonywania oceny skutków dla ochrony danych, brane pod uwagę są również cele przetwarzania danych, co może sprzyjać realizacji zasady.	
Art. 36 ust. 3 RODO - „Uprzednie konsultacje” – „cele i sposoby zamierzonego przetwarzania” są jednym z elementów, o których informowany jest organ nadzoru podczas uprzednich konsultacji, co może poważnie sprzyjać realizacji zasady.	
Art. 37 ust. 1 lit b RODO w zw. z art. 39 ust. 2 RODO (IOD) – „Wyznaczenie inspektora ochrony danych” uzależnione jest m.in. od tego czy cele przetwarzania danych „wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę”, zaś IOD „wypełnia swoje zadania z należyty uwzględnieniem ryzyka	

związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i <u>cele</u> przetwarzania”.	
Art. 47 ust. 2 lit b RODO w zw. z art. 47 ust. 2 lit. d RODO („Wiążące reguły korporacyjne”) – „W wiążących regułach korporacyjnych, o których mowa w ust. 1, określone zostają co najmniej: (...) rodzaj przetwarzania i jego cele (...)”, co może sprzyjać realizacji zasady u ADO, którzy się do danych reguł stosują.	
Art. 83 ust. 2 lit. a RODO – „Ogólne warunki nakładania administracyjnych kar pieniężnych” – „ (...) Decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należyta uwagę na: (...) charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania (...)”. Branie pod uwagę celu przetwarzania danych przy nakładaniu kar administracyjnych może skutkować wzrostem poszanowania zasady, choć z uwagi na swoistą prewencję ogólną.	
Art. 85 ust. 2 RODO – „Przetwarzanie a wolność wypowiedzi i informacji”(Dla przetwarzania do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej), „Dla przetwarzania do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej państwa członkowskie określają odstępstwa lub wyjątki od rozdziału (...), jeżeli są one niezbędne, by pogodzić prawo do ochrony danych osobowych z wolnością wypowiedzi i informacji.” – ograniczenie uprawnień, osób, których dane dotyczą, w sensie materialnym narusza zasadę, jednak w sensie formalnym, ponieważ jest dopuszczone w przepisie RODO – zasady nie narusza.	
Art. 88 ust. 1 RODO – „Przetwarzanie w kontekście zatrudnienia” „Państwa członkowskie mogą zawrzeć w swoich przepisach lub w porozumieniach zbiorowych bardziej szczegółowe przepisy mające zapewnić ochronę praw i wolności w przypadku przetwarzania danych osobowych pracowników w związku z zatrudnieniem, w szczególności do celów rekrutacji, wykonania umowy o pracę, (...)” – wprowadzenie wskazanych przepisów powinno sprzyjać realizacji zasady.	

Art. 89 RODO - „Zabezpieczenia i wyjątki Mające zastosowanie do przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych” – „Przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych podlega odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą, zgodnie z niniejszym rozporządzeniem. (...)” – przetwarzanie w celach wskazanych w przepisie, nie wyłącza ochrony praw osób, których dane dotyczą, a tym samym sprzyja realizacji zasady.	
--	--

Zasada minimalizacji danych
1. Dane osobowe muszą być: (...) c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”)
Rozporządzenie RODO
Art. 5 ust. 1 lit. c)
Obowiązek
Art. 5 ust. 1 lit. c RODO nakłada na administratora obowiązek przetwarzania danych osobowych w sposób adekwatny, stosowny i ograniczony do tego co jest niezbędne do celów przetwarzania. Inaczej, art. 5 ust. 1 lit. c RODO nakłada na administratora obowiązek przetwarzania danych osobowych wyłącznie w niezbędnym zakresie.
Uprawnienie
Art. 5 ust. 1 lit. c RODO ustanawia uprawnienie, które przysługuje każdej osobie której dane dotyczą, polegające na tym, że administrator przetwarza dotyczące jej dane w sposób adekwatny, stosowny i ograniczony do tego co jest niezbędne do celów przetwarzania Inaczej art. 5 ust. 1 lit. c RODO ustanawia uprawnienie, które przysługuje każdej osobie której dane dotyczą, polegające na tym, że administrator przetwarza dotyczące jej dane wyłącznie w niezbędnym zakresie.
Dokumentacja wewnętrzna potwierdzająca realizację zasady a w tym przepisów ja konkretyzujących

Zasada minimalizacji danych oznacza obowiązek przetwarzania danych osobowych w sposób adekwatny, stosowny oraz ograniczony do tego, co niezbędne do celów, w których są przetwarzane.

Zasada minimalizacji danych oznacza tym samym obowiązek przetwarzania danych osobowych w taki sposób, że administrator przetwarza jedynie te dane, których przetwarzanie jest konieczne, z uwagi na realizowane przez administratora cele.

Przetwarzanie danych osobowych zgodnie z zasadą minimalizacji danych czyli przetwarzanie danych osobowych w sposób adekwatny, stosowny oraz ograniczony do tego, co niezbędne do celów, w których są przetwarzane to przetwarzanie w taki sposób, że administrator przetwarza jedynie te dane, których przetwarzanie jest konieczne, z uwagi na realizowane przez administratora cele.

I poziom

Zasada minimalizacji danych konkretyzowana jest przez wymienione poniżej przepisy:	Sposób realizacji przepisu konkretyzującego zasadę:
Art. 13 RODO – informowanie osoby, której dane dotyczą o szczegółach przetwarzania danych a zwłaszcza informowanie o celu przetwarzania, podstawie prawnej przetwarzania i o odbiorcach danych uświadamia osobie, której dane dotyczą, po co dane są przetwarzane, co może skłonić tę osobę do skorzystania z uprawnień, które mogą skutkować zmniejszeniem zakresu przetwarzania danych lub co najmniej kontrolą tego zakresu.	
art. 14 RODO - informowanie osoby, której dane dotyczą o szczegółach przetwarzania danych, czyli informowanie o celu przetwarzania, podstawie prawnej przetwarzania i o odbiorcach danych a zwłaszcza o kategoriach przetwarzanych danych, uświadamia osobie, której dane dotyczą, po co dane są przetwarzane a zwłaszcza jakie dane są przetwarzane, co może skłonić tę osobę do skorzystania z uprawnień, które mogą skutkować zmniejszeniem zakresu przetwarzania danych lub co najmniej kontrolą tego zakresu.	
art. 15 RODO – informowanie o zakresie przetwarzanych danych uświadamia osobie której dane dotyczą, ten zakres i pozwala na jego kontrolę.	
Art. 17 RODO – usuwanie danych wskutek realizacji prawa do bycia zapomnianym.	
Art. 18 RODO – jeżeli ograniczenie przetwarzania danych osobowych w przyszłości oznacza żądanie usunięcia danych w przyszłości.	
Art. 19 RODO – jeżeli ADO informuje odbiorcę o usunięciu danych, lub o ograniczeniu przetwarzania, które ma na celu usunięcie danych.	
Art. 20 RODO – prawo do przenoszenia danych pozwala osobie, której dane dotyczą na dokładne zapoznanie się z danymi, jakie przetwarza ADO, a tym samym na skorzystanie z uprawnień, które mogą skutkować zmniejszeniem zakresu przetwarzania.	
Art. 21 RODO – prawo do sprzeciwu wobec przetwarzania danych osobowych.	

II poziom

Zasada minimalizacji danych konkretyzowana jest przez wymienione poniżej przepisy:	Sposób realizacji przepisu konkretyzującego zasadę:
Art. 30 ust. 1 lit. c RODO – sporządzanie RCPD, pozwala ADO na kontrolę tego jakie dane przetwarza, przy jakich czynnościach i tym samym pozwala na zmniejszenie zakresu przetwarzania danych.	
Art. 34 RODO - Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych może skutkować podjęciem przez tę osobę decyzji o skorzystaniu z uprawnień, które mogą skutkować zmniejszeniem zakresu przetwarzania.	
Art. 35 RODO, zwłaszcza art. 35 ust. 7 RODO – opis operacji przetwarzania i ocena ich niezbędności, mogą skłonić ADO do zmniejszenia zakresu przetwarzania.	

Zasada prawidłowości danych
1. Dane osobowe muszą być: (...) d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”)
Rozporządzenie RODO
Art. 5 ust. 1 lit. d)
Obowiązek
Art. 5 ust. 1 lit. d RODO nakłada na administratora obowiązek przetwarzania danych osobowych w taki sposób by były one prawidłowe i w razie potrzeby uaktualniane. Inaczej art. 5 ust. 1 lit. d RODO nakłada na administratora obowiązek by dane osobowe były prawidłowe i aktualne. Jednocześnie art. 5 ust. 1 lit. d RODO nakłada na administratora obowiązek podjęcia wszelkich rozsądnych działań aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.
Uprawnienie
Art. 5 ust. 1 lit. d RODO ustanawia uprawnienie, które przysługuje każdej osobie której dane dotyczą, polegające na tym, że administrator przetwarza dotyczące jej dane w sposób że są one prawidłowe i w razie potrzeby uaktualniane. Inaczej art. 5 ust. 1 lit. d RODO ustanawia uprawnienie, które przysługuje każdej osobie której dane dotyczą, polegające na tym, że administrator dba o to by przetwarzał dotyczące jej dane wyłącznie prawidłowe i aktualne. Jednocześnie art. 5 ust. 1 lit. d RODO ustanawia uprawnienie, które przysługuje każdej osobie której dane dotyczą, polegające na tym, że administrator podejmuje wszelkie rozsądne działania aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.
Dokumentacja wewnętrzna potwierdzająca realizację zasady a w tym przepisów ją konkretyzujących

Zasada prawidłowości oznacza obowiązek przetwarzania danych osobowych w taki sposób by były one prawidłowe i w razie potrzeby uaktualniane. Zasada prawidłowości danych oznacza również obowiązek podjęcia wszelkich rozsądnych działań aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

I poziom

Zasada prawidłowości danych konkretyzowana jest przez wymienione poniżej przepisy:	Sposób realizacji przepisu konkretyzującego zasadę:
Art. 16 RODO – żądanie sprostowania danych osobowych przez osobę, której dane dotyczą.	
Art. 19 RODO – jeżeli ADO informuje odbiorcę o poprawieniu lub zaktualizowaniu danych.	
Art. 25 ust. 1 RODO – o ile projektowanie systemu ma przyczynić się do prawidłowości danych.	

II poziom

Zasada prawidłowości danych konkretyzowana jest przez wymienione poniżej przepisy:	Sposób realizacji przepisu konkretyzującego zasadę:
Art. 18 RODO – jeżeli ograniczenie przetwarzania danych osobowych w przyszłości oznacza żądanie sprostowania lub zaktualizowania danych w przyszłości.	
Art. 13 RODO – informacje na temat szczegółów przetwarzania danych osobowych, podawane osobie, której dane dotyczą mogą skutkować skorzystaniem przez tę osobę z jej uprawnień, co z kolei Może skutkować poprawieniem lub usunięciem danych osobowych.	
art. 14 RODO - informacje na temat szczegółów przetwarzania danych osobowych, podawane osobie, której dane dotyczą mogą skutkować skorzystaniem przez tę osobę z jej uprawnień, co z kolei Może skutkować poprawieniem lub usunięciem danych osobowych.	
art. 15 RODO – informowanie o zakresie przetwarzanych danych uświadamia osobie której dane dotyczą, ten zakres i pozwala na jego kontrolę, pod kątem prawidłowości i aktualności danych.	
Art. 20 RODO – prawo do przenoszenia danych pozwala osobie, której dane dotyczą na dokładne zapoznanie się z danymi, jakie przetwarza ADO, a tym samym na skorzystanie z uprawnień, które mogą skutkować poprawieniem lub zaktualizowaniem danych.	
Art. 30 ust. 1 lit. c RODO – sporządzanie RCPD, pozwala ADO na kontrolę tego jakie dane przetwarza, przy jakich czynnościach i tym samym pozwala na zmniejszenie zakresu przetwarzania danych.	
Art. 34 RODO - Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych może skutkować podjęciem przez tę osobę decyzji o skorzystaniu z uprawnień, które mogą skutkować poprawieniem lub zaktualizowaniem danych.	
Art. 35 RODO, zwłaszcza art. 35 ust. 7 RODO – opis operacji przetwarzania i ocena ich niezbędności, mogą skłonić ADO do zaktualizowania lub poprawienia danych.	

Zasada ograniczenia przechowywania
Art. 5.1. Dane osobowe muszą być: (...) e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”)
Rozporządzenie RODO
Art. 5 ust. 1 lit. e)
Obowiązek
Art. 5 ust. 1 lit. e RODO nakłada na administratora obowiązek przetwarzania danych osobowych przez ograniczony czas.
Uprawnienie
art. 5 ust. 1 lit. d RODO ustanawia uprawnienie, które przysługuje każdej osobie której dane dotyczą, polegające na tym, że administrator przetwarza dotyczące jej dane przez ograniczony czas.
Dokumentacja wewnętrzna potwierdzająca realizację zasady a w tym przepisów ja konkretyzujących

Zasada ograniczenia przechowywania oznacza obowiązek przetwarzania danych osobowych przez ograniczony czas.

Jeśli chodzi o dane medyczne, to należy zwracać głównie uwagę na terminy z art. 29 ustawy o prawach pacjenta i Rzeczniku praw pacjenta, tudzież prowadzić rejestr, lub rejestry udostępnianej dokumentacji medycznej.

Zasada integralności
1. Dane osobowe muszą być: (...) f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”)
Rozporządzenie RODO
Art. 5 ust. 1 lit. f)
Obowiązek
Art. 5 ust. 1 lit. f RODO nakłada na administratora obowiązek dbałości o to by modyfikacja danych osobowych, w tym zniszczenie lub uszkodzenie, zachodziły jedynie w sposób autoryzowany przez administratora.
Uprawnienie
Art. 5 ust. 1 lit. f RODO ustanawia uprawnienie, które przysługuje każdej osobie której dane dotyczą, polegające na tym, że może ona oczekiwać, że modyfikacja danych osobowych, w tym zniszczenie lub uszkodzenie danych, zachodzą jedynie w sposób autoryzowany przez administratora.
Dokumentacja wewnętrzna potwierdzająca realizację zasady a w tym przepisów ja konkretyzujących

Zasada integralności oznacza obowiązek przetwarzania danych osobowych w taki sposób by modyfikacja danych, w tym zniszczenie lub uszkodzenie, zachodziły jedynie w sposób autoryzowany przez administratora.

I poziom

Zasada integralności konkretyzowana jest przez wymienione poniżej przepisy:	Sposób realizacji przepisu konkretyzującego zasadę:
Art. 6 RODO – <i>Zgodność przetwarzania z prawem</i> stanowi ramy dla przetwarzania, które nie jest niezgodne z prawem.	
Art. 9 RODO – <i>Przetwarzanie szczególnych kategorii danych osobowych</i> stanowi ramy dla przetwarzania, które nie jest niezgodne z prawem.	
Art. 10 RODO – <i>Przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa</i> stanowi ramy dla przetwarzania, które nie jest niezgodne z prawem.	
Art. 29 RODO – <i>Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego</i> – istota autoryzowanego dostępu.	
Art. 32 RODO, zwłaszcza art. 32 ust. 4 RODO – <i>Bezpieczeństwo przetwarzania</i> , a w art. 32 ust. 4 RODO mowa jest o konieczności autoryzowanych działań.	
Art. 24 ust. 1 RODO – wdrożenie odpowiednich środków technicznych i organizacyjnych powinno zapewniać autoryzowane przetwarzanie a co za tym idzie, poszanowanie zasady integralności.	
Art. 32 ust. 1 lit. b ¹⁵¹ – <i>zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania</i> – jako jeden z elementów technicznego zabezpieczenia danych, którego opis powinien znaleźć się w OOTiOŚB.	
Art. 28 RODO – <i>Podmiot przetwarzający</i> – przetwarzanie przez ten podmiot jest istotne w kontekście poszanowania zasady integralności, podmiot przetwarzający zwykle przetwarza dane osobowe w sposób autoryzowany, ale gdy jest jednoosobowy, gdy podmiot przetwarzający ma strukturę, a zwykle ma, to skutkuje to pojawieniem się zagrożeń.	

¹⁵¹ P. Litwiński, P. Barta, M. Kawecki. w P. Litwiński (red.) P. Barta, M. Kawecki. *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz.* Warszawa 2018. s. 267. Uszczegółowienia Zasady Integralności, nazywanej przez nich „zasadą integralności i poufności danych”, wskazani autorzy dopatrują się w art. 32 RODO.

II poziom

Zasada integralności konkretyzowana jest przez wymienione poniżej przepisy:	Sposób realizacji przepisu konkretyzującego zasadę:
Art. 4 ust. 12 RODO - <i>naruszenie ochrony danych osobowych</i> jest zwykle bliskie naruszeniu integralności tych danych.	
Art. 11 RODO – <i>Przetwarzanie niewymagające identyfikacji</i> – jeżeli takie przetwarzanie jest dopuszczalne, to należy je stosować, co chroni w pewnym stopniu przed złamaniem zasady integralności.	
Art. 16 RODO – <i>Prawo do sprostowania danych</i> sprzyja integralności danych, można bowiem utożsamić dane nieprawidłowe z nieintegralnymi. Utożsamienie to jest pewnym uproszczeniem, ale można założyć, że jeżeli ktoś wprowadził dane nieprawidłowe, to są one w jakimś sensie nieintegralne, acz jak piszę wyżej, jest to pewne uproszczenie.	
Art. 17 RODO – <i>Prawo do usunięcia danych</i> („prawo do bycia zapomnianym”) sprzyja integralności danych, usuwanie zainicjowane na gruncie tego przepisu jest zapewne usuwaniem, które nie narusza zasady integralności.	
Art. 18 RODO – <i>Prawo do ograniczenia przetwarzania</i> – może sprzyjać integralności.	
Art. 25 ust. 1 RODO – <i>Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych</i> , o ile projektowanie systemu ma przyczynić się do integralności danych przez zapobieganie przed nieautoryzowanym dostępem.	
Art. 30 RODO – <i>Rejestrowanie czynności przetwarzania</i> – samo sporządzanie a potem posługiwanie się rejestrem czynności przetwarzania danych osobowych powinno sprzyjać kontroli czynności, oczywiście o ile administrator uzupełnia rejestr czynności przetwarzania danych osobowych o pozycję: „czynność”.	
Art. 35 RODO, zwłaszcza art. 35 ust. 7 RODO – <i>Ocena skutków dla ochrony danych</i> ” opis operacji przetwarzania i ocena ich niezbędności, mogą skłonić administratora do kontroli czy dane są przetwarzane w sposób autoryzowany.	

Zasada poufności
1. Dane osobowe muszą być: (...) f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”)
Rozporządzenie RODO
Art. 5 ust. 1 lit. f)
Obowiązek
Art. 5 ust. 1 lit. f RODO nakłada na administratora obowiązek ujawnienia danych jedynie uprawnionym podmiotom.
Uprawnienie
Jednocześnie art. 5 ust. 1 lit. f RODO ustanawia uprawnienie, które przysługuje każdej osobie której dane dotyczą, polegające na tym, że może ona oczekiwać, że administrator będzie ujawniał dane jedynie uprawnionym podmiotom.
Dokumentacja wewnętrzna potwierdzająca realizację zasady a w tym przepisów ja konkretyzujących

Zasada poufności oznacza obowiązek przetwarzania danych osobowych w taki sposób by były one ujawniane jedynie uprawnionym podmiotom lub osobom.

I poziom

Zasada poufności konkretyzowana jest przez wymienione poniżej przepisy:	Sposób realizacji przepisu konkretyzującego zasadę:
Art. 6 RODO – „Zgodność przetwarzania z prawem” stanowi ramy dla przetwarzania, które nie jest niezgodne z prawem – udostępnienie musi mieścić się w przesłankach przetwarzania, jest to widoczne zwłaszcza na przykładzie udostępniania danych odbiorcom.	
Art. 9 RODO - „Przetwarzanie szczególnych kategorii danych osobowych” stanowi ramy dla przetwarzania, które nie jest niezgodne z prawem – udostępnienie musi Mieścić się w przesłankach przetwarzania, jest to widoczne zwłaszcza na przykładzie udostępniania danych odbiorcom.	
Art. 10 RODO - „Przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa” stanowi ramy dla przetwarzania, które nie jest niezgodne z prawem.	
Art. 29 RODO - „Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego” – istota autoryzowanego dostępu wewnątrz struktury ADO	
Art. 32 RODO, zwłaszcza art. 32 ust. 1 lit b RODO – „Bezpieczeństwo przetwarzania”- mowa jest tam m.in. o zdolności do ciągłego zapewnienia poufności.	
Art. 24 ust. 1 RODO – wdrożenie odpowiednich środków technicznych i organizacyjnych powinno zapewniać autoryzowane przetwarzanie a co za tym idzie, poszanowanie zasady poufności.	
Art. 28 RODO – „Podmiot przetwarzający” – przetwarzanie przez ten podmiot jest istotne w kontekście poszanowania zasady poufności, PP zwykle przetwarza w sposób zgodny z tą zasadą, jednak gdy PP ma strukturę, a zwykle ma, to skutkuje to pojawieniem się zagrożeń, sam PP nie narusza poufności, ale może ujawnić dane dalej w ten sposób, że to ujawnienie doprowadzi do naruszenia poufności.	

II poziom

Zasada poufności konkretyzowana jest przez wymienione poniżej przepisy:	Sposób realizacji przepisu konkretyzującego zasadę:
Art. 4 ust. 12 RODO - „naruszenie ochrony danych osobowych” jest zwykle bliskie naruszeniu poufności tych danych.	
Art. 11 RODO - „Przetwarzanie niewymagające identyfikacji” – jeżeli takie przetwarzanie jest dopuszczalne, to należy je stosować, co chroni w pewnym stopniu przed złamaniem zasady poufności. Jeżeli wyciekają dane, których nie można nikomu przypisać, to poufność nie jest zagrożona.	
Art. 17 RODO – „Prawo do usunięcia danych („prawo do bycia zapomnianym”)” sprzyja poufności danych. Usunięcie danych uniemożliwia naruszenie poufności. Jak danych nie ma to nie można ich już nikomu ujawnić. Wydaje się to truizmem, ale często dla ADO najwygodniej jest nie dane chronić, ale ich nie mieć.	
Art. 18 RODO – „Prawo do ograniczenia przetwarzania” – może sprzyjać poufności, jeżeli osoba, której dane dotyczą zażąda działań sprzyjających poufności.	
Art. 25 ust. 1 RODO – „Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych”, o ile projektowanie systemu ma przyczynić się do poufności danych przez zapobieganie przed nieautoryzowanym dostępem.	
Art. 30 RODO – „Rejestrowanie czynności przetwarzania” – samo sporządzanie a potem posługiwanie się RCPD powinno sprzyjać kontroli czynności, oczywiście o ile ADO uzupełnia RCPD o pozycję: „czynność”. Jeśli ADO wie co z danymi czyni, to może je lepiej chronić.	
Art. 35 RODO, zwłaszcza art. 35 ust. 7 RODO – „Ocena skutków dla ochrony danych” opis operacji przetwarzania i ocena ich niezbędności, mogą skłonić ADO do kontroli czy dane są przetwarzane w sposób zabezpieczający poufność.	

