KONSULTACJE KODEKSU POSTĘPOWANIA DLA JEDNOSTEK OŚWIATOWYCH

MAJĄCY NA CELU DOPRECYZOWANIE STOSOWANIA ROZPORZĄDZENIA 2016/679 W WERSJA IV (IV. 2020)

Autor: Mariusz Stasiak vel Stasek https://msvs.com.pl/

Recenzja i poprawki: Robert Stańczyk http://odoonline.pl/

Korekta i uwagi uzupełniające: Dominik Spałek https://prostetorodo.pl/

Konsultacje mają na celu przedstawić opinie oraz propozycje modyfikacji lub uzupełnień treści zapisów projektu postępowania dla jednostek oświatowych. Konsultowane oraz opiniowane nie są natomiast zagadnienia, z którymi autor zgadza się w pełni lub prezentuje to samo stanowisko.

1. Wprowadzenie

1.2 Zakres podmiotowy Kodeksu

W pkt 1.2 w zakresie podmiotowym kodeksu wyszczególnia się placówki oświatowe określone ogólnie w art. 1 i 2 PO. Rozpisane są 1 i 2 a) i b).

Kodeks postepowania nie określa swoim zakresem całości placówek określonych w art. 2 pkt 1 -11 mimo, że jego nazwa mogłaby to sugerować KODEKS POSTĘPOWANIA DLA JEDNOSTEK OŚWIATOWYCH MAJĄCY NA CELU DOPRECYZOWANIE STOSOWANIA ROZPORZĄDZENIA 2016/679 Podstawa opracowania: art. 40 rozporządzenia 2016/679.

Ogólnie to jest kodeks dla szkół i przedszkoli i to też nie wszystkich (brak regulacji dla placówek, gdzie organem prowadzącym nie jest JST). Należy odpowiednio zatytułować kodeks.

Zaleca się wprowadzenie zapisów wskazujących jednoznacznie na podmiotowy zakres stosowania regulacji kodeksowych.

1.3 Zakres przedmiotowy Kodeksu

1.3.3 minimalnego zakresu regulacji zawartych w polityce bezpieczeństwa informacji,

W art. 24 ust. 2 wskazana jest polityka ochrony danych, pojęcie polityki bezpieczeństwa informacji wynika z poprzednio obowiązujących przepisów, warto by kodeks wskazywał nomenklaturę nie wskazującą na zastosowanie poprzednich przepisów.

Propozycja zapisu: 1.3.3 minimalnego zakresu regulacji zawartych w Politykach Ochrony Danych

1.3.9 metodologii przeprowadzania analizy ryzyka

Ze słownika PWN:

- *Metodologia*:
  nauka o metodach badań naukowych stosowanych w danej dziedzinie wiedzy;
- *Metodyka*:
  - zbiór zasad dotyczących sposobów wykonywania jakiejś pracy,
  - dział pedagogiki omawiający cele i sposoby nauczania jakiegoś przedmiotu;
- Metoda:
  świadomie stosowany sposób postępowania mający prowadzić do osiągnięcia zamierzonego celu

Propozycja zapisu: 1.3.9 proponowana metodyka przeprowadzenia analizy ryzyka,

Propozycja zapisu: 1.3.10 proponowana metodyka kwalifikacji oraz przeprowadzania oceny skutków dla ochrony danych,

Propozycja zapisu: 1.3.12 proponowana metoda monitorowania wdrożonych zabezpieczeń.

2.1. Przepisy oświatowe dotyczące przebiegu kształcenia i wychowania dzieci i młodzieży.

Podstawowym celem implikującym przetwarzanie danych osobnych w jednostkach oświatowych jest kształcenie i wychowanie dzieci i młodzieży. Opiera się on na dwóch głównych aktach prawnych: 1.5.1. Ustawa z dnia 7 września 1991 r. o systemie oświaty (tj. Dz.U.2019.0.1481) 1.5.2. Ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe (tj. Dz.U.2019.0.1148) 1.5.3. Ustawa z dnia 14 grudnia 2016 r. przepisy wprowadzające ustawę – Prawo oświatowe (Dz.U. 2017.0.60) 1.5.4. Ustawa z dnia 27 października 2017 r. – o finansowaniu zadań oświatowych (tj. Dz.U.2020.0.17) 1.5.5. Ustawa z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej (tj. Dz.U.2019.0.1942)

Wskazuje się dwa akty prawne a wymienia pięć.

3.2 Umowa

Umowa, lub czynności zmierzające do jej zawarcia, jako postawa prawna przetwarzania danych osobowych zostały przewidziane w art. 6 ust. 1 lit. b RODO.

Zgodnie z definicją art. 6 ust. 1 lit. b) 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;

Warto, aby definicja była przytoczona kompletnie, gdyż nie wszystkie czynności zmierzające do zawarcia umowy legalizują przetwarzanie danych osobowych, a jedynie działań na żądanie osoby, której dane dotyczą.

Przesłanka ta nie legalizuje wysyłania niechcianych informacji handlowych, a jedynie legalizuje przetwarzanie danych potencjalnych wykonawców, którzy ubiegają się o zamówienie.

Propozycja zapisu: Wykonanie umowy, lub niezbędne działania na żądanie osoby, której dane dotyczą, przed zawarciem umowy, jako postawa prawna przetwarzania danych osobowych zostały przewidziane w art. 6 ust. 1 lit. b RODO.

3. Podstawy przetwarzania danych osobowych

W artykule 6 RODO ustawodawca unijny przewidział 6 przesłanek pozwalających (lepiej brzmi legalizujących) na przetwarzanie danych osobowych. Podstawowe działania w zakresie realizacji zadań statutowych publicznych jednostek oświatowych określają trzy przesłanki:

3.1

3.2.

3.3

Brakuje litery e). Sugeruje dodanie pkt 3.4.

Główny błąd jaki zauważam w tym rozdziale to brak wskazania przesłanek legalizujących przetwarzanie danych wrażliwych z art. 9 RODO oraz podania przykładów. Skoro rozdział mówi o podstawach przetwarzania to powinny być wszystkie. Są też dane karne z art. 10.

3.3. Przetwarzanie niezbędne do realizacji obowiązków prawnych ciążących na administratorze.

3.3.6. udzielanie zamówień publicznych;

Wszystkie zakupy finansowane z środków publicznych są zamówieniami publicznymi, powołując się na podstawę prawną jako obowiązek prawny warto było by wskazać, że dotyczy ono Zamówień publicznych realizowanych w reżimie ustawy Prawo Zamówień Publicznych, gdyż zamówienia poniżej kwoty 30 tyś euro są realizowane zgodnie z KC, a zgodnie z nim przetwarzanie danych nie jest niezbędne, gdyż nie nakłada reżimu konkursowych, a jedynie do uregulowania pozostają kwestie zawarcia umowy oraz rozliczeń podatkowych, jednak to już inna czynność przetwarzania.

Propozycja zapisu: 3.3.6. udzielanie zamówień publicznych w trybie określonym w ustawie Prawo Zamówień Publicznych;

3.3.8. zawieranie umów cywilnoprawnych;

Przetwarzanie danych w celu zawarcia umowy cywilno-prawnej legalizuje przesłanka z art. 6 ust. 1 lit. b), przepisy prawa nie nakładają obowiązku przetwarzania danych osobowych w związku z zawarciem umowy, natomiast ich przetwarzanie jest niezbędne do jej zawarcia oraz jej realizacji.

Również w art. 13 ust. 2 lit. e) Prawodawca wskazuje na wyraźne rozróżnienie tych czynności, kiedy obowiązek przetwarzania danych nakłada przepis prawa, a kiedy jest on warunkiem umowy lub warunkiem jej zawarcia.

Art. 13 ust. 1 lit e) „informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy…".

Propozycja usunięcie pozycji

3.3.9. zapewnienie bezpieczeństwa za pomocą narzędzia, jakim jest monitoring wizyjny

Stanowisko, że zastosowanie monitoringu wizyjnego jako narzędzie zapewniające bezpieczeństwo w szkole jest obowiązkiem Szkoły, stoi w sprzeczności z poglądami wyrażanymi przez Urząd Ochrony Danych Osobowych MONITORING WIZYJNY W SZKOLE ASPEKTY PRAWNE I TECHNICZNE IX edycja Ogólnopolskiego Programu Edukacyjnego „Twoje dane – Twoja sprawa" 11 stycznia 2019, OEIiZK

„Art. 6 ust. 1 lit. e RODO – wykonanie zadania realizowanego w interesie publicznym przez administratora Art. 108a ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz. U. z 2018 r. poz. 996 z późn. zm.) w zw. Z art. 68 ust. 1 pkt 6 - doprecyzowanie zasad realizacji zadania dyrektora szkoły (placówki) – zapewnianie bezpiecznych warunków zajęć i pracy".

Również EROD w swoich wytycznych Guidelines 3/2019 on processing of personal data through video devices Version 2.0 Adopted on 29 January 2020 wskazuje identyczne stanowisko dotyczące podstawy prawnej przetwarzania danych osobowych za pomocą monitoringu wizyjnego.

16. In principle, every legal ground under Article 6 (1) can provide a legal basis for processing video surveillance data. For example, Article 6 (1) (c) applies where national **law stipulates an obligation to carry out video surveillance**.

7 However in practice, the provisions most likely to be used are

• Article 6 (1) (f) (legitimate interest),

• Article 6 (1) (e) (necessity to perform a task carried out in the public interest or in the exercise of official authority).

In rather exceptional cases Article 6 (1) (a) (consent) might be used as a legal basis by the controller

Przykłady obowiązku stosowania monitoringu wizyjnego, gdzie przesłanka legalizującą jest art. 6 ust. 1 lit. c jest np. stadion piłkarski, gdzie przepisy Ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych w art. 8 nakładają na administratora taki obowiązek.

Szkoła ma obowiązek zapewnienia bezpieczeństwa uczniom, a zastosowanie monitoringu wizyjnego nie jest jej obowiązkiem, a jedynie jednym ze sposobów jego zapewnienia, przepis art. 108a daje ustawowe zezwolenie na realizację monitoringu, gdyż jego zastosowanie jest w interesie publicznym.

Propozycja modyfikacji stanowiska: Monitoring wizyjny jako uprawnienie administratora realizowane w interesie publicznym w związku z art. 6 ust. 1 lit. e) na podstawie art. 108a ustawy Prawo Oświatowe.

4. Realizacja praw podmiotów danych

RODO, w rozdziale III, nakłada na administratora danych obowiązek realizacji praw osób, których dane dotyczą. Do praw tych należą:

a. prawo do informacji, realizowane przy pozyskiwaniu danych;
b. prawo dostępu do danych osobowych i otrzymania ich kopii;
c. prawo do poprawiania i uzupełniania danych osobowych;
d. prawo do usunięcia danych;
e. prawo do ograniczenia przetwarzania;
f. prawo do przenoszenia danych;
g. prawo do sprzeciwu wobec przetwarzania
h. prawo do niepodlegania zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

RODO w rozdziale III nakłada na administratora jeszcze jeden bardzo ważny obowiązek, o którym wielu administratorów zapomina, więc tym bardziej kodeks winien mocno go podkreślić:

Artykuł 12. Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą.

Prawo to wskazuje na bardzo ważny obowiązek, a mianowicie to Administrator ma dołożyć wszelkich starań, aby przekazywać informacje osobie, której dane dotyczą w sposób zrozumiały i łatwo dostępnej formie. Ponadto cała komunikacja z podmiotem danych ma być prowadzona właśnie w ten sposób.

Należy w kodeksie mocno zaakcentować, że nie da się zrealizować praw opisanych w art. 13-22 bez prawidłowej realizacji prawa z art. 12.

Zwięzłej, przejrzysta, zrozumiała i łatwo dostępna forma, jasnym i prostym językiem to nie tylko klauzula informacyjna, która nie jest pisana językiem prawniczym, szczególnie, gdy mówimy o placówkach oświatowych, ale to również powiadomienie o naruszeniu, czy udzielanie informacji na żądanie z art. 15. Ponadto art. 12 ust. 1 informuje nas, o konieczności prowadzenia komunikacji z podmiotem danych na piśmie w tym elektronicznie, a na żądanie podmiotu danych ustnie (to również telefonicznie), jeżeli potwierdzi się tożsamość tej osoby.

Artykuł 12 wskazuje również w ust. 2 na konieczność ułatwienia realizacji praw osobie, której dane dotyczą i nie odmawia podjęcia działań w ich realizacji. Ważną informacją jest również wskazanie przez Prawodawcę Unijnego terminów udzielania informacji osobie, której dane dotyczą opisanych w art. 12 ust. 3 oraz 4.

Propozycja zmiany: Opisanie jako pkt 4.1 Prawo do przejrzystego informowania i przejrzystej komunikacji

4.1. Prawo do informacji art. 13 i 14 RODO

4.1.1. Prawo do informacji przy pozyskiwaniu danych osobowych bezpośrednio od podmiotu danych.

6. Celem przetwarzania danych osobowych w postaci wizerunku w systemie monitoringu wizyjnego jest zapewnienie bezpiecznych warunków pracy oraz nauki uczniom i pracownikom oraz ochrona mienia placówki.

Podstawa prawna:

Ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe

Jak już wyżej wskazywałem prezentuje stanowisko zbieżne z Prezesem UODO oraz wytycznymi Europejskiej Rady Ochrony Danych, które jasno przedstawia, iż art. 6 ust. 1 lit. c dla monitoringu wizyjnego jest podstawą, gdy przepis prawa nakazuje administratorowi stosować to szczególne rozwiązanie w celu zapewnienia bezpieczeństwa, a nie gdy daje mu takie uprawnienie.

Ponadto w prezentowanym przykładzie cel został wskazany jako: Celem przetwarzania danych osobowych w postaci wizerunku w systemie monitoringu wizyjnego jest zapewnienie bezpiecznych warunków pracy oraz nauki uczniom i pracownikom oraz ochrona mienia placówki.

Natomiast jako podstawę prawną wskazano Ustawę z dnia 14 grudnia 2016 r. – Prawo oświatowe.

W związku z tym chciałbym zwrócić autorom uwagę na to, iż ustawodawca wskazał jasno cel przetwarzania w jakim można stosować monitoring wizyjny, więc nie widzę konieczności ubierania tego celu w inne słowa niż wprost wskazane w ustawie, gdyż celem przetwarzania wizerunku w systemie monitoringu wizyjnego jest zapewnienie bezpieczeństwa uczniom i pracownikom lub/oraz ochrona mienia.

Ponadto placówkę oświatową jako pracodawcę obowiązują również przepisy Kodeksu Pracy w zakresie stosowania monitoringu wizyjnego, stąd niezbędnym jest wskazanie obu przesłanek legalizujących tj. art. 22[2] Kodeksu Pracy

Propozycja zmiany: zmiana proponowanej nazwy celu przewarzania na ten określony w ustawie oraz wskazanie jako podstawy prawnej również Kodeks Pracy

7. Celem przetwarzania danych osobowych zawartych w umowie na /przedmiot umowy/ jest wypełnienie jej zobowiązań.

Podstawa prawna:

Ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe

W tej pozycji nie wiem co autorzy mieli na myśli, gdyż wskazany cel jest bardzo ogólny oraz wprost wpisuje się w definicję art. 6 ust. 1 lit. b)

Propozycja zmiany: wykreślenie przykładu

Odbiorcy danych (art. 13 ust. 1 lit. e)

Informacje o odbiorcach danych osobowych lub kategoriach odbiorców

Autorzy kodeksu słusznie wskazali katalog przykładowych odbiorców danych jednak nie sprecyzowali jak ustalać tych odbiorców, a tu z definicji art. 4 pkt. 9) „odbiorca" 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;

Warto więc wskazać, że odbiorcami danych osobowych będą podmiotu uprawnione na podstawie przepisów prawa np. w związku z obowiązkami pracowniczymi będzie to Bank, Zakład Ubezpieczeń Społecznych czy Urząd Skarbowy, odbiorcami jednak nie będą podmioty uprawnione w związku z prowadzonym postępowaniem np. organy ścigania, sądy, komornicy, którzy prowadzą postępowanie zgodnie z Kodeksem Postępowania Administracyjnego/Cywilnego/Karnego etc.

Propozycja zmian: Wskazanie 2 głównych grup odbiorców tj. Pomiotów przetwarzających oraz podmiotów uprawnionych na podstawie przepisów wraz ze wskazaniem przykładów każdego z nich.

Prawa podmiotu danych

Przysługuje Pani / Panu:

1. prawo dostępu do przetwarzanych danych osobowych i otrzymania ich kopii;

2. prawo do sprostowania i uzupełnienia swoich danych osobowych;

3. prawo do usunięcia danych osobowych przetwarzanych na podstawie zgody, po jej wycofaniu;

4. prawo do ograniczenia przetwarzania danych osobowych;

Autorzy wskazali tylko i wyłącznie możliwość skorzystania z prawa do usunięcia swoich danych osobowych po wycofaniu zgody co nie znajduje poparcia w art. 17 RODO

Prawo do usunięcia danych przysługuje na warunkach określonych w art. 17 i nie zasadnym jest w klauzuli informacyjnym ograniczanie go do tylko jednej sytuacji. Jeżeli administrator przetwarza dane niezgodnie z prawem tj. bez podstawy prawnej lub zbiera je nadmiarowo osobie, której dane dotyczą przysługuje prawo żądania usunięcia danych lub jeżeli umowa została rozliczona, a terminy przedawnienia roszczeń wygasły, lecz administrator danych nie usunął to osobie, której dane dotyczą ma prawo żądać usunięcia tych danych.

Ponadto należy zwrócić uwagę, iż nie podanie prawa do przenoszenia danych w sytuacji, gdy dane przetwarzane są na podstawie art. 6 ust. 1 lit. a lub b jest mocno kontrowersyjną, należy językowo rozważać co art. 13 ust. 2 lit b) wymaga od administratora:

b) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

Należy podzielić ten wymóg na części:

Informacje o prawie do żądania od administratora:

- dostępu do danych osobowych dotyczących osoby, której dane dotyczą,

- ich sprostowania,

- usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania,

- a także o prawie do przenoszenia danych.

Warto więc zwrócić uwagę, iż Administrator zgodnie z art. 13 ust. 2 lit. b) musi podać osobie, której dane dotyczą 4 informacje o tym, że ma prawo do:

- dostępu do danych osobowych zgodnie z art. 15

- usunięcia (art. 17) lub ograniczenia (art. 18) lub wniesienia sprzeciwu (art. 21)

- prawo do przenoszenia zgodnie z art. 20, gdy przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub lit. b) lub art. 9 ust. 2 lit. a)

Tak więc należy przysługujące prawa dostosować do przede wszystkim określonej podstawy prawnej i odpowiednio wskazać, które prawa przysługują.

Określenie w kodeksie, że przysługują tylko wskazane prawa może spotkać się z sytuacją, że jednostki stosujące kodeks będą wskazywać tylko te przedstawione. Dlatego tak jest istotne, aby kodeks wskazywał kiedy jakie prawa przysługują.

Proponowana zmiana: Wskazanie, że przysługują wszystkie prawa jednak z określeniem w jakiej sytuacji i przy jakiej podstawie prawnej.

Informacja czy podanie danych osobowych jest wymogiem ustawowym, umownym czy warunkiem zawarcia umowy.

Wskazanie ewentualnych konsekwencji niepodania danych. Art. 13 ust. 2 lit. e
Przetwarzanie na podstawie art. 6 ust. 1 lit. a RODO

Podanie danych jest obowiązkiem umownym. Niepodanie danych będzie skutkowało: (do wyboru)

a. brakiem możliwości publikacji zdjęć i informacji promujących osiągnięcia ucznia;

b. brakiem możliwości publikacji wizerunku pracownika na stronie internetowej szkoły;

c. brakiem możliwości przechowywania dokumentów aplikacyjnych celem wykorzystania w przyszłych rekrutacjach pracowników;

d. brakiem możliwości wykorzystania danych innych niże te wymienione w art. 221 § 1 i 3 Kodeksu pracy podczas procesu rekrutacji na wolne stanowisko urzędnicze / pedagogiczne.

e. brakiem możliwości wykorzystania danych osobowych pracownika innych niże te wymienione w art. 221 § 1 i 3 Kodeksu pracy do … /wpisać cel lub rodzaj czynności przetwarzania/

Przetwarzanie na podstawie udzielonej zgody, a wskazanie, że Podanie danych jest warunkiem umownym jest zapewne błędem redakcyjnym.

Proponowana zmiana: Podanie danych jest dobrowolne. Niepodanie danych będzie skutkowało:

Przetwarzanie na podstawie art. 6 ust. 1 lit. c RODO

Podanie danych osobowych jest obowiązkiem ustawowym.

Brak wskazanych konsekwencji niepodania danych, a podstawową konsekwencją będzie brak możliwości przyjęcia dziecka/ucznia, uczestnictwa w konkursach, wydarzeniach, wycieczkach itd. Lub w stosunku do pracownika brak możliwości zatrudnienia, udziału w rekrutacji, dofinansowania z ZFŚS.

Proponowana zmiana: Podanie danych jest obowiązkiem ustawowym. Niepodanie danych będzie skutkowało: (wskazać jak w przypadku umowy kilka przykładów)

4.1.1. Klauzule informacyjne umieszczane są :

- na stronie internetowej

- w biuletynie informacji publicznej

- w sekretariacie szkoły

- na tablicy ogłoszeń

- przy tzw. „księdze wejść i wyjść" – jeśli taka jest prowadzona w jednostce

- a także na drukach i formularzach, na których są zbierane po raz pierwszy dane osobowe

Częstą i w mojej ocenie trafną praktyką jest zamieszczanie również obowiązków informacyjnych w różnego rodzaju regulaminach np. regulaminach konkursów czy rekrutacji, a na druku, który stanowi załącznik do regulaminu umieszczanie tylko informacji w którym pkt. regulaminu są te informacje.

Proponowane rozszerzenie: - w regulaminach konkursów, rekrutacji, wydarzeń. Warto wspomnieć o informacji warstwowej (definicji i sposobach). Poza wymienionymi w stopce wiadomości email, umowach, decyzjach, ogłoszeniach, ofertach i in. Katalog sposobów jest nieograniczony.

Zasadą powinno być, iż obowiązek informacyjny realizowany z wykorzystaniem tzw. klauzul informacyjnych powinien być wykonany podczas pozyskiwania danych, co oznacza, iż każdy z kanałów jakimi pozyskiwane są dane powinien zostać odpowiednio oznaczony. Nie jest wystarczające aby dla danych pozyskiwanych via email klauzula informacyjna umieszczona została na tablicy ogłoszeń w placówce.

4.1.2. Prawo do informacji przy pozyskiwaniu danych osobowych w sposób inny niż od osoby, której dane dotyczą.

W tabelce w części art. 14 ust. 1 lit. c) autorzy wskazują na konieczność wskazania jedynie celu przetwarzania, pominięta została całkowicie podstawa prawna przetwarzania.

Proponowana zmiana: dopisanie podstawy prawnej art. 6 ust. 1 lit. f) prawny interes administratora jakim jest konieczność prawidłowego wywiązania się z warunków umowy.

Informacje te należy przekazać najpóźniej w ciągu miesiąca od momentu otrzymania danych lub, jeśli dane osobowe mają być stosowane do komunikacji z osobą, której dotyczą, informacje wynikające z art. 14 RODO, należy podać przy pierwszej takiej komunikacji.

W kodeksie należało by wskazać stosującym w jaki sposób interpretować termin miesiąca, gdyż może zostać to opacznie zrozumiane jakoby termin to był miesiąca lub pierwszego kontaktu do wyboru, co nie jest właściwą interpretacją.

W art. 14 ust. 3. Czytamy „Informacje, o których mowa w ust. 1 i 2, administrator podaje:

a) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;

b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; **lub**

c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

W art. 14 ust. 3 jasno jest wskazane, iż administrator który dane pozyskał z innego źródła ma dwa kryteria terminu podania informacji z art. 14 ust. 1 i 2, w związku z tym musi zastosować się do tego, który upłynie jako pierwszy:

W ciągu miesiąca, chyba że wcześniej skontaktuje się z tą osobą lub ujawni dane innemu odbiorcy wtedy przed pierwszą z tych czynności musi wypełnić obowiązek informacyjny.

Należy wskazać, że w przywołanym fragmencie autorzy nie ujęli w nim art. 14 ust. 3 lit. c jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu, co wymaga korekty.

Propozycja zmiany zapisu: Informacje te należy przekazać najpóźniej w ciągu miesiąca od momentu otrzymania danych, chyba że wcześniej skontaktuje się z tą osobą lub ujawni dane innemu odbiorcy wtedy przed pierwszą z tych czynności musi wypełnić obowiązek informacyjny.

4.2. Prawo dostępu do danych – art. 15 RODO

W jednostkach oświatowych udzielenie dostępu do danych możliwe jest wyłącznie w przypadku danych przetwarzanych w dzienniku elektronicznym. Technologia ta pozwala zarówno osobom sprawującym władzę rodzicielską, dzieciom, jak i pełnoletnim uczniom na dostęp do swoich danych osobowych. W innym przypadku udzielenie dostępu do danych jest niemożliwe, gdyż w dokumentach szkolnych znajdują się najczęściej dane osobowe osób innych niż ta, która zwróciła się do administratora z żądaniem dostępu.

Autorzy dość jednoznacznie i kategorycznie wskazują, iż umożliwienie dostępu do danych jest możliwe tylko i wyłącznie w przypadku korzystanie z dziennika elektronicznego, nie jestem w stanie się z tą sytuacją zgodzić, gdyż procesów w placówce oświatowej jest zdecydowanie więcej niż tylko prowadzenie dokumentacji nauczania. Nawet w sytuacji dokumentowania przebiegu nauczania mamy sytuacje z prawem dostępu do danych i uzyskaniem ich kopii, to jest regulowane chociaż by Art. 44e. ust. 4 ustawy o systemie oświaty, który nakazuje na udostępnienie sprawdzonej pracy uczniowi i jego rodzicom. Ponadto w ust. 5 jest mowa o udostępnieniu egzaminów na wniosek, są to przepisy szczegółowo regulujące uprawnienia, które są tożsame z uprawnieniami z art. 15. O tym, że odpowiedzi na egzaminie to są informacje o charakterze danych osobowych wypowiedział się również Trybunał Sprawiedliwości UE 20 grudnia 2017 roku w sprawie Peter Nowak przeciwko Data Protection Commissioner (Irlandia) o numerze C-434/16.

Warto zauważyć również, że inne procesy też mają swoje prawo dostępu do danych i tu chociażby warto zwrócić uwagę na proces naboru do szkoły/przedszkola, gdzie dostęp do dokumentów rekrutacyjnych czy uzyskanie kopi danych w nich zawartych nie wpływa niekorzystnie na prawa i wolności innych. Podobnie będzie w sytuacji dostępu do dokumentacji kadrowej, która też jest ściśle regulowana przepisami prawa pracy. Dostęp do danych jest możliwy także w innych przypadkach w związku zatrudnieniem, zfśs, umowami, zamówieniami itd.

Propozycja zmiany: W jednostkach oświatowych udzielenie dostępu do danych najczęściej realizowane będzie w przypadku danych przetwarzanych w dzienniku elektronicznym. Technologia ta pozwala zarówno osobom sprawującym władzę rodzicielską, dzieciom, jak i pełnoletnim uczniom na dostęp do swoich danych osobowych. W innych przypadkach należy ustalić czy umożliwienie dostępu do danych nie wpływa na prawa lub wolność innych osób, czyli czy nie udostępnimy danych osób trzecich.

4.2.3. Wydanie kopii danych

Należy sporządzić kopię danych osobowych osoby wnioskującej i przekazać jej w formie uniemożliwiającej wprowadzenie zmian, /na przykład dokumentu pdf./ Wydanie kopii danych może odbywać się drogą elektroniczną, listownie lub wydając kopię do rąk własnych osobie wnioskującej.

W każdym przypadku, należy potwierdzić, ponad wszelką wątpliwość, tożsamość wnioskującego. Nie można przesyłać kopii danych osobowych, jeżeli wniosek spłynął za pośrednictwem poczty elektronicznej, a administrator nie jest w stanie potwierdzić tożsamości wnioskodawcy.

Autorzy słusznie wskazali, iż wydanie kopii może odbywać się na kilka sposobów, jednak nie zostało wskazane pouczenie, które jest zawarte w art. 15 ust. 3 „…Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się w powszechnie stosowanej formie elektronicznej."

Brakuje definicji kopii danych. Czy to określenie odnosi się do wyszczególnienia jakie dane posiadamy czy chodzi np. o ksero dokumentacji czy odpis z dokumentu.

Propozycja zmiany: Wydanie kopii danych może odbywać się drogą elektroniczną, listownie lub wydając kopię do rąk własnych osobie wnioskującej. Jeżeli wniosek wpłyną drogą elektroniczną i nie została wskazana forma udzielenia informacji, informacji udziela się w powszechnie stosowanej formie elektronicznej. Ponadto zaleca się określenie definicji kopii danych.

4.3. Prawo do sprostowania danych – art. 16 RODO

Zgodnie z art. 16 RODO osoba, której dane dotyczą ma prawo żądania od administratora wprowadzenia korekty jej danych (bądź danych jej dziecka), oraz ich uzupełnienia, jeżeli uzna, że są one niekompletne. Aktualne i poprawne dane osobowe są podstawą właściwej realizacji zadań administratora. Wnioski podmiotów danych o sprostowanie i aktualizację danych osobowych powinny być realizowane najszybciej jak to możliwe. W przypadku jednostek oświatowych opis sposobu korygowania lub uzupełniania danych należy ująć w polityce bezpieczeństwa, bądź w osobnej procedurze. Ważnym jest, aby osoby odpowiedzialne za korektę danych w poszczególnych dokumentach i systemach znały przyjęty sposób postępowania. O wprowadzeniu korekty danych osobowych należy poinformować osobę, której dane dotyczą.

Polityka bezpieczeństwa - Nieodpowiedni termin, brak definicji polityki bezpieczeństwa i polityki bezpieczeństwa informacji w kodeksie, w RODO wskazane w art. 24 ust. 2 są polityki ochrony.

4.5. Prawo do ograniczenia przetwarzania – art. 18 RODO.

4.5.3. Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub ochrony roszczeń.

Zastosowanie takiej procedury może mieć miejsce w przypadku przetwarzania danych w związku z realizacją umów cywilno-prawnych. Jeżeli okres archiwizacji nie obejmuje czasu, w którym możliwe jest dochodzenie roszczeń przez strony z tytułu zawartej umowy, należy przedłużyć okres archiwizacji dokumentów.

Umowy cywilnoprawne nie są właściwym przykładem realizacji prawa do ograniczenia przetwarzania, gdyż wskazany przykład porusza zabezpieczenie roszczeń co jest interesem administratora, a prawo do ograniczenia przetwarzania jest prawem podmiotu danych, a obowiązkiem administratora.

Bardzo częsty przypadek zastosowania prawa do ograniczenia przetwarzania to wykorzystanie monitoringu wizyjnego w sytuacji np. bójki w szkole lub uszkodzenia samochodu rodzica lub nauczyciela, gdzie osoba, której dane dotyczą może zażądać od administratora przechowania danych dłużej niż wynika to z jego okresu retencji. Sytuacja będzie najczęściej występować, gdy zachodzić będą przesłanki postępowania cywilnego.

Propozycja zmiany: Inny przykład prawa do ograniczenia ze wskazaniem jako prawa podmiotu danych, jak ten który podałem wyżej.

4.5.4. Osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 rozporządzenia 2016/679 – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

W placówce oświatowej nie zachodzi taka sytuacja.

Ponieważ nie jestem w stanie zgodzić się z podejściem, iż podmiot publiczny w postaci placówki oświatowej nie może korzystać z przesłanki z art. 6 ust. 1 lit. e) również nie mogę się zgodzić, iż prawo to nie przysługuje.

W sytuacji, gdy nagranie monitoringu wizyjnego godzi w godność osobistą ucznia, nauczyciela, rodzica lub osoby odwiedzającą placówkę, podmiot danych ma prawo złożyć sprzeciw wobec przetwarzania. W szczególności, gdy monitoring wizyjny obejmuje pomieszczenia, o których mowa w art. 108a ust. 3 Prawa Oświatowego.

Ponieważ monitoring jest szczególnym uprawnieniem, a nie obowiązkiem szkoły nie widzę logicznej ani prawnej możliwości ograniczenia osobie, której dane dotyczą prawa do wniesienia sprzeciwu, w szczególności, gdy monitoring godzi w dobra osobiste (godność) osoby nagrywanej. Należy pamiętać, że dobra osobiste w postaci godności mogą zostać naruszone poprzez monitoring nie tylko w miejscach opisanych w art. 108a ust. 3 ustawy Prawo Oświatowe, ale również np. na boisku szkolnym podczas zajęć sportowych, na terenie przed lub za szkołą w związku z agresywnym zachowaniem dzieci i młodzieży.

Należy zwrócić uwagę na to, iż myślą przewodnią ustawodawcy, który zezwolił na stosowanie monitoringu wizyjnego jest przede wszystkim bezpieczeństwo uczniów, pracowników i mienia przy czym bezpieczeństwo to nie tylko bezpieczeństwo fizyczne, ale również psychiczne. Nie można więc stosując jedno z rozwiązań, które ma gwarantować zapewnienie bezpieczeństwa naruszać godność zagrażając tym samym bezpieczeństwu psychicznemu ucznia.

Propozycja zmiany: Ograniczenie przetwarzania nagrania z monitoringu wizyjnego wobec, którego osoba wniosła sprzeciw.

4.6. Prawo do przenoszenia danych – art. 20 RODO

Nie ma zastosowania w placówce oświatowej.

Na pierwszy „rzut oka" autorzy mają rację, gdyż szkoła nie przetwarza danych w związku ze świadczeniem usług, a realizuje swoje uprawnienia i obowiązki.

Warto jednak przyjrzeć się art. 20 RODO

a) przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) lub na podstawie umowy w myśl art. 6 ust. 1 lit. b); oraz

b) przetwarzanie odbywa się w sposób zautomatyzowany.

Ponieważ promocja placówki z wykorzystaniem wizerunku odbywa się na podstawie zgody oraz zdjęcia są obrazem cyfrowym naszego wizerunku i są przetwarzane w sposób zautomatyzowany to uważam, iż autorzy kodeksu powinni zając swoje stanowisko na temat przetwarzania wizerunku i realizacji prawa do przenoszenia danych szczególnie do uzyskania tych danych w formacie ustrukturyzowanym co w postaci zdjęcia w formacie np. jpeg może być dość kłopotliwe.

Samo określenie, iż prawo to nie przysługuje jest w mojej ocenie zbyt ogólne i nie pokazuje kierunku rozumowania i uzasadnienia odmowy jego realizacji, co w przypadku sytuacji, gdy podmiot danych wysunie żądanie jego realizacji może być dla Administratora kłopotliwe.

Propozycja zmiany: Uzasadnienie odmowy realizacji prawa z art. 20 z uwzględnieniem motywu 68 preambuły do RODO.

4.7. Prawo do sprzeciwu – art. 21 RODO

Nie ma zastosowania w placówce oświatowej w ramach jej działalności statutowej objętej niniejszym kodeksem.

Tak jak już wyżej wskazałem dla przetwarzania z art. 6 ust. 1 lit. e) prawo to przysługuje.

5.1. Szkolenie wstępne

Każdy pracownik podejmujący pracę, a którego obowiązki związane są przetwarzaniem danych osobowych, przed przystąpieniem do niej, powinien przejść szkolenie z zakresu ochrony danych osobowych.

Ważne jest jednak aby materiał szkoleniowy był przygotowany przez inspektora ochrony danych powołanego w placówce, gdyż oprócz przepisów dotyczących ochrony danych osobowych, zna on również przepisy regulujące działalność jednostki oświatowej.

Powyższy zapis zalecałbym usunąć. Co prawda szkolenia leżą w obowiązkach IOD, to jednak nie jest jedyne źródło, z którego placówka może i powinna korzystać przy realizacji szkoleń. Są podmioty zewnętrzne, specjaliści z zakresu cyberbezpieczeństwa, może być informatyk (w zakresie systemów inf., nieraz powoływany jest też ASI i ma on określone obowiązki wynikające z zarządzenia lub polityki, SZBI) itd.

Każdy pracownik ma obowiązek zapoznać się zasadami i systemem ochrony danych obowiązującym w placówce i winno to wynikać z wewnętrznych regulacji. W tym celu Administrator udostępnia np. materiały przygotowane przez IOD, politykę ochrony danych, organizuje szkolenia dla nowych pracowników itp.

Sposób realizacji wymagania jest do określenia w wewnętrznie.

5.2. Szkolenie okresowe

Szkolenia powinny się odbywać minimum raz na 3 lata.

Ponieważ autorzy kodeksu wskazują okres 3 lat jako czasookres częstotliwości szkoleń, pożądanym przez administratorów danych jest wskazanie uzasadnienia takie czasookresu. Osobiście szkolenia okresowe zalecam raz na 2 lata, jednak ponieważ zawsze jest to uzasadnione dynamikom zmian w przepisach i ich interpretacji, a także poziomu ryzyka związanego z czynnikiem ludzkim, a także ilości naruszeń spowodowanych błędem ludzkim.

Administrator organizuje szkolenia okresowe dla pracowników z uwagi na powyższe. Częstotliwość szkoleń określają regulacje wewnętrzne, umowa z IOD (lub obowiązki IOD w zakresie umowy o pracę), plan pracy IOD, wyniki działań monitorujących IOD, kontrola zarządcza, zalecenia po audytach, po uwzględnieniu zmieniających się przepisów, wydanych decyzji, orzecznictw, wytycznych i obowiązujących praktyk.

Propozycja zmiany: Wskazanie uzasadnienia okres 3 lat dla szkoleń okresowych.

6. Upoważnienia / oświadczenie o zachowaniu poufności

Osoby upoważnione do przetwarzania danych osobowych powinny złożyć oświadczenia o zachowaniu poufności.

W opracowaniu brakuje odniesienia do bardzo istotnego elementu jakim jest wprowadzona zmiana do prawa oświatowego ustawą 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 związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) w art. 22 oraz 148 zostały dodane ustawowe zobowiązania do zachowania w poufności danych osobowych uczniów określonych w art. 9 ust. 1 RODO, co jest niezbędne do powoływania się na zapisy art. 9 ust. 2, gdzie wymagane są przepisy prawa zapewniające mechanizmy ochrony praw i wolność osób, których dane dotyczą.

Warto również omówić sytuację, gdzie ustawodawca zadecydował, kiedy pracownik oświaty jest zwolniony z tego obowiązku.

Propozycja zmiany: Omówienie art. 22 i 148 w zakresie zachowania w poufności danych szczególnej kategorii.

Ponadto Rozporządzenie o dokumentacji pracowniczej nie określa w części B wymogu przechowywania upoważnień w aktach osobowych pracownika. Co prawda w rozdziale 2 art. 3 ust 2 rozporządzenia jest zapis o dokumentach i oświadczeniach dotyczących danych osobowych, jednak dotyczy to kwestionariuszy, formularzy, oświadczeń itd. Upoważnienia i klauzule można trzymać w aktach pracowniczych albo sposób przechowywania określić w polityce ochrony danych wraz ze wskazaniem osoby odpowiedzialnej za kontrolę i ewidencję. Kodeks wymusi zmianę struktury akt pracowniczych w wielu jednostkach oraz zmianę polityk ochrony danych.

Upoważnienia wynikające z przepisu dziedzinowego mają formę pisemną i mogą wynikać z treści lub załącznika do regulaminu, zarządzenia i innych dok. Pracownicy są członkami różnych komisji a zakres przetwarzania nie wynika wtedy z umowy o pracę. W takich sytuacjach regulaminy komisji powinny określać kwestie upoważnień i klauzul.

7. Polityka bezpieczeństwa informacji

Nieodpowiedni termin patrz opinię do 4.3

d. Każdą umowę powierzenia przetwarzania danych osobowych parafuje inspektor ochrony danych, a podpisuje administrator danych osobowych.

Całkowicie nie zrozumiał dla mnie zapis, który w kontekście usprawnienia pracy placówki oświatowej może zrobić więcej krzywdy niż pożytku. W zdecydowanej większości placówek oświatowych funkcja inspektora ochrony danych jest funkcją przydzieloną na część etatu lub zlecona na podstawie umowy o współpracę lub świadczenie usług. W tej sytuacji wskazanie Administratorowi konieczność uzyskania parafki IOD na każdej umowie spowoduje problemy organizacyjne lub wręcz uniemożliwi dostęp do profesjonalnych podmiotów.

Efektem ubocznym może być również niechęć do oficjalnego stosowania kodeksu, gdyż realizacja zapisów tego punktu będzie kontrolowana przez podmioty monitorujące.

W opisywanym procesie decyzyjnym należy dostrzec i nazwać wyraźnie rolę ADO, który to ostatecznie podejmuje decyzję w przedmiocie danego zagadnienia, w tym wypadku zawarcia / nie zawarcia stosownej umowy powierzenia przetwarzania danych. W takim stanie rzeczy, parafowanie projektu umowy przez IOD, może stanowić element oddziaływania na ww., który jako niezależny w swoich działaniach, może mieć inny pogląd na zasadność zawierania umowy w ogóle, bądź na zasadność poszczególnych zapisów kontraktu. Rolą IOD jest poinformowanie ADO o swoich zastrzeżeniach / uwagach, decyzję natomiast podejmuje ostatecznie ADO.

Propozycja zmiany: Usunięcie pkt „d. Każdą umowę powierzenia przetwarzania danych osobowych parafuje inspektor ochrony danych, a podpisuje administrator danych osobowych.” Na rzecz zapisu „d. Każdą umowę powierzenia przetwarzania danych osobowych opiniuje Inspektor Ochrony Danych, a ewentualne zapisu budzące kontrowersje są uzgadniane między IOD, a ADO”.

Ogólne uwagi:

- poszczególne elementy polityki powinny być opisane pod kątem konieczności zastosowania dla spełnienia zasad przetwarzania oraz obowiązków wynikających z przepisów o ochronie danych osobowych,
- proponowane zapisy kodeksu w rozdziale 7.2 rodzą ryzyko, że administrator wykorzysta je jako „gotowiec” tym samym ograniczy się do powyższego zakresu,
- polityka ochrony danych w placówkach wielokrotnie jest elementem wdrażanym na podstawie wieloletnich doświadczeń i ewolucji przepisów. Wiele polityk zostało zaproponowanych i wdrożonych przez kancelarie i inne podmioty świadczące usługi z zakresu ochrony danych osobowych, wskazywanie „szablonu” w kodeksie może spowodować masowe zmiany w placówkach oświatowych na niekorzyść,
- propozycja polityki, pomimo wskazania rozporządzenia KRI jako podstawy prawnej nie określa i nie wyczerpuje wszystkich wymogów wskazanych w paragrafie 20 ust. 2 rozporządzenia KRI. – brakuje opisu wymogów w Kodeksie oraz proponowanych rozwiązań
- polityki mogą być częścią wdrożonego w jednostce Systemu Zarządzania Bezpieczeństwem Informacji.
- w Kodeksie powinny być opisane obowiązki placówki oświatowej w świetle przepisów. Polityki natomiast mają formę dowolną i nie należy wskazywać przykładowego rozwiązania, nawet wskazując, że jest to wersja o minimalnym zakresie,
- „13. Zadania i odpowiedzialności osób, biorących udział w przetwarzaniu danych osobowych. a. Administrator Danych Osobowych (ADO) – **Dyrektor**” – błędnie wskazany Administrator

8. Umowy powierzenia.

Powierzenie przetwarzania danych osobowych podmiotowi, który będzie działał w imieniu **dyrektora** placówki, wymaga zawarcia stosownej umowy. Powinno być Administratora.

9.1.24. Pomoc zdrowotna dla nauczycieli;

Zgodnie z brzmieniem art. 72 Ustawy z dnia 26 stycznia 1982 r. - Karta Nauczyciela „Niezależnie od przysługującego nauczycielowi i członkom jego rodziny prawa do świadczeń z ubezpieczenia zdrowotnego, organy prowadzące szkoły przeznaczą corocznie w budżetach odpowiednie środki finansowe z przeznaczeniem na pomoc zdrowotną dla nauczycieli korzystających z opieki zdrowotnej oraz określą rodzaje świadczeń przyznawanych w ramach tej pomocy oraz warunki i sposób ich przyznawania."

Ustawodawca w sposób bezpośredni wskazał jaki podmiot jest odpowiedzialny za realizację zadania, którym jest organ prowadzący, którego kompetencje w myśl art. 91d pkt. 1) wykonuje rada gminy, rada powiatu, sejmik województwa, a nie dyrektor szkoły.

Brak jest podstawy legalizującej podjęcia uchwały przez radę gminy na delegowanie tego obowiązku na dyrektora szkoły, a powołanie się w rejestrze czynności na art. 6 ust. 1 lit. c oraz art. 9 ust. 2 lit. b) RODO jest nieprawidłowe, gdyż przepis ten odnosi się Administratorów na, których w przepisach krajowych lub unijnych zostały nałożone obowiązki, do których realizacji niezbędne jest przetwarzanie danych. W prawie krajowym ani unijnym nie ma obowiązku zapewnienia przez szkoły funduszu zdrowotnego nauczycieli, a co za tym idzie na Administratorze nie ciąży taki obowiązek.
Propozycja zmiany: Usunięcie czynności lub doprowadzenie jej do stanu faktycznego, a więc działania organizacyjno-techniczne przy realizacji zadania organu prowadzącego.

9.2. Zakres informacji w rejestrze czynności przetwarzania

/rejestr czynności przetwarzania wykazanych w punkcie 10.1. w zakresie zaproponowanym w punkcie 10.2. stanowi załącznik nr 2 do Kodeksu/

Prawdopodobnie w tym miejscu nastąpiło przeoczenie przy korekcie numeracji rozdziałów.

10. Rejestr kategorii czynności przetwarzania
W przypadku gdy placówka oświatowa przetwarza dane osobowe, realizując zadania spoczywające na innym administratorze, staje się podmiotem przetwarzającym. W związku z tym zobowiązana jest do prowadzenia zgodnie z art. 30 ust. 2 rejestru kategorii czynności przetwarzania.

Niestety w przypadku rejestru kategorii czynności przetwarzania autorzy nie pokusili się o wskazanie przykładowych czynności, a co za tym idzie kodeks nie doprecyzowuje tego skomplikowanego dla Administratorów tematu.

W placówkach oświatowych nie ma zbyt wielu sytuacji, gdy placówka oświatowa jest podmiotem przetwarzającym jednak warto by było o kilku przykładach wspomnieć np. gdy placówka oświatowa jest jednocześnie jednostką obsługującą w rozumieniu art. 10b ustawy o samorządzie gminnym lub art. 6b ustawy o samorządzie powiatowym, a także sytuację, gdy jednostki oświatowe prowadzą wspólną działalność socjalną w rozumieniu art. 9 ustawy o zakładowym funduszu świadczeń socjalnych.

Propozycja zmiany: dopisanie przykładowych czynności do rejestru kategorii czynności przetwarzania.

11. Przetwarzanie danych osobowych w systemie monitoringu wizyjnego.

11.1.5. Zapewnienie, aby monitoring nie obejmował pomieszczeń, w których udzielana jest uczniom pomoc psychologiczno-pedagogiczna, pomieszczeń przeznaczonych do odpoczynku i rekreacji pracowników, pomieszczeń sanitarno-higienicznych, gabinetu profilaktyki zdrowotnej, szatni i przebieralni. Ewentualne objęcie ww. pomieszczeń monitoringiem wizyjnym musi być uzasadnione wysokim prawdopodobieństwem naruszenia bezpieczeństwa osób lub mienia, z uwzględnieniem nienaruszalności godności oraz dóbr osobistych osób przebywających w tych pomieszczeniach.

Autorzy kodeksu słusznie zauważają, iż zgodnie z art. 108a ust. 3 monitoring nie powinien obejmować pomieszczeń opisanych powyżej. Autorzy używają bardziej zrozumiałego języka, który uzasadnia zastosowanie monitoringu w tych pomieszczeniach, choć przydatnym zdaje się zrobienie w kodeksie wykazu czynności, które mogły by uzasadniać taki monitoring.

Na dzień dzisiejszy Administratorzy sami muszą podejmować decyzję kiedy istnieje zagrożenia dla zapewnienia bezpieczeństwa uczniom, pracownikom i mienia, a wskazówki otrzymywane na infolinii UODO, w większości sprowadzają się do zaniechania takiego przetwarzania.

Warto więc na zasadzie konsultacji przedstawić propozycje zastosowania monitoringu w pomieszczeniach, o których mowa w art. 108a ust. 3 oraz wskazanie technik uniemożliwiających rozpoznanie osób przebywających w tych pomieszczeniach.

Warto przy tym wziąć pod uwagę zamiast zastosowanie monitoringu zastosowanie dozoru osobistego oraz uzasadnienie czemu nie jest on możliwy lub nieskuteczny.

Przykładem takim może być prowadzenie zajęć lekcyjnych w specjalistycznych salach lub laboratoriach wyposażonych w bardzo drogi i specjalistyczny sprzęt, którego upilnowanie przez dozór osobisty było by niemożliwe lub nieskuteczne.

Propozycja zmiany: Zajęcie stanowiska w zakresie stosowania monitoringu wizyjnego w pomieszczeniach opisanych w art. 108a ust. 3 w zakresie kiedy jest to dozwolone oraz stosowania jakich technik zapewni nienaruszalność godności oraz dóbr osobistych.

12. Podejście oparte na ryzyku – szacowanie ryzyka

W opracowaniu Autorzy wskazują jedną wybraną przez siebie metodykę wykonania analizy ryzyka budzi to dość duże kontrowersję, gdyż RODO nie ogranicza Administratorów w stosowaniu dowolnych metodyk szacowania ryzyka. Podmioty, które zaczną stosować kodeks postępowania będą zobowiązane do stosowania tylko tej jednej metodyki analizy ryzyka co uważam za niewłaściwe.

Kodeks w swoim założeniu ma doprecyzować stosowanie RODO, a więc wskazywać winien, iż Administratorzy są zobowiązani do wyboru metodyki analizy ryzyka oraz jej opisania w polityce bezpieczeństwa. Ponadto kodeks powinien wskazywać na konieczność dokonania oceny szacowania ryzyka, a nie skupiać się na sposobie i algorytmie jej wykonania, szczególnie, że kodeks jest kierowany do bardzo szerokiego kręgu podmiotów i inna metodyka analizy i szacowania ryzyka sprawdzi się w jednoodziałowym przedszkolu, a inny w wielofiliowym zespole szkół.

Uważam, że w kodeksie autorzy powinni wskazać niezbędne etapy przetwarzania opartego na ryzyku, a nie skupiać się na wykładni jej z metodyk, gdyż kodeks to nie materiały szkoleniowe, a dokumentacja jedynego słusznego postępowania podmiotów, które będą go stosować.

Nie rolą autorów kodeksu jest wybór lepszej czy gorszej metodyki, a wskazanie niezbędnych elementów analizy ryzyka.

Podejście, które zaprezentowano w kodeksie w sposób bardzo rażący będzie godziło w bardzo małe i mniej sformalizowane podmioty, które mogą nie być w stanie wykonać wskazanej analizy ryzyka.

Ponadto wszystkie podmioty, które wybrały inną metodykę w celu przystąpienia do stosowania kodeksu będą zobowiązane całkowicie zmienić swoje podejście oparte na ryzyku do tylko jednego sposobu co rodzi problem w kontekście kontroli zarządczej.

W wielu samorządach metodyka analizy ryzyka i ocena ryzyka jest określona zarządzeniem w kontekście stosowania kontroli zarządczej i podmioty takie nie będą mogły przystąpić do stosowania kodeksu, gdyż będą ograniczone innymi aktami prawa lokalnego.

Kodeks powinien zawierać niezbędne elementy analizy ryzyka oraz częstotliwość i zakres jej oceny, a nie sam opis wybranej metodyki.

Propozycja zmiany: Wskazanie elementów niezbędnych w analizie ryzyka oraz odniesienie do praw i wolności zamiast wskazanie jednej wybranej metodyki w sposób szkoleniowy.

12.11. Analiza ryzyka

Analizy ryzyka projektowanej czynności przetwarzania dokonujemy zgodnie z metodologią zaproponowaną w niniejszym Kodeksie.

W Kodeksie postępowań nie proponuje się metodyk, a wprowadza się do użytku daną metodykę przez podmioty, które zaczną stosować kodeks postępowań, co powodować będzie monitorowanie jego przestrzegania przez podmioty o których mowa w art. 41 ust. 1.

Propozycja zmiany: Również jak w poprzednich pkt, rekomenduję zmianę z słowa metodologia na metodyka.

13. Zarządzanie naruszeniami ochrony danych osobowych

Identycznie jak w przypadku analizy ryzyka rekomenduję wskazanie niezbędnych elementów oceny skutków naruszenia, bez wskazywania jedynej metodyki ich przeprowadzenia

13.7. Zawiadomienie osób, których dane osobowe zostały naruszone

Zgodnie z art. 40 ust. 2 Kodeks ma doprecyzowywać zastosowanie niniejszego rozporządzenia, a w przedstawionym punkcie jest w dużej mierze przekopiowana treść rozporządzenia.
Pożądanym w tym punkcie jest wskazanie co rozumieją autorzy kodeksu pod pojęciem rodzaj danych osobowych, charakter naruszenia, jakie dane kontaktowe inspektora ochrony danych, możliwe konsekwencje oraz środki zastosowane przez administratora oraz zaproponowane podmiotowi danych w celu zminimalizowania negatywnych skutków z szczególnym uwzględnieniem motywu 86, 87 i 88 preambuły.

Kodeks powinien wskazywać minimalny zakres informacji jaki powinien się znaleźć w takim zawiadomieniu, jednak jego poziom szczegółowości powinien być większy niż Ogólnego Rozporządzenia, gdyż tylko wtedy ma on możliwość doprecyzowania stosowania RODO.

13.8. Zawiadomienie wymagające niewspółmiernie dużego wysiłku

Jeżeli zawiadomienie osoby / osób, których dane osobowe zostały naruszone, wymagałoby niewspółmiernie dużego wysiłki, ww. informacje należy uzupełnić o określenie kategorii osób, których dane zostały naruszone i umieścić taką informację na stronie internetowej jednostki oświatowej. Jeżeli naruszenie dotyczyło danych osobowych uczniów lub ich rodziców / opiekunów prawnych, a placówka korzysta z dziennika elektronicznego, należy ww. informację rozesłać do osób zainteresowanych, za pomocą modułu: korespondencja / wiadomości, jeśli takowy został przewidziany w oprogramowaniu.

W komentowanym punkcie autorzy skupili się tylko na jednym z 3 powodów zaniechania zawiadomienia osób, których dane dotyczą, nie wskazując jednocześnie co należy rozumieć poprzez niewspółmiernie duży wysiłek w placówce oświatowej. Ponadto w punkcie mówiącym o zaniechaniu zawiadomienia z niewiadomych powodów wskazywana jest propozycja realizacji zawiadomienia poprzez dziennik elektroniczny co przeczy pierwszej części tego punktu.

Propozycja zmiany: Opisanie jak autorzy interpretują niewspółmiernie duży wysiłek w placówce oświatowej oraz opisanie pozostałych przesłanek zaniechania zawiadomienia zgodnie z art. 34 ust. 3 lit. a i b. Ponadto proponuję sposoby realizacji zawiadomienia ująć jako osobny punkt w kodeksie, aby nie wprowadzać stosujących kodeks w błąd.

14. Stałe monitorowanie wdrożonych zabezpieczeń oraz wykazanie prowadzenia przetwarzań zgodnie z założeniami Kodeksu

Zakres przeprowadzanej analizy ryzyka, według metodologii opisanej w pkt 13 niniejszego Kodeksu musi zawierać minimum:

Punkt 13 opisuje metodykę oceny naruszenia, a stałe monitorowanie winno odnosić się do procedur przyjętych nie tylko w sytuacji naruszenia systemu ochrony danych osobowych.

Same zapisy pkt. 14 są właściwe co do minimalnych wymagań przeprowadzonej analizy ryzyka i przedstawiają założenia jakie w mojej ocenie winien spełniać kodeks.

15.3. Realizacja praw osób, których dane dotyczą
15.3.1. Prawo do informacji – art. 13 RODO

Notę informacyjną należy opublikować na stronie internetowej oraz w miarę możliwości przekazać za pomocą narzędzia służącego do zdalnego nauczania.

Opublikowanie informacji z art. 13 RODO na stronie internetowej nie stanowi realizację wymagań RODO w zakresie przejrzystego informowania osób, których dane dotyczą w momencie pozyskiwania danych.

Przy czym należy zwrócić uwagę na to, iż cel przetwarzania w zakresie zdalnej nauki nie został zmieniony zgodnie z brzmieniem art. 13 ust. 3. 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.

Administrator w celu kształcenia dzieci i młodzieży wykorzystuje techniki zdalnego nauczania, w związku z tym nie ma konieczności ponownego wypełniania obowiązku informacyjnego.

Obowiązek informacyjny winien być zrealizowany na etapie pozyskiwania danych, a więc w karcie zgłoszenia dziecka, wskazując przy tym właściwych odbiorców.

Należy w kodeksie jednoznacznie określić definicję podstawy prawnej przetwarzania. Określenie „przesłanka" jest mylna. W obowiązku inf. należy wskazać podstawę prawną przetwarzania i tak trzeba to nazwać a nie „przesłanka". Przepis prawa dziedzinowego nie jest wymagany, a jedynie dla przejrzystości wpisywany w klauzule, co stanowi dobrą praktykę i dookreślenie celu. W praktyce dany cel opiera się często na więcej niż jednej podstawie z przepisów sektorowych.

Przekazywanie informacji do państwa trzeciego (art. 13 ust. 1 lit. f)
Brak jest informacji czy to element konieczny do wskazania czy nie oraz kiedy należy o tym informować osobę, której dane dotyczą.

„gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego…"

16. Załączniki

W mojej ocenie kodeks postępowania nie powinien narzucać konkretnych szablonów dokumentów w postaci załączników w szczególności, gdy w 2018 roku rejestr czynności zaproponowany i używany przez wiele podmiotów (szczególnie mniejszych) był przez Urząd Ochrony Danych Osobowych na przykładzie szkoły był całkiem inny

https://uodo.gov.pl/pl/123/214

Układ karty jest zdecydowanie przyjemniejszy i czytelniejszy, jednak kodeks nie powinien narzucać wyglądu poszczególnych dokumentów, a jedynie ich zakres.

16.2. Załącznik nr 2 – Rejestr czynności przetwarzania – główne przetwarzania w jednostkach oświatowych

Kategorie danych osobowych

Wskazywanie przez autorów kodeksu poszczególnych rodzajów danych osobowych oraz podstaw prawnych z uwzględnieniem artykułów jest niewłaściwą i niebezpieczną praktyką, gdyż mogą wprowadzić osoby stosujące kodeks w błąd, przykład ten można zaobserwować już w pierwszej czynności przetwarzania:

W przypadku rekrutacji do przedszkoli, na mocy art. 131 ust. 2 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe przetwarzane są dane osobowe:
a. Wielodzietność rodziny kandydata;
b. Niepełnosprawność kandydata;
c. Niepełnosprawność jednego z rodziców kandydata;
d. Niepełnosprawność obojga rodziców kandydata;
e. Niepełnosprawność rodzeństwa kandydata;

f. Samotne wychowywanie kandydata w rodzinie;
g. Objęcie kandydata pieczą zastępczą.

Zapis ten sugeruje, że powyższe dane mogą być przetwarzane tylko w przypadku rekrutacji do przedszkoli, co w sposób rażący wprowadza czytelnika kodeksu w błąd, gdyż kryteria ustawowe opisane w art. 131 ust. 2 na dzień pisania opinii do kodeksu są wykorzystywane w rekrutacji np. do pierwszej klasy szkoły ponadpodstawowej zgodnie z brzmieniem art. 134 ust. 4

„W przypadku równorzędnych wyników uzyskanych na drugim etapie postępowania rekrutacyjnego lub jeżeli po zakończeniu tego etapu dana szkoła, o której mowa w ust. 1, nadal dysponuje wolnymi miejscami, na trzecim etapie postępowania rekrutacyjnego są brane pod uwagę łącznie kryteria, o których mowa w art. 131 kryteria przyjęć do publicznych placówek wychowania przedszkolnego ust. 2. Przepis art. 131 kryteria przyjęć do publicznych placówek wychowania przedszkolnego ust. 3 stosuje się.”.

Ponadto szczegółowe określanie jakie dane rodzajowo są przetwarzane powoduje problem pominięcia niektórych informacji, co również można zaobserwować w pierwszej czynności, gdzie całkowicie pominięto dane z art. 131 ust. 5.

W mojej ocenie autorzy kodeksu winni wskazać jedynie kategorie dany w zakresie informacji podzielonych rodzajowo np. dane identyfikacyjne, dane kontaktowe, dane o sytuacji rodzinnej, dane o sytuacji majątkowej, dane o stanie zdrowia itd. Nie wskazując konkretnych danych, gdyż dla każdej placówki mają one inny zakres, a opisany połowicznie może nieść za sobą poważne problemy w egzekwowaniu prawidłowego stosowania kodeksu.

Propozycja zmiany: Określanie kategorii danych zamiast szczegółowych danych w czynnościach przetwarzania.

Do pozostałych załączników w przedstawionej opinii postanowiłem się nie odnosić, gdyż w swoim założeniu uważam, iż przedstawianie ich formy wizualnej nie powinno podlegać regulacji kodeksu postępowania.

Swój udział w poszczególnych dokumentach autorzy powinni ograniczyć jedynie do wskazanego minimum jakie dany dokument powinien zawierać.

Uwaga ogólna i ostateczna ocena kodeksu

Projekt kodeksu należy ocenić pozytywnie ze względu na swoją przejrzystą i przystępną formę oraz bardzo szeroki zakres regulacji, który w podmiotach oświatowych jest wręcz pożądany co wielokrotnie w opinii przedstawiłem. Autorzy kodeksu dołożyli starań, aby kodeks nie był tylko check listą zgodności z RODO, a materiałem wspomagającym w codziennym stosowaniu przepisów o ochronie danych osobowych.

Niestety część zapisów powstała w sposób obligatoryjny co w mojej ocenie nie powinno być regulowane kodeksem, a jako przykład warto tu wskazać cały szereg załączników stworzony zdecydowanie inaczej niż w Polityka Bezpieczeństwa, gdzie autorzy prawidłowo wskazują co powinno się w niej minimalnie znaleźć, a nie podają jej konkretną treść.

Krytycznie należy odnieść się również do załącznika upoważnienia, gdzie autorzy słusznie w rozdziale 6 wskazują, iż upoważnienie może mieć dowolną formę, a w załącznikach niepotrzebnie narzucają konkretną wybraną przez autorów, ponadto podzieloną na elementy z ustawy wdrażającej co może budzić mylne wyobrażenie wśród czytelników o konieczności zastosowania dla jednej osoby kliku różnych upoważnień jako osobne dokumenty.

Na koniec również warto podkreślić, iż nie podzielam zdania autorów o braku zastosowania podstawy prawnej określonej w art. 6 ust. 1 lit. e w zakresie realizacji zadań w interesie publicznym. Co istotne autorzy wielokrotnie w kodeksie wskazują wykorzystanie danych w interesie publicznym w zakresie danych szczególnej kategorii.

Ponadto zdawać się może, iż w zakresie objętym kodeksem całkowicie autorzy pominęli zakres władczy dyrektora szkoły w związku z wydawaniem przez niego decyzji administracyjnej, gdzie podstawą prawną jest zawsze art. 6 ust. 1 lit. e) „…. lub w ramach sprawowania władzy publicznej powierzonej administratorowi"; Przykładem jest czynność spełniania obowiązku szkolnego poza szkołą, która kończy się wydaniem decyzji administracyjnej zezwalającej lub odmawiającej.

Uwaga 1.

Brak szczegółowego omówienia zasad przetwarzania określonych m.in. w art. 5 RODO na przykładach. To jest fundament RODO

Uwaga 2.

Termin „szkoła" występuje w treści całego kodeksu i zamieniłbym go na „placówka oświatowa". Zakres podmiotowy określa o czym już wspominałem tylko szkoły i przedszkola konkretnego typu a później już tylko info o szkole, dyrektorze szkoły itd.

Reasumując kodeks opiniuje pozytywnie, jednak apeluję do autorów o złagodzenie stanowiska, które w zakresie monitoringu nie powinno znaleźć uznania UODO ani Administratorów danych, a tym bardziej podmiotów danych, gdzie ograniczane jest ich prawo do wniesienia sprzeciwu.

Ponadto sugeruję skupić się w kodeksie na precyzowaniem zapisów RODO a nie wskazywanie „gotowców", gdyż może spotkać się to z oporem we wdrażaniu i zmianie dotychczas wdrożonych wzorców i procedur. Kodeks winien być Skazówkami jak coś interpretować i jakie elementy należy wdrożyć i dostosować, tak aby był możliwy do łatwego monitorowania dla podmiotów monitorujących, a nie był kolejnym dokumentem wymagającym interpretacji.