MATERIAŁY POKONFERENCYJNE

„DRONY A PRYWATNOŚĆ”

autorstwa uczestników
Ogólnopolskiej Konferencji Naukowej
pt. „Drony a prywatność”
o bezpiecznym i świadomym użytkowaniu
dronów, organizowanej przez
Urząd Ochrony Danych Osobowych

Autorzy porad:

mec. Maciej Gawroński
Uczelnia Łazarskiego, Gawroński & Partners S.K.A.

dr Edyta Bielak – Jomaa
Europejskie Centrum Ochrony Danych Osobowych UKSW

dr Dariusz Wasiak
WSB we Wrocławiu

mgr inż. Joanna Wieczorek
Uniwersytet Jagielloński, DENTONS Europe Dąbrowski i Wspólnicy sp. k.

ppor. mar. Łukasz Grzyb
Akademia Marynarki Wojennej WDiOM

URZĄD OCHRONY DANYCH OSOBOWYCH

Redaktor prowadzący:

Tomasz Soczyński

Opracowanie redakcyjne:

Balbina Hermanowicz

Natalia Misiuk

Autorstwo poszczególnych rozdziałów:

mec. Maciej Gawroński
Uczelnia Łazarskiego, Gawroński & Partners S.K.A.

dr Edyta Bielak – Jomaa
Europejskie Centrum Ochrony Danych Osobowych UKSW

dr Dariusz Wasiak
WSB we Wrocławiu

mgr inż. Joanna Wieczorek
Uniwersytet Jagielloński, DENTONS Europe Dąbrowski i Wspólnicy sp. k.

ppor. mar. Łukasz Grzyb
Akademia Marynarki Wojennej WDiOM

Urząd Ochrony Danych Osobowych
ul. Stawki 2,
00-193 Warszawa

URZĄD OCHRONY DANYCH OSOBOWYCH

Warszawa, 8 lipca 2020 r.

Spis treści

Wstęp

Jak naruszyć prywatność za pomocą drona i co za to grozi?

- 1. Odpowiedzialność za naruszenie prywatności za pomocą drona
- 2. Korzystanie z dronów a RODO. Czy każdy użytkownik drona jest ADO?

Monitoring pracowniczy a drony

- 1. Uwagi wstępne
- 2. Podstawy prawne kontroli pracowników
- 3. Drony w środowisku pracy
- 4. Monitoring pracowniczy a drony
- 5. Dron jako źródło informacji o pracowniku
- 6. Zasady przetwarzania danych osobowych z dronów
- 7. Monitoring pracowniczy przy użyciu dronów – zagrożenia

Drony w działaniach straży gminnych (miejskich)

- 1. Wprowadzenie
- 2. Zakres obowiązków komendantów straży jako administratorów
- 3. Zakres i czas przetwarzania danych
- 4. Klasyfikacja danych
- 5. Cel wykorzystywania dronów
- 6. Warunki wykorzystywania dronów
- 7. Drony a mir domowy
- 8. Drony a prywatność
- 9. Prawa osób, których dane dotyczą
- 10. Podstawowe akty prawne

Ochrona danych osobowych uzyskanych przy wykorzystaniu drona

- 1 Wstęp
- 2. Ochrona administracyjna na płaszczyźnie ustawy o ochronie danych

osobowych i RODO

3. Obowiązki dostawców nowych technologii (technology providers). Zasady privacy by design i privacy by default (art. 25 RODO)

4. Monitoring wizyjny a drony. Wytyczne Europejskiej Rady Ochrony Danych

5. Nagrywanie

Wykonując loty dronami marki DJI pamiętaj o tym że:

Przypisy

Wstęp

Zachęcamy Państwa do zapoznania się z materiałami pokonferencyjnymi „Drony a Prywatność”, które stanowią doskonałą okazję do zdobycia niezbędnej wiedzy z zakresu bezzałogowych statków powietrznych oraz budowania świadomości wśród użytkowników dronów w kwestii ochrony prywatności.

Nowoczesna technologia bezzałogowa zaznacza swoją obecność w wielu dziedzinach życia, nie tylko w kwestiach militarnych, ale również biznesie, edukacji, rolnictwie czy sporcie. Dynamiczne tempo rozwoju sektora BSP wymusza konieczność stosowania odpowiednich regulacji prawnych, również tych w zakresie ochrony danych osobowych. Możliwość gromadzenia i przetwarzania przez te urządzenia informacji może bowiem prowadzić do mimowolnego lub celowego pozyskiwania danych, niejednokrotnie stanowiących dane osobowe, co z kolei może prowadzić do utraty prywatności. Dlatego niezwykle istotne jest podejmowanie odpowiednich działań i wypracowanie takich rozwiązań, które przyczynią się do zwiększenia bezpieczeństwa oraz świadomości na temat zagrożeń wynikających z korzystania z dronów.

W materiałach pokonferencyjnych omówione zostały tematy związane z wykorzystywaniem bezzałogowych statków powietrznych oraz związanych z tym regulacji w zakresie ochrony danych osobowych. Poruszono kwestie dotyczące odpowiedzialności za naruszenie prywatności za pomocą dronów oraz ich zastosowania w środowisku pracy. Nie zabrakło również zagadnień z obszaru działalności straży gminnych (miejskich) oraz informatyki śledczej.

Szanowni Państwo, Drodzy Czytelnicy,

oddajemy w Wasze ręce zbiór tekstów prelegentów, którzy wystąpili na Ogólnopolskiej Konferencji Naukowej „Drony a prywatność”. Materiały pokonferencyjne stanowią uzupełnienie wiedzy z zakresu odpowiednich rozwiązań prawnych regulujących korzystanie z dronów, w tym, w szczególności, kwestie ochrony danych osobowych pozyskiwanych za ich pomocą.

Jestem przekonany, że przedstawione zagadnienia przyczynią się do propagowania bezpiecznego używania bezzałogowych statków powietrznych, zgodnie z prawem i poszanowaniem zasad ochrony danych osobowych oraz podniesienia świadomości społeczeństwa na temat zagrożeń dla prywatności wynikających z korzystania z tych urządzeń.

Dziękuję wszystkim osobom, które przyczyniły się do powstania materiałów pokonferencyjnych „Drony a Prywatność”. Szczególne podziękowania kieruję pod adresem Autorów, za poświęcony czas oraz eksperckie i merytoryczne podejście do zagadnienia.

Jan Nowak

Prezes Urzędu Ochrony Danych Osobowych

Jak naruszyć prywatność za pomocą drona i co za to grozi ?

Autor: mec. Maciej Gawroński

1. Odpowiedzialność za naruszenie prywatności za pomocą drona

Prawo do prywatności jest wartością chronioną konstytucyjnie. Zgodnie z art. 47 Konstytucji, każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym[12]. Brak legalnej definicji prywatności. Prywatność można określić jako prawo osoby do utrzymania swoich danych, zwyczajów i zachowań nieujawnionych.

Użytkownik drona za naruszenie czyjejś prywatności może zostać pociągnięty do odpowiedzialności cywilnej, karnej lub administracyjnej. Za to samo działanie użytkownik może zostać pociągnięty do każdej z tych odpowiedzialności niezależnie.

Rodzaje odpowiedzialności za naruszenie prywatności za pomocą drona:

I. Odpowiedzialność cywilna

a) za naruszenia dóbr osobistych. Prywatność jest dobrem osobistym chronionym na gruncie kodeksu cywilnego. Użytkownik drona podglądając, podsłuchując, nagrywając (bez względu na cel takich nagrań), nękając lataniem czy ujawniając informacje prywatne o osobie fizycznej bez wiedzy lub zgody takiej osoby narusza dobra osobiste (art. 23 kodeksu cywilnego).

b) za rozpowszechnianie wizerunku bez zgody. Jeżeli użytkownik drona rozpowszechnia filmiki czy zdjęcia osoby, bez zezwolenia (zgody) danej osoby fizycznej, narusza również art. 81 ustawy o prawie autorskim i prawach pokrewnych. Wyjątkiem są sytuacje, gdy film lub zdjęcie dotyczy „szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza” lub dotyczy osoby publicznej w jej publicznej funkcji.

Odpowiedzialność cywilna użytkownika drona:

Użytkownik za naruszenie dóbr osobistych czy rozpowszechnianie wizerunku bez zgody może zostać zobowiązany do: (i) zaniechania działania (np. usunięcia wrzuconego filmiku na YouTube czy zdjęcia na Facebooku), (ii) złożenia oświadczenia o odpowiedniej treści i odpowiedniej formie (np.

publikacja w gazecie, post na Instagramie), (iii) zapłaty zadośćuczynienia (za krzywdę poniesioną przez osobę, której prywatność została naruszona), (iv) naprawienia szkody, jeżeli na skutek naruszenia osoba fizyczna ponosiła szkodę majątkową (art. 24, 448 kc, 78 ustawy o prawie autorskim i prawach pokrewnych).

WAŻNE: To użytkownik drona musiałby wykazać zgodność z prawem swoich działań w razie sporu.

c) Naruszenie RODO. Kiedy użytkownik drona zostanie uznany za administratora danych w rozumieniu RODO, może także zostać pozwany w oparciu o art. 82 ust. 1 RODO o zapłatę odszkodowania na rzecz osoby, która poniosła szkodę w wyniku przetwarzania jej danych niezgodnie z RODO.

II. Odpowiedzialność karna

Działanie użytkownika drona może w konkretnym przypadku stanowić:

a) zniewagę innej osoby, publikując nagrania znieważające (upokarzające) daną osobę w internecie użytkownik drona podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku (art. 216 § 2 kodeksu karnego);

b) zniesławienie, gdy za pomocą środków masowego przekazu (internet) użytkownik dopuszcza się pomówienia innej osoby, może również zostać pociągnięty do odpowiedzialności z art. 212 kodeksu karnego (grozi grzywna, ograniczenie wolności, a jeśli publikacja w internecie, to do roku pozbawienia wolności);

c) podsłuchiwanie i podglądanie, kiedy użytkownik za pomocą drona bezprawnie uzyskuje informację, do której nie jest uprawniony, może zostać pociągnięty do odpowiedzialności z art. 267 § 3 kodeksu karnego (grzywna, ograniczenie odpowiedzialności, kara pozbawienia wolności do lat 2). Dron można uznać za urządzenie wizualne w rozumieniu tego przepisu. Jeżeli użytkownik drona komukolwiek ujawni bezprawnie pozyskane informacje, również podlega tej odpowiedzialnośc;.

d) naruszenie intymności seksualnej, gdy użytkownik nagrywa podstępnie lub bez zgody rozpowszechnia wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej, odpowiada od 3 miesięcy do 5 lat (art. 191a kodeksu karnego). Czyli jak nagramy parę uprawiającą publiczny seks na plaży, to nie wrzucamy filmiku na Twitter…ani go nie podajemy dalej. Nie nagrywamy też sąsiadów w sytuacji intymnej zaglądając im dronem w okno;

e) złośliwe niepokojenie, kiedy użytkownik drona uporczywie lata (lub w

inny sposób złośliwie niepokoi) inną osobę, może ponieść odpowiedzialność z art. 107 kodeksu wykroczeń, albo

f) uporczywe nękanie – stalking, kiedy użytkownik uporczywie nęka i lata dronem wzbudzając u ofiary uzasadnione okolicznościami poczucie zagrożenia, poniżenia lub udręczenia lub istotnie narusza jej prywatność, może również zostać pociągnięty do odpowiedzialności z art. 190a kodeksu karnego przewidującego od 6 miesięcy do 8 lat pozbawienia wolności;

g) przetwarzanie danych bez podstawy prawnej, kiedy użytkownik drona przetwarza dane, do których przetwarzania nie jest uprawiony, zgodnie z art. 107 ust. 1 i 2 ustawy o ochronie danych osobowych podlega odpowiedzialności karnej do 2 lub 3 lat w zależności od kategorii nielegalnie przetwarzanych danych.

III. Odpowiedzialność administracyjna

Gdy użytkownika drona można uznać za administratora danych osobowych, może on również podlegać karze nakładanej przez Prezesa UODO w trybie art. 83 RODO, której maksymalne limity wynoszą 10 i 20 mln Euro w zależności od kwalifikacji przewinienia.

2. Korzystanie z dronów a RODO. Czy każdy użytkownik drona jest ADO?

Nie każdy użytkownik drona jest administratorem danych osobowych (ADO), nawet jeśli z pomocą drona pozyska informacje o innych osobach, ale każdy może się nim stać.

Zgodnie z art. 2 ust. 2 lit. c. RODO, korzystanie z drona „przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze" nie podlega RODO. Jeśli więc z użyciem drona dowiemy się lub zarejestrujemy coś o innej osobie, ale „nie wyniesiemy tej wiedzy" poza nasz dom, to raczej nie zostaniemy „administratorem" tak pozyskanych danych osobowych w rozumieniu RODO. A kiedy stanie się inaczej?

Aby wyjaśnić powyższe, podzielmy umownie „świat" na 3 strefy latania: strefa własna (nieruchomości własne), strefa publiczna (nieruchomości dostępne publicznie), strefa cudza (obszary niedostępne publicznie), zaś samo korzystanie z drona podzielmy na cztery czynności: latanie, obserwowanie, rejestrowanie, rozpowszechnianie.

Strefa własna. Kiedy latamy/obserwujemy/rejestrujemy strefę własną, nie stajemy się ADO (np. nagrywamy dronem uroczystość domową). Kiedy jednak rozpowszechniamy nagrania, nawet ze strefy własnej, (np. w internecie, w tym na portalu społecznościowym) zawierające wizerunek innych osób lub inne o nich informacje, to prawdopodobnie staniemy się ADO (babcia publikująca zdjęcia wnuczka na Facebooku została uznana za ADO przez sąd holenderski[3]).

Strefa publiczna. Podobnie, kiedy nagrywamy strefę publiczną dla własnych celów rekreacyjnych, żeby potem puszczać je domownikom, jeszcze nie staniemy się ADO. Co innego, gdyby obserwacja lub nagrywanie strefy publicznej lub cudzej (np. granic posesji) miała cel inny, na przykład zapewnienie bezpieczeństwa (element systemu monitoringu), zbieranie materiałów dla celów profesjonalnych lub dla celów publikacji, wtedy będziemy ADO.

Strefa cudza. Natomiast, kiedy nagrywamy strefę cudzą, prawdopodobnie będziemy ADO, nawet jeżeli nie planujemy publikacji. Wynika to z faktu, że obserwacja i nagrywanie osób w ich strefie prywatnej stanowi domyślnie naruszenie ich prywatności, szczególnie gdy wykorzystywane jest do tego specjalistyczne oprzyrządowanie. Należy pamiętać, że takie obserwowanie i

nagrywanie cudzej sfery prywatnej może podlegać odpowiedzialności.

Publikacja w Internecie. Pamiętaj, nagranie naszych domowników czy rodziny w czysto domowym charakterze nie upoważnia do rozpowszechniania czy publikacji takich nagrań np. mediach społecznościowych. Możemy nagrywać naszych domowników czy gości u nas w ogródku i RODO nie ma nic do tego. Jednak, gdy użytkownik drona chce opublikować zdjęcia czy nagrania swoich bliskich w mediach społecznościowych, będzie podlegał wymogom RODO a formalnie także art. 81 ustawy o prawie autorskim i prawach pokrewnych.

Monitoring pracowniczy a drony

Autor: Dr Edyta Bielak-Jomaa

1. Wprowadzenie

Dron to bezzałogowy statek powietrzny, który może odbywać lot autonomiczny (samodzielnie, z użyciem autopilota lub innego systemu na pokładzie) lub sterowany zdalnie przez operatora drona. Dron może przemieszczać się zarówno w zasięgu wzroku operatora oraz poza zasięg jego wzroku, na znaczne odległości. Dron sam w sobie jest technologią, której zastosowanie opiera się na wykorzystaniu danych (w tym danych osobowych – np. na temat pracownika obsługującego dron i o miejscu, w którym się znajduje), jak i może być wyposażony w systemy i narzędzia służące gromadzeniu i przetwarzaniu danych.

Uwzględniając techniczne możliwości bezzałogowych statków powietrznych oraz nieograniczony potencjał systemów, w jakie mogą być wyposażone albo możliwości wykorzystania ich np. do przenoszenia sprzętu, akcesoriów i narzędzi, drony mogą polepszyć, usprawnić i przyspieszyć proces świadczenia pracy, wpłynąć na zwiększenie konkurencyjności świadczonych usług i podnieść ich jakość.

Stosunkowo niski koszt dronów powoduje, że są one wykorzystywane w szeregu rozwiązań. Sam dron, jako taki, nie stanowi większego ryzyka wkroczenia w sferę prywatności i naruszenia ochrony danych osobowych. Może oczywiście być uciążliwy, powodować irytację, czy zaniepokojenie osób, w obszarze funkcjonowania których porusza się.

Zagrożenie dla ochrony danych osobowych mogą stanowić natomiast systemy, w jakie dron jest wyposażony albo narzędzia, jakie na jego pokładzie są umieszczone, lub jakie transportuje. Jeżeli drony przetwarzają dane osobowe (wizerunki osób, pojazdów, tablic rejestracyjnych, danych biometrycznych) za pomocą akcesoriów w nich montowanych, może mieć to istotny wpływ na ochronę danych. Warto zauważyć, że nawet prawidłowe korzystanie z dronów może powodować poważną ingerencję w prywatność i prawa osób, których dane dotyczą. W wielu przypadkach, osoby, których dane dotyczą, nie są świadome „pracy” drona ani tego, jakie urządzenia znajdują się na jego pokładzie, czy następuje nagrywanie, podsłuch, śledzenie osób, czy dochodzi do przetwarzania danych osobowych, przez kogo i do jakich celów służą zbierane. Drony mogą poruszać się zarówno nad terenem publicznym, jak i prywatnym, w zależności od technologii, zbierać

informację z różnych źródeł, łączyć je z danymi pozyskanymi przez inne drony „roju”, należy bowiem również uwzględnić możliwość łączenia kilku dronów np. w celu nadzorowania dużego lub strategicznego, obszaru.

2. Podstawy prawne kontroli pracowników

Najważniejszą powinnością pracownika jest, zgodnie z art. 22§1 k.p., obowiązek wykonywania pracy umówionego rodzaju, na rzecz i pod kierownictwem pracodawcy. Główną przesłanką dla przeprowadzania kontroli pracowników jest zasada podporządkowania. Konkretyzację tego obowiązku określa art. 100 §1 k.p., który wskazuje, że pracownik jest obowiązany wykonywać pracę sumiennie i starannie oraz stosować się do poleceń przełożonych, a zgodnie z art. 100 § 2 pkt 2 k.p. ciąży na nim obowiązek przestrzegania ustalonego porządku pracy.

Zgodnie z treścią art. 22 § 1 k.p., przez nawiązanie stosunku pracy pracownik zobowiązuje się do wykonywania pracy określonego rodzaju na rzecz pracodawcy i pod jego kierownictwem. Pracownicza forma zatrudnienia ma więc miejsce wówczas, gdy mieści się ona w ramach, które są przewidziane przez ustawodawcę dla stosunku pracy – ma charakter pracy podporządkowanej, świadczonej na rzecz konkretnego pracodawcy za wynagrodzeniem i pod jego kierownictwem. Najważniejszą cechą charakteryzującą stosunek pracy jest świadczenie pracy przez pracownika w warunkach podporządkowania. W doktrynie i orzecznictwie panuje zgodność poglądów, że podporządkowanie pracownika jest cechą charakterystyczną dla stosunku pracy i ma charakter konstrukcyjny dla jego istnienia[4].

Zobowiązanie się pracownika do pracy podporządkowanej oznacza jego poddanie się kierownictwu pracodawcy, którego istotą jest prawo wydawania pracownikowi poleceń. Jest ono nieodzownym elementem treści stosunku pracy, ponieważ wchodzi w skład przyjętej konstrukcji przedmiotu zobowiązania pracowniczego[5]**. Pracodawca przyjmuje określony model organizacji i struktury swojej działalności i wyznacza ramy, w których praca ma być wykonywana.** Nie ulega wątpliwości, że kierownictwo obejmować będzie cały czas realizacji procesu pracy. Należy zatem uznać, że w ramach podporządkowania pracowniczego mieści się także przestrzeganie reguł ustalonych przez pracodawcę. Fakt, że pracodawca jest organizatorem tego procesu i ponosi w tym zakresie ryzyko, uzasadnia przyznanie mu szerokich uprawnień władczych, realizowanych poprzez wydawanie poleceń, nakazów, zakazów, zarządzeń, instrukcji, wydawanych w formie ustnej lub pisemnej, adresowanych do jednego, grupy lub ogółu pracowników,

konkretyzowanych co jakiś czas lub codziennie[6] .

Najważniejszą powinnością pracownika jest, zgodnie z art. 22§1 k.p., obowiązek wykonywania pracy umówionego rodzaju. Konkretyzację tego obowiązku określa art. 100§1 k.p., który wskazuje, że pracownik jest obowiązany wykonywać pracę sumiennie i starannie oraz stosować się do poleceń przełożonych[7]. Sumienność jest subiektywnym kryterium oceny przez pracownika jego stosunku do wykonywanej pracy. Pracownik powinien świadczyć pracę wykorzystując w należyty sposób siły i umiejętności oraz kwalifikacje i doświadczenie zawodowe[8], przy uwzględnieniu jego wieku czy stanu zdrowia. Staranność natomiast charakteryzuje się dbałością o jakość pracy, do której pracownik jest obowiązany i ma ona charakter zobiektywizowany. Ustalenie, czy pracownik zachował wymaganą staranność oznacza konieczność odwołania się do obowiązujących, w danym procesie pracy, zasad postepowania. To z kolei rodzi konieczność odwołania się do wzorców staranności, czyli reguł wiedzy, doświadczenia oraz zasad racjonalnego postepowania, którymi pracownik powinien kierować się przy wykonywaniu pracy danego rodzaju. Należyta staranność będzie musiała być oceniana w odniesieniu do charakteru wykonywanej pracy i realizowanych zadań, ponieważ nie jest wzorcem jednolitym dla wszystkich zatrudnionych. Dla poszczególnych branż, grup zawodowych, stanowisk są różne wzorce staranności. Staranność jest niewątpliwie jednym z elementów, które wpływają na ocenę realizacji obowiązków pracownika, w tym jednego z podstawowych - obowiązku przestrzegania ustalonego porządku pracy, o którym mowa w art. 100 § 2 pkt 2 k.p. Gotowość pracownika do świadczenia pracy jest kluczową przesłanką pozostawania w dyspozycji pracodawcy. Gotowość oznacza, że pracownik stawia się do pracy w umówionym czasie i miejscu do dyspozycji pracodawcy z zamiarem wykonywania pracy w stanie (fizycznym i intelektualnym), który umożliwia mu faktyczne jej świadczenie.

> *Kontrola pracowników nie ma charakteru władztwa nad osobami zatrudnionymi.*
>
> *Jej granice wyznacza, z jednej strony cel stosunku pracy, a z drugiej – reguły obowiązującego porządku prawnego, prawa pracy, prawa cywilnego, karnego, ochrony danych osobowych.*

To oznacza, że pracodawca może kontrolować pracownika, czas jego pracy i sposób jej świadczenia. Wymaga to jednak zastosowania rozwiązań zgodnych

z prawem i dopuszczalnych w stosunkach pracy. Kodeks pracy de facto przewiduje, że dopuszczalną formą kontroli pracowników jest monitoring określony w przepisach art. 22^2 i Art. 22^3 k.p. i prowadzony zgodnie z nimi. Podstaw prawnych do innych, niż monitoring, form kontroli pracowników należałoby poszukiwać w przepisach innych ustaw (np. przepisach zezwalających na wykorzystanie biometrii).

3. Drony w środowisku pracy

Trzeba pamiętać, że wykorzystanie narzędzi, które zapisują obraz, czy dźwięk i lokalizują, umieszczonych na pokładzie drona daje większą możliwość nagrywania, podsłuchiwania i śledzenia niż standardowy monitoring. To powoduje, że choć sam dron może nie naruszać prywatności, to jednak dzięki urządzeniom, jakie zawiera można podglądać, podsłuchiwać i oglądać osoby w przestrzeni nie tylko ogólnodostępnej – sferze publicznej ale także w przestrzeni cudzej - prywatnej, w sytuacjach osobistych, a nawet intymnych. Warto też pamiętać, że nawet w sytuacji korzystania z drona w sferze własnej, w sposób zgodny z prawem, można naruszać prywatność. Nietypowość przetwarzania danych osobowych z dronów, czyli odmienne od standardowych metod monitoringu wymagają innych niestandardowych rodzajów i form realizowania obowiązków wobec podmiotów danych, zwłaszcza w zakresie realizacji obowiązków informacyjnych.

Dopuszczalność stosowania dronów w środowisku pracy jest dozwolona, a w wielu przypadkach pomocna lub wręcz pożądana. Dron może być narzędziem pracy wykorzystywanym do prowadzenia badań naukowych, pomiarów, obserwacji. Zastosowanie znajdują min. w budownictwie, transporcie, branży filmowej, górnictwie, logistyce, rolnictwie, turystyce, w pracy służb ratunkowych, itd. Jednak, należy pamiętać, że możliwość używania dronów uzależniona jest od kilku kwestii. W pierwszej kolejności należy odpowiedzieć na pytanie, czy obowiązujące przepisy pozwalają na ich wykorzystywanie do celów cywilnych, komercyjnych. Po drugie, należy uwzględnić cel, w jakim są one wykorzystywane i odpowiedzieć na pytanie, czy gromadzą one dane osobowe. Pozytywna odpowiedź spowoduje konieczność przeprowadzenia analizy systemów, akcesoriów czy narzędzi, w jakie są wyposażone w kontekście ochrony danych osobowych. W dalszej kolejności dokonać takiej analizy w odniesieniu do sprzętu, jaki znajdować ma się na pokładzie dronu (kamery wideo, urządzenia wykrywające – skanery podczerwieni, urządzenia rejestrujące dźwięk, itd.). Uwagi wymaga również określenie obszaru, jaki ma być objęty praca drona i wreszcie zapewnić aby przetwarzanie danych osobowych było uregulowane w sposób zgodny z przepisami o ochronie danych oraz przepisami prawa pracy. Oznacza to, konieczność dokonania oceny wpływu na ochronę danych, biorąc pod uwagę cel operacji, rodzaj dronów (wymiary, widoczność itp.) i technologii na jego pokładzie, określić podstawę prawną przetwarzania danych (zgoda osób, których dane dotyczą, wykonanie umowy, obowiązek prawny, uzasadniony interes itp.) i ewentualną potrzebę powiadomienia /konsultacji z organem

nadzorczym.

Poszukując podstawy prawnej zastosowania dronów przez pracodawcę należy odnieść się do przepisów kodeksu pracy. Nie ulega wątpliwości, że drony mogą być z powodzeniem wykorzystywane do celów zapewnienia bezpieczeństwa i higieny pracy pracowników. Pracodawca ma bowiem **bezwzględny obowiązek** zapewnić wszystkim pracownikom bezpieczne i higieniczne warunki pracy. Zgodnie z art. 207§ 1 k.p., pracodawca ponosi odpowiedzialność za stan bezpieczeństwa i higieny pracy w zakładzie pracy a w świetle § 2, jest on obowiązany chronić zdrowie i życie pracowników przez zapewnienie bezpiecznych i higienicznych warunków pracy przy odpowiednim wykorzystaniu osiągnięć nauki i techniki. Oznacza to, że drony wyposażone w systemy rejestrowania obrazu, dźwięku, narzędzia służące pomiarom np. zadymienia, zapylenia gęstości mgły, mogą być elementami szeroko pojętej polityki bhp. Kamera będąca na pokładzie dronu może być zastosowana do oceny bezpieczeństwa pracownika obsługującego dźwig budowlany w sytuacji braku z nim kontaktu, bądź wówczas, gdy dron transportuje wodę czy posiłek regeneracyjny pracownikom wykonującym pracę w warunkach trudnodostępnych, niezbędny sprzęt ratujący życie lub zdrowie w czasie wypadku lub zagrożenia życia, nadzór nad stanowiskiem archeologicznym, ale tylko wtedy, gdy użycie dronów jest absolutnie konieczne i proporcjonalne.

Drony jako bezzałogowe statki powietrzne przemieszczać się mogą na różne odległości. Rzecz jasna mogą one służyć do kontroli bezpieczeństwa zakładu pracy i obszaru wokół zakładu pracy. Jeżeli dron wyposażony jest w kamerę, powinna ona mieć niską rozdzielczość, tak aby nie można było rozróżnić twarzy, wybór trasy oblotu drona powinien zapewnić gromadzenie jak najmniejszą ilość danych, ograniczeniu powinien podlegać także czas nagrywania, należy rozróżnienie stref lotów – przestrzeń publiczna, obszar zakładu pracy i przestrzeń prywatna (np. tereny przylegające do terenu zakładu pracy), niezbędne jest również przeprowadzanie oceny skutków dla ochrony danych. Nie jest dopuszczalne, aby urządzenia automatycznie rejestrowały obraz i dźwięk (bez dyspozycji operatora) bez uzasadnienia wynikającego z potrzeby realizacji określonego celu.

Zakres stosowania monitoringu na terenie wokół zakładu pracy jest uzależniony od tego, czy rzeczywiście służy ustawowo określonym celom. Pracodawca może wprowadzić szczególny nadzór (monitoring) nad terenem

zakładu pracy lub terenem wokół zakładu pracy, ale tylko jeżeli jest to niezbędne do zrealizowania celów w zakresie bezpieczeństwa osób lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.

Użycie drona wyposażonego w kamerę, który dokonuje oblotów terenu zakładu pracy, utrwala informację o osobach znajdujących się na drodze dojazdowej może być uzasadnione np. w sytuacji, gdy w inny sposób nie można zapewnić bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji.

Nie znajduje jednak uzasadnienia nagrywanie terenu sąsiednich firm, czy sąsiadujących z terenem zakładu pracy prywatnych posesji, ponieważ wykracza to poza cele określone przepisami k.p., przetwarzanie więc danych osobowych w związku z takimi nagraniami nie byłyby adekwatne, stosowne oraz ograniczone do tego, co jest niezbędne do celów, w których są przetwarzane, co prowadziłoby do naruszenia zasady minimalizacji danych.

Celem zastosowania drona i urządzeń znajdujących się na jego pokładzie nie może być kontrola pracownika, jego czasu pracy ani sposobu wykonywania pracy.

4. Monitoring pracowniczy a drony

Wykorzystanie dronów w stosunkach pracy dotyczyć będzie najczęściej, choć nie wyłącznie, monitoringu pracowniczego. Należy zauważyć, że kwestie monitoringu zostały uregulowane w przepisach kodeksu pracy. Zgodnie z art. 22^2 § 1.k.p. , jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, pracodawca może wprowadzić szczególny nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring). Nagrywanie dźwięku niesie za sobą ryzyko przetwarzania przez administratora danych szczególnych kategorii i jest nadmiernym ingerowaniem w prywatność pracownika. Takie stanowisko wyraził także Prezes UODO "Przepisy o monitoringu nie zezwalają co do zasady na nagrywanie dźwięku towarzyszącego zdarzeniom. Takie uprawnienia posiadają jedynie służby porządkowe i specjalne na podstawie ustaw regulujących ich działalność. Stosowanie rejestracji dźwięku może zostać uznane za nadmiarową formę przetwarzania danych, wiązać się z odpowiedzialnością administracyjną i cywilną, a nawet karną" *(Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego, s.26,* [*https://uodo.gov.pl/pl/383/354*](https://uodo.gov.pl/pl/383/354)).

Art. 22^3 § 1 k.p. reguluje monitoring poczty elektronicznej. W świetle tego przepisu, jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, pracodawca może wprowadzić kontrolę służbowej poczty elektronicznej pracownika (monitoring poczty elektronicznej).

Ustawodawca przewiduje także możliwość stosowania innych, niż wskazane wyżej, form monitoringu (22^3§4 k.p.). Jednocześnie zastrzega, że mogą być one stosowane wyłącznie z sytuacji, gdy ich zastosowanie jest konieczne do realizacji celów określonych w § 1 oraz, że w razie ich wprowadzenia, odpowiednio stosuje się do nich przepisy o monitoringu wizyjnym. Zatem dopuszczalne jest stosowanie przez pracodawcę, innych form monitoringu np. monitoringu GPS samochodów służbowych, monitoringu urządzeń

kserograficznych, monitoringu zachowania w Internecie czy też monitoringu przemieszczania się po zakładzie pracy. Jednocześnie nie oznacza to, że pracodawca może stosować wszystkie, jakiekolwiek formy monitorowania technologicznie dające się instalować i korzystać z nich w miejscu pracy.

Muszą one bowiem:

1. być kwalifikowane jako monitoring, o jakim mowa w art. 22^3 k.p.,
2. realizować cele określone w art. 22^3 § 1 k.p. (zapewnienie organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy),
3. spełniać wszystkie z wymogów przewidzianych w Kodeksie pracy dla stosowania form monitoringu i zapewnić, aby monitoring w poszczególnych formach był stosowany jedynie w takich celach, dla jakich jest to możliwe na podstawie odpowiednich przepisów kodeksu pracy.

Monitoring nie może obejmować pomieszczeń udostępnianych zakładowej organizacji związkowej, jak również pomieszczeń sanitarnych, szatni, stołówek oraz palarni, chyba że pracodawca jest w stanie obiektywnie wykazać niezbędność monitorowania tych pomieszczenia w celu ochrony osób i mienia, kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę i nie naruszy godności oraz innych dóbr osobistych pracownika, w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób. Monitoring pomieszczeń sanitarnych wymaga uzyskania uprzedniej zgody zakładowej organizacji związkowej, a jeżeli u pracodawcy nie działa zakładowa organizacja związkowa - uprzedniej zgody przedstawicieli pracowników wybranych w trybie przyjętym u danego pracodawcy.

Pracodawca jest zobowiązany do ustalenia celów, zakresu oraz sposobu zastosowania monitoringu w układzie zbiorowym pracy lub w regulaminie pracy albo w obwieszczeniu, jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy. Pracodawca jest zobowiązany do poinformowania pracowników o wprowadzeniu monitoringu, w sposób przyjęty u danego pracodawcy, nie później niż 2 tygodnie przed jego uruchomieniem.

W przypadku wprowadzenia monitoringu pracodawca oznacza pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż jeden dzień przed jego uruchomieniem.

Nagrania obrazu pracodawca przetwarza wyłącznie do celów, dla których zostały zebrane, i przechowuje przez okres nieprzekraczający 3 miesięcy od dnia nagrania. W przypadku, gdy nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub pracodawca powziął wiadomość, iż mogą one stanowić dowód w postępowaniu, termin ten ulega przedłużeniu do czasu prawomocnego zakończenia tego postępowania. Natomiast po upływie tych terminów, uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe, podlegają zniszczeniu, o ile odrębne unormowania nie stanowią inaczej.

Administrator danych (pracodawca) powinien przeprowadzić ocenę skutków dla czynności przetwarzania, jaką jest nagrywanie obrazu w miejscach publicznych. Konieczność jej przeprowadzenia a art. 22^2 k.p., zgodnie z którymi administrator może zastosować monitoring wizyjny, tylko i wyłącznie wtedy gdy jest to niezbędne do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.

> *Pracodawca może legalnie wykorzystywać monitoring wizyjny do wskazanych celów, jeżeli będzie w stanie bezsprzecznie i formalnie wykazać, że jest to faktycznie niezbędne.*

Pracownicy wykonujący czynności w postaci monitorowania pracy innych pracowników, powinni w tym zakresie posiadać odpowiednie upoważnienie do przetwarzania danych osobowych.

5. Dron jako źródło informacji o pracowniku

Należy zauważyć, że mimo, iż dron nie może być wykorzystywany jako narzędzie kontroli pracowników, to jego stosowanie przez pracodawcę do określonych, zgodnych z prawem celów będzie automatycznie powodować możliwość kontroli pracownika – operatora drona. System, w jaki wyposażone jest urządzenie pozwala na monitorowanie zachowań operatora, czasu w jakim rozpoczyna obsługę urządzenia, czasu zakończenia jego sterowania, miejsce, w jakim się znajduje. Może zatem być źródłem informacji o wykonywaniu zadań, sposobu wykorzystania urządzenia i czasu pracy. Należałoby więc uznać, że dron w stosunku do obsługującego go pracownika, stanowi inną formę monitoringu, wskazaną w art. 22^3 § 4 k.p.

Przyjmując takie stanowisko, należy pamiętać, że w stosunku do tego pracownika, w razie ich wprowadzenia, odpowiednio stosuje się do nich przepisy o monitoringu wizyjnym, a ponadto w stosunku do tego pracownika, pracodawca powinien spełnić obowiązek informacyjny.

We wszystkich przypadkach pracodawcy powinni rozważyć, czy stosowanie określonego sposobu kontroli, np. przy użyciu dronów:

- ma prawną podstawę,
- jest konieczne,
- jest proporcjonalne,
- czy czynność przetwarzania jest przejrzysta, jest to też istotne z punktu widzenia zakazu dyskryminacji pracowników.

6. Zasady przetwarzania danych osobowych z dronów

Przetwarzanie danych osobowych w związku ze stosowaniem przez pracodawcę drona musi następować zgodnie z zasadami określonymi w RODO. Wymaga się zatem od pracodawcy/administratora aby przetwarzanie było oparte o przesłanki: zgodności z prawem, rzetelności, przejrzystości, ograniczenia do celu, minimalizacji danych, ograniczenia przechowywania, integralność i poufność oraz rozliczalności.

Pracodawcy w świetle przepisów o ochronie danych mogą kontrolować pracowników. Muszą jednak uwzględnić, że:

1. dane osobowe muszą być gromadzone w określonych, wyraźnych i prawnie uzasadnionych celach, i nie przetwarzane dalej w sposób niezgodny z tymi celami;
2. w odniesieniu do większości przypadków przetwarzania danych w miejscu pracy podstawą prawną **nie może i nie powinna być zgoda pracowników** ze względu na charakter stosunków między pracodawcą i pracownikiem;
3. jeżeli pracodawca powołuje się na uzasadniony interes, cel przetwarzania danych musi być **zgodny z prawem**; **wybrana metoda lub określona technologia musi być konieczna**, **proporcjonalna i wdrażana w możliwie najmniej inwazyjny sposób**, a także **musi umożliwiać pracodawcy wykazanie, że wprowadzono odpowiednie środki w celu zapewnienia równowagi z podstawowymi prawami i wolnościami pracowników**;
4. pracownicy powinni zostać wyraźnie i dokładnie poinformowani o przetwarzaniu ich danych osobowych, w tym o istnieniu technologii kontrolowania;
5. dane osobowe mogą być przetwarzane tak długo, jak wymaga tego osiągnięcie celu;
6. pracodawca musi przestrzegać zasady minimalizacji danych. Musi więc odpowiedzieć na pytanie, czy cel, jakim jest bezpieczeństwo pracowników, ochrona mienia, tajemnicy produkcji czy przedsiębiorstwa nie może być osiągnięty w inny, mniej inwazyjny sposób, niż wykorzystywanie obrazu z dronu; jeżeli nie ma innego sposobu, musi zastosować taką technologię i przyjąć środki ochrony danych, które pozwolą na uniknięcie gromadzenia i przetwarzania zbędnych danych;
7. w odniesieniu do technologii, które mogą elektronicznie odczytywać i

przetwarzać dane biometryczne (rozpoznawanie twarzy, identyfikacja behawioralna), stosować np. efekty graficzne uniemożliwiające rozpoznawanie twarzy, aby uniknąć gromadzenia wizerunków osób możliwych do zidentyfikowania, gdy nie jest to konieczne;

8. pracodawcy muszą przyjąć i wdrożyć odpowiednie środki techniczne i organizacyjne mające zapewnić bezpieczeństwo przetwarzania;
9. dron jest nośnikiem informacji, wyposażonym w pamięć i jako nośnik podlega zabezpieczeniu, samo urządzenie jest zbiorem danych, które gromadzi;
10. jeżeli dron przekazuje dane bezpośrednio przez teletransmisję, to tę teletransmisję należy zabezpieczyć, poprzez zaszyfrowane kanały przesyłowe.

7. Monitoring pracowniczy przy użyciu dronów – zagrożenia

Pracodawcy zamierzający korzystać z systemu dronów, powinni uwzględnić także zagrożenia, jakie mogą towarzyszyć stosowaniu tego rodzaju technologii. Mogą mieć one bowiem negatywny wpływ na prawa podstawowe pracowników do organizowania się, organizowania spotkań pracowniczych oraz do komunikowania się w sposób poufny (w tym na prawo do uzyskiwania informacji). Kontrolowanie komunikacji i zachowań może wywierać presję na pracowników, aby zachowywali się w sposób oczekiwany przez pracodawcę. Inne zachowania oceniane mogą być jako anomalie i powodować mogą wyciąganie negatywnych konsekwencji wobec pracowników. Pracownicy mogą nie zdawać sobie sprawy z istnienia samej technologii i mogą nie być świadomi, jakie dane osobowe i do jakich celów są przetwarzane. Monitorowanie przy użyciu dronów może odbywać się w sposób ukryty. W przypadku braku łatwo zrozumiałej i łatwo dostępnej polityki monitorowania w miejscu pracy pracownicy mogą nie zdawać sobie sprawy z istnienia i skutków stosowania tej formy kontroli, a w związku z tym nie są w stanie korzystać ze swoich praw. Taka technologia może powodować gromadzenie nadmiernej ilości danych, np. danych dotyczących lokalizacji, nałogów (np. tytoniowego), rozmów o charakterze osobistym.

Zwiększenie ilości danych generowanych w środowisku pracy, w połączeniu z tą techniką oraz stosowanie technik analizowania i zestawiania danych, może stwarzać ryzyko dalszego przetwarzania niezgodnego z przepisami, np. wykorzystywanie systemów, które zgodnie z prawem zainstalowano w celu ochrony własności, do monitorowania dostępności i wyników pracy pracowników czy też regularnego monitorowania zachowania pracowników i do ciągłego śledzenia ich ruchów. Szerokie wykorzystanie takiej technologii może zmniejszyć gotowość pracowników do informowania pracodawców o nieprawidłowościach lub nielegalnych działaniach przełożonych lub innych pracowników, które mogą zaszkodzić działalności lub miejscu pracy. Kontrolowanie naruszające prawa pracowników do prywatności może utrudniać konieczną komunikację z odpowiednimi służbami na terenie zakładu pracy, np. społecznym inspektorem pracy. Z punktu widzenia psychologii pracy, może także wpływać na obniżenie samooceny pracownika i zaburzenie prawidłowych wzajemnych relacji pracownik – pracodawca.

Wykorzystując drony pracodawca powinien pamiętać, aby wybrać najbardziej proporcjonalną do celu monitoringu technologię na pokładzie drona i zastosować wszystkie odpowiednie środki bezpieczeństwa, tak aby uniknąć gromadzenia i / lub dalszego przetwarzania niezgodnego z prawem, znaleźć najbardziej odpowiedni sposób spełnienia obowiązku informacyjnego oraz wcześniejszego powiadomienia osób, na które może mieć wpływ przetwarzanie danych (np. za pomocą drogowskazów lub arkuszy informacyjnych w przypadku operacji wizualnych na określonym obszarze), podjąć wszelkie odpowiednie środki techniczne i organizacyjne, aby zapewnić poziom bezpieczeństwa odpowiedni do zagrożeń, jakie stwarza przetwarzanie i charakter przetwarzanych danych, usuwać dane osobowe wkrótce po ich zebraniu lub tak szybko, jak wymagają tego przepisy kodeksu pracy.

Drony w działaniach straży gminnych (miejskich)

Autor: dr Dariusz Wasiak

1. Wprowadzenie

W dniu 31 grudnia 2020 r. rozpocznie się bezpośrednie stosowanie przepisów rozporządzenia Wykonawczego Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych[9], które znacząco zaostrzą wymagania stawiane producentom, dystrybutorom oraz operatorom i pilotom bezzałogowych statków powietrznych m.in. w zakresie ochrony danych osobowych i zapewnienia prywatności osobom fizycznym, o których mogą zostać uzyskane informacje w wyniku eksploatacji dronów.

Z uwagi na wprowadzane w Rozporządzeniu rozwiązania, pojawiła się konieczność przeprowadzenia, przez straże gminne (miejskie)[10] wszechstronnej oceny występujących procesów, w ramach których dochodzi do przetwarzania informacji, w tym danych osobowych na potrzeby realizacji zadań wynikających z ustaw i aktów prawa miejscowego, a prowadzonych z zastosowaniem środków technicznych[11],do których zaliczyć należy drony[12].

Niniejszy poradnik skierowany jest do komendantów straży gminnych (miejskich)[13] jako administratorów danych osobowych[14] oraz podległych im strażników, którzy przetwarzając szeroki zakres informacji w ramach realizowanych ustawowych zadań decydują o całości procesu, bądź mają wpływ na sposób i cel przetwarzania danych osobowych, w szczególności ich pozyskiwania za pośrednictwem posiadanych, lecz prawnie dopuszczalnych środków technicznych – dronów, czyli bezzałogowych statków, w szczególności powietrznych[15]. Przy czym dronem określamy, na potrzeby poradnika, urządzenie zdolne do unoszenia się w atmosferze na skutek oddziaływania powietrza innego niż oddziaływanie powietrza odbitego od podłoża[16].

2. Zakres obowiązków komendantów straży jako administratorów

Na mocy przepisów ustawy o strażach każdy komendant straży, niezależnie od wielkości i ulokowania straży w strukturze określonej gminy, jest administratorem danych osobowych przetwarzanych w celu:

1. rozpoznawania,
2. zapobiegania,
3. wykrywania i
4. zwalczania czynów zabronionych dla bezpieczeństwa i porządku publicznego[17].

Innymi słowy, każdy komendant jest administratorem danych osobowych wskazanym przez ustawodawcę, który może samodzielnie lub wspólnie z innym właściwym organem lub właściwymi organami ustalać cele i sposoby przetwarzania danych osobowych, oczywiście wyłącznie w zakresie nie wykraczającym poza zasięg ustawowo wskazanych uprawnień. Bez wątpienia każdy komendant jest zatem zobowiązany do przestrzegania obowiązków określonych przez przepisy ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[18].

W zależności natomiast od rodzaju operacji, bądź też realizowanych procesów w straży oraz jej ulokowania w strukturach gminy, komendant zobowiązany jest również do:

1. przestrzegania przepisów 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)[19] oraz

2. wymogów stawianych przez przepisy rozporządzenia Wykonawczego Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych[20] w zakresie ochrony danych osobowych.

Należy jednocześnie podkreślić, że nawet w przypadku wykazania przez komendanta, że przetwarzane przez straż dane osobowe znajdują się wyłącznie w aktach spraw lub czynności bądź urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych, które prowadzone są na podstawie m.in. ustawy z dnia 24 sierpnia 2001 r. - Kodeks postępowania w sprawach o wykroczenia[21], nie jest możliwe stwierdzenie, iż komendant jako administrator zwolniony jest z obowiązku ochrony przetwarzanych przez straż danych osobowych. Wyłącznie, o którym mowa w art. 3 ust.1 DODO należy odnosić i odczytywać przez pryzmat art. 26 DODO, który ogranicza zakres dostępu do danych osobowych pomiotu praw, ale nie znosi obowiązku ich ochrony. W takich okolicznościach uprawnienia dostępowe podmiotu praw, których dane przetwarza straż regulują przepisy prawa procesowego – właściwego, z uwagi na postępowanie, w ramach którego tworzone są akta lub urządzenia ewidencyjne. Podmiotom danym przysługiwać będą zatem prawa zależne od roli w jakiej będą w takim postępowaniu występować.

3. Zakres i czas przetwarzania danych

Straże na mocy przepisów ustawy o strażach posiadają prawo do:

1. przetwarzania, w celu realizacji zadań ustawowo określonych, danych osobowych zwykłych i wrażliwych (szczególnych kategorii) a także danych o naruszeniach prawa,
   oraz
2. przetwarzania danych osobowych bez wiedzy i zgody osoby, której one dotyczą, co jest jednak możliwe wyłącznie w przypadku przetwarzania danych uzyskanych:

   (a) w wyniku wykonywania czynności podejmowanych w postępowaniu w sprawach o wykroczenia,

   (b) z rejestrów, ewidencji i zbiorów, do których straże posiadają dostęp na podstawie odrębnych przepisów,

w celu zidentyfikowania sprawcy naruszenia obowiązujących przepisów. A więc wyłącznie po wykazaniu podjęcia przez straż czynności dających podstawę do tego, aby określony czyn, a tym samym określone zachowanie podmiotu danych można było uznać za wykroczenie, o którym mowa w art. 1 ustawy z dnia 20 maja 1971 r. Kodeks wykroczeń[22].

Należy zatem przyjąć, że:

(1) przywołane prawo nie przekłada się na:

(a) w pełni swobodne wyznaczania celów i zakresu przetwarzania danych osobowych,

(b) możliwość działania straży z niejawnym wykorzystaniem dronów,

(2) celem działań straży z wykorzystaniem dronów nie może być przetwarzanie danych wrażliwych w zakresie:

(a) pochodzenia rasowego lub etnicznego,

(b) poglądów politycznych,

(c) przekonań religijnych lub filozoficznych,

(d) przynależności wyznaniowej,

(e) partyjnej lub związkowej, jak również danych o

(f) stanie zdrowia,

(g) kodzie genetycznym,

(h) nałogach lub życiu seksualnym,

nawet w przypadku odebrania zgody. Chyba, że dane takie zostały upublicznione lub straż uzyskała do nich dostęp bez intencji przetwarzania tego rodzaju danych (np. dane zostały zarejestrowane w związku z innym celem i stanowią integralna część nagrania – a informacje objęte zakazem ujawniają kontekstowo). Jednakże nawet w takich okolicznościach straż jest obwiązana wykazać niezbędność ich przetwarzania (oraz/lub brak możliwości natychmiastowego usunięcia).

Ponadto możliwość przetwarzania danych wrażliwych, pojawiająca się w sytuacji współdziałania z właściwymi podmiotami, w celu:

- ochrony życia lub zdrowia lub
- interesów osoby, której dane dotyczą, lub innej osoby,
  jest wyjątkiem od zasady zakazu ich przetwarzania i nie zwalnia od wykazania niezbędności ich przetwarzania.

W ten sam sposób należy traktować wszystkie inne sytuacje, wskazane w art. 11 ust. 1 ustawy o strażach, których zaistnienie będzie potencjalnie generować możliwość pozyskania danych wrażliwych. Każdorazowo wymaga to przeprowadzenia oceny niezbędności ich przetwarzania.

(3) przetwarzanie danych osobowych zebranych z wykorzystaniem dronów po ustaniu celu głównego, określonego w ramach planowanej operacji dronem wymusza na strażach konieczność wykazania wystąpienia niezbędności ich dalszego przetwarzania lub obowiązku prawnego z uwzględnieniem możliwych zmiennych klasyfikujących utrwalony czyn jako czyn zabroniony, do których zalicza się:

(a) społeczną szkodliwość czynu, której stopień szkodliwości uzależniony jest od uzewnętrznionego zachowania człowieka (działania lub zaniechania), będącego przejawem woli tego człowieka. Stąd też brak wykazania szkodliwości czynu przekreśla byt wykroczenia,

(b) bezprawność, która wiąże się z tym, że określony czyn musi być

zabroniony przez ustawę obowiązującą w czasie jego popełnienia pod groźbą kary aresztu, ograniczenia wolności, grzywny do 5000 złotych lub nagany,

(c) zawinienie, które wymusza niezbędność przypisania dokonania czynu zabronionego konkretnemu podmiotowi danych w określonym czasie, bądź dokonania ustaleń, że możliwość braku przypisania winy konkretnemu człowiekowi w określonym czasie jest wykluczona z punktu widzenia przeciętnie roztropnego człowieka. Stąd też do katalogu tego zaliczyć należy zachowanie podmiotu danych w określonym stadium popełniania czynu z uwzględnieniem:

- zamiaru,
- przygotowania,
- usiłowania,
- dokonania,

gdzie każda postać stadialna objęta jest karalnością tylko wówczas, gdy ustawa tak stanowi.

4. Klasyfikacja danych

Obowiązek wynikający z ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[23] wymusza na strażach:

(1) niezbędność prowadzenia kategoryzacji pozyskanych danych na dane:

(a) osób, w stosunku do których istnieją poważne podstawy, aby przypuszczać, że popełniły lub zamierzają popełnić czyn zabroniony,

(b) osób skazanych za czyn zabroniony,

(c) pokrzywdzonych czynem zabronionym lub osób, w przypadku których określone fakty wskazują, że mogą stać się ofiarami czynu zabronionego,

(d) innych osób związanych z czynem zabronionym, takich jak osoby, które mogą zostać wezwane do złożenia zeznań w sprawie czynu zabronionego lub na dalszych etapach postępowania, osoby, które mogą dostarczyć informacji o czynach zabronionych, lub osoby, które mają kontakty lub powiązania z jedną z osób, o których mowa w pkt (a) i (b).

(2) rozróżniania danych na dane mające swoje źródło w:

(a) faktach,

(b) indywidualnych ocenach

o ile będzie to możliwe lub nie będzie dalece utrudnione na dane osobowe.

(3) ewidencjonowania operacji przetwarzania danych polegających w szczególności na:

(a) zbieraniu,

(b) modyfikowaniu,

(c) przeglądaniu,

(d) ujawnianiu wraz z przekazywaniem,

(e) łączeniu,

(f) usuwaniu.

(4) ewidencjonowania operacji przetwarzania danych w oparciu o:

(a) datę i godzinę operacji,

(b) tożsamość osoby, która przeglądała lub ujawniła dane osobowe – w miarę możliwości,

(c) tożsamość odbiorców danych osobowych – w miarę możliwości,

(d) zasadność operacji – dla ewidencji prowadzonych w sposób niezautomatyzowany;

z tym, że: ewidencje winny być przeznaczone wyłącznie:

• do weryfikowania zgodności przetwarzania danych z prawem;

• do monitorowania własnej działalności;

• dla zapewnienia integralności i bezpieczeństwa danych osobowych;

• na potrzeby prowadzonych postępowań.

Należy jednak zdawać sobie sprawę, że obowiązujące wyłączenia, obejmujące stosowanie ustawy w zakresie akt i urządzeń ewidencyjnych, czynią z tych zasad problem raczej teoretyczny niż praktyczny. Oczywiście gdyby straż dysponowała możliwością oznaczania kategorii osób, których dane są przetwarzane, bezpośrednio przez drony (w trakcie realizacji nagrań lub monitorowania) należało by zastosować odpowiednie oznaczenia. Biorąc jednak pod uwagę specyfikę omawianej sytuacji wszelkie oznaczenia i kategoryzacja będą jednak zasadniczo występować na późniejszych etapach procesów przetwarzania – czyli w ramach tworzenia owych, wyłączonych ze stosowania ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, akt i urządzeń ewidencyjnych, rządzących się autonomicznymi regułami przetwarzania wynikającymi z regulacji właściwych postępowań.

5. Cel wykorzystywania dronów

W ramach realizacji zadań wynikających z ustaw i aktów prawa miejscowego straże na terenie gminy, na której zostały one powołane mogą przetwarzać dane osobowe[24], także z wykorzystaniem dronów wykonujących określone operacje w przestrzeni powietrznej[25], wyłącznie w celu:

(1) utrwalenia dowodów popełnienia przestępstwa lub wykroczenia,

(2) przeciwdziałania przypadkom naruszania spokoju i porządku w miejscach publicznych,

(3) realizowania ochrony obiektów komunalnych i urządzeń użyteczności publicznej,

przy wykazaniu niezbędności wsparcia takich działań w ramach:

(1) obserwacji i rejestracji obrazu zdarzeń[26],

(2) określenia emisji poziomu szkodliwych substancji wydobywających się z obiektu poddanego kontroli,

(3) ratowania życia lub zdrowia.

Stąd też możliwość wykonania operacji w przestrzeni powietrznej zależna jest m.in. od:

(1) wykazania zgodności z celami ustawowo wskazanymi,

(2) wykazania niezbędności zastosowania dronów,

(3) ustalonego poziomu i zakresu występujących ryzyk w obszarze ochrony danych osobowych i zapewnienia prywatności.

Innymi słowy:

(1) zbyt wysoki poziom występujących zagrożeń w obszarze niezbędności zapewnienia ochrony danych osobowych i prywatności, których zakres straż nie będzie mogła skutecznie zminimalizować w ramach posiadanych aktywów i zasobów

oraz

(2) brak wykazania zgodności z celami ustawowo wskazanymi

(3) brak wykazania niezbędności zastosowania dronów w celu wspomożenia działań straży,

uniemożliwia wykonanie planowanej operacji.

6. Warunki wykorzystywania dronów

Drony wyposażone w urządzenia umożliwiające rejestrację danych osobowych mogą być wykorzystywane przez straże tylko i wyłącznie na terenie gminy, w których zostały one powołane oraz tylko i wyłącznie w miejscach ogólnodostępnych, czyli z wyłączeniem stref objętych zasięgiem miru domowego lub innych stref geograficznych ustawowo oznaczonych oraz w szczególności pod warunkiem, że:

(1) rejestrator zainstalowany na dronie nie ma możliwości utrwalania dźwięku oraz temperatury ciała,

(2) dron będzie zaliczony co najmniej do kategorii szczególnej,

(3) dane osobowe nie będą przetwarzane poza EOG, w tym na terenie USA,

(4) dane osobowe będą chronione adekwatnie do ustalonych zagrożeń,

(5) operator systemu[27] posiadać będzie wymagane uprawnienia i ubezpieczenie,

(6) pilot systemu[28] posiadać będzie wymagane kwalifikacje i uprawnienia, w szczególności szkolenia z zakresu:

(a) ochrony danych,

(b) zapewnienia prywatności,

(7) dokonano uprzedniej analizy mogących wystąpić zagrożeń podczas operacji,

(8) zgłoszono i uzgodniono z Polską Agencją Żeglugi Powietrznej planowaną operację,

(9) przeprowadzona analiza wskazała na niezbędność wspierania działań strażników z wykorzystaniem dronów.

7. Drony a mir domowy

Każda realizowana przez straż operacja z wykorzystaniem dronów wyposażonych w rejestrator danych, w szczególności w ramach realizacji zadań związanych z ochroną środowiska, niesie ze sobą ryzyko bezprawnej ingerencji w obszary objęte mirem domowym.

Stanu tego nie zmienia posiadanie upoważnienia wydanego przez wójta na mocy przepisu art. 379 ust. 2 ustawy z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska[29]. Obszary objęte mirem domowym chronione są bowiem na mocy art. 50 Konstytucji RP, art. 193 ustawy z dnia 6 czerwca 1997 r. - Kodeksu karnego[30] oraz art. 23 ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny[31].

Co więcej, przepisy procesowe regulowane przez art. 220 ustawy z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego[32] nie uzbrajają straży w jakiekolwiek uprawnienie do działania w ramach posiadanych kompetencji na terenie objętym mirem domowym w godzinach 22.00 – 6.00 (czas ciszy nocnej) nawet w ramach uprzednio już podjętej kontroli.

Do obszarów zastrzeżonych (z uwagi na chroniący je mir domowy) zaliczyć należy każdy teren zamieszkałej nieruchomości oznaczonej choćby małym, nawet niewidzialnym z lotu drona oznaczeniem, jak i inne pomieszczenie lub teren, w którym przebywa lub może przebywać osoba nie przyzwalająca na ingerencje w strefę, w której przebywa oraz czuje się bezpiecznie.

Innymi słowy, mir domowy chroni pewną określoną przestrzeń, strefę, w której osoba w niej przebywająca ma prawo zakładać, że bez jej wyraźnej zgody lub wiedzy, nikt, w zgodzie z obowiązującym prawem, go nie naruszy.

Zatem do obszarów nie objętych mirem domowym zaliczyć należy niezamieszkały teren nieruchomości, obiektu lub ich części, na których prowadzona jest działalność gospodarcza.

Przestrzeń objęta mirem domowym rozciąga się nie tylko horyzontalnie, ale również wertykalnie nad obszarem określonej, otwartej nieruchomości, na co

komendant straży, jako administrator danych, zobowiązany jest zwrócić uwagę w ramach projektowania każdej operacji z udziałem dronów wyposażonych w rejestrator danych.

8. Drony a prywatność

Każdy organ władzy publicznej, jakim jest również straż, może działać wyłącznie na podstawie i w granicach prawa, o czym stanowi wprost art. 7 Konstytucji RP. Natomiast każdy podmiot danych objęty zasięgiem rejestratora danych ulokowanego na dronie uzbrojony jest w prawo do poszanowania swojego życia prywatnego i rodzinnego, o czym mówi wprost art. 47 Konstytucji RP (w sposób pośredni, ale odnoszący się wprost do informacji o osobie, również art. 51 Konstytucji RP).

Stąd też straże, a dokładniej ich komendanci, planując operacje z wykorzystaniem dronów zobowiązane są uwzględnić w swoich analizach skuteczność respektowania zasady proporcjonalności osadzonej w art. 31 ust. 3 Konstytucji RP, odczytywanej tutaj jako norma gwarancyjna, której celem jest ochrona praw i wolności każdego podmiotu przed nadmierną ingerencją działań realizowanych przez straż, a także zminimalizować ryzyko ingerencji w prywatność, czyli zaplanować lot dronem w taki sposób, aby działania prowadzone z jego wykorzystaniem nie powodowały szkody dla podmiotu danych, a możliwość gromadzenia danych o osobach wynikała bezpośrednio z ustawy, czego wymaga art. 51 Konstytucji RP.

9. Prawa osób, których dane dotyczą

Każda osoba fizyczna ma prawo zakładać, że jej prywatność nie jest naruszana, a jej dane osobowe nie są przetwarzane z naruszeniem prawa. Dlatego też w przypadku podejrzenia wystąpienia naruszenia jej praw dysponuje ona uprawnieniem skutkującym możliwością:

(1) uzyskania w każdym czasie informacji w zakresie określonym przez:

(a) art. 15-22 i 33 RODO

(b) art. 22-30 DODO

(c) art. 6 ustawy z 6 września 2001 r. o dostępie o informacji publicznej[33]

(2) zgłoszenia naruszenia do Prezesa UODO,

(3) wniesienia wobec komendanta roszczenia o naruszenie dóbr osobistych, o których mowa w art. 23 ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny[34],

(4) zgłoszenia przekroczenia lub niedopełnienia obowiązków do Prokuratury. W tym przypadku istotnym jest to, że do zaistnienia znamion przestępstwa nie jest konieczne, aby wystąpił jakikolwiek uszczerbek w dobrach chronionych prawem, gdyż przedmiotem ochrony jest prawidłowe funkcjonowanie instytucji państwowych i samorządu terytorialnego, a także wynikający z tego ich autorytet. Stąd też źródłem naruszeń mogą być zarówno normy prawne regulujące obowiązki komendanta, jak i polecenia organów kontrolnych, bądź nadzorczych lub polecenia służbowe wydane przez wójta[35], o ile ich zakres mieści się w granicach posiadanych uprawnień, a niebezpieczeństwo będzie rzeczywiste i skonkretyzowane[36],

(5) a nawet w sytuacjach szczególnych, wniesienia, do sądu cywilnego, roszczenia o odszkodowanie w związku z naruszeniem zasad wskazanych w RODO skutkujących powstaniem szkody, w przypadku, gdy użycie dronów nie mieści się w zakresie określonym w ustawie o strażach i ustawie o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[37].

10. Podstawowe akty prawne

(1) Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U.1997.78.483 ze zm.);

(2) ustawa z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.);

(3) ustawa z dnia 24 sierpnia 2001 r. - Kodeks postępowania w sprawach o wykroczenia (Dz.U. 2001. 106.1148 ze zm.);

(4) ustawa z dnia 20 maja 1971 r. Kodeks wykroczeń (Dz.U. 1971 nr 12 poz. 114 ze zm.);

(5) ustawa z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego (Dz.U.1997. 88.555 ze zm.);

(6) ustawa z dnia 6 czerwca 1997 r. - Kodeks karny (Dz.U.1997.88.553 ze zm.);

(7) ustawa z dnia 14 grudnia 2012 r. o odpadach (Dz.U. 2013.21ze zm.);

(8) ustawa z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska (Dz.U. 2001.62.627 ze zm.);

(9) 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) (Dz.U.UE.L.2016.119.1);

(10) ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000 ze zm.);

(11) dyrektywa Paramentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowańprzygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U.UE.L.2016.119.89);

(12) ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125);

(13) ustawa z dnia 3 lipca 2002 r. - Prawo lotnicze;

(14) rozporządzenie (WE) NR 785/2004 Parlamentu Europejskiego i Rady z dnia 21 kwietnia 2004 r. w sprawie wymogów ubezpieczeniowych przewoźników lotniczych i operatorów statków powietrznych (Dz.U.UE.L.2004.138.1);

(15) rozporządzenia Wykonawczego Komisji (UE) 2019/945 z dnia 12 marca 2019 r. w sprawie bezzałogowych systemów powietrznych oraz operatorów bezzałogowych systemów powietrznych z państw trzecich (Dz.U.UE.L.2019.152.1);

(16) rozporządzenie Wykonawczego Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych (Dz.U.UE.L.2019.152.45);

(17) rozporządzenie delegowane Komisji (UE) 2020/1058 z dnia 27 kwietnia 2020 r. zmieniające rozporządzenie delegowane (UE) 2019/945 w odniesieniu do wprowadzenia dwóch nowych klas systemów bezzałogowych statków powietrznych (Dz.U.UE.L.2020.232.1);

(18) rozporządzenie wykonawcze Komisji (UE) 2020/639 z dnia 12 maja 2020 r. zmieniające rozporządzenie wykonawcze (UE) 2019/947 w odniesieniu do standardowych scenariuszy operacji wykonywanych w zasięgu wzroku lub poza nią (Tekst mający znaczenie dla EOG) (Dz.U.UE.L.2020.150.1);

(19) rozporządzenie wykonawcze Komisji (UE) 2020/746 z dnia 4 czerwca 2020 r. zmieniające rozporządzenie wykonawcze (UE) 2019/947 w odniesieniu do odroczenia dat rozpoczęcia stosowania niektórych środków w związku z pandemią COVID-19 (Dz.U.UE.L.2020.176.13);

(20) dyrektywa Parlamentu Europejskiego i Rady 2009/48/WE z dnia 18 czerwca 2009 r. w sprawie bezpieczeństwa zabawek (Dz.U.UE.L.2009.170.1).

Ochrona danych osobowych uzyskanych przy wykorzystaniu drona

Autor: mgr inż. Joanna Wieczorek

1. Wprowadzenie

Drony same w sobie nie kreują nowych, nieznanych do tej pory zagadnień prawnych z zakresu ochrony danych osobowych. Ich właściwości powodują jednak, że działalność prowadzona z ich wykorzystaniem jest szczególnie wrażliwa z perspektywy danych osobowych. Drony mogą być bowiem wykorzystywane, celowo lub mimowolnie, do pozyskiwania dużej ilości danych kwalifikowanych jako dane osobowe, bardzo często bez wiedzy podmiotu, którego te dane dotyczą. Ryzyko naruszenia prywatności oraz bezprawnego przetwarzania danych osobowych jest więc w przypadku dronów bardzo wysokie. Należy wskazać, że w dotychczasowym orzecznictwie sądów administracyjnych również specjalnie nie zwracano uwagi na techniczne sposoby gromadzenia danych osobowych (np. w wyniku użytkowania drona, czy przez inne inteligentne urządzenia służące do gromadzenia danych i ich upowszechniania), ale raczej na aspekt ochrony danych osobowych pozyskanych w ten sposób.

Ochrona danych osobowych oparta o przepisy m.in. RODO ma inny charakter niż ochrona prywatności na gruncie przepisów prawa cywilnego. Ta odbywa się bowiem na poziomie administracyjnym, co znaczy, że to państwo czuwa nad tym, aby w zakresie ochrony danych osobowych nie dochodziło do nieprawidłowości. Organem administracyjnym powołanym do tych zadań jest Urząd Ochrony Danych Osobowych i jego naczelny organ (prezes). Zakres ochrony jest jednak bardzo podobny jak w przypadku spraw o naruszenie dóbr osobistych (ochrona danych wrażliwych) w postaci danych wskazujących na pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe. Administracyjnie chroniona jest też informacja o przynależności do związków zawodowych, zdrowiu, seksualności lub orientacji seksualnej. Nikt nie może zatem gromadzić tego typu danych, a jeśli już to robi, to co do zasady musi uzyskać zgodę zainteresowanego (I element), która powinna także obejmować przetwarzanie danych (II element). Należy jednak zaznaczyć, że jeśli osoba, której dane wrażliwe dotyczą, sama je udostępniła publicznie albo wyraźnie udzieliła na to zgody, nie jest objęta ustawową ochroną.

2. Ochrona administracyjna na płaszczyźnie ustawy o ochronie danych osobowych i RODO

Od 25 maja 2018 r. system ochrony danych osobowych w Polsce uległ znaczącej zmianie. Dotychczasowa ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych została w znacznej części zastąpiona przez wchodzące w życie w tym dniu: rozporządzenie 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. UE L119 s.i; dalej: RODO); oraz ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych. Wskazane regulacje prawne nie tworzą jeszcze kompletnego unormowania materii ochrony danych osobowych, ale istotnie dostosowały przepisy z tego obszaru do rozwoju nowych technologii i nałożyły na podmioty przetwarzające dane osobowe nowe obowiązki, które pozwalają lepiej chronić prywatność w świecie nowych technologii. Wynika to z faktu, że ciągle trwają prace nad kolejnymi aktami prawnymi, które wprowadzą pewne zmiany w stosowaniu tych przepisów. Należy wskazać w tym przypadku na już obowiązujące rozporządzenie w sprawie nieuzasadnionego blokowania geograficznego szerzej ujmowanego w ramach inicjatyw unijnych jako Digital Single Market, ale również – obecne cały czas w formie prac koncepcyjnych - rozporządzenie Parlamentu Europejskiego i Rady (UE) w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej, tzw. rozporządzenie e-privacy, które ma być swoistą nadbudową nad RODO w zakresie ochrony użytkowników tzw. urządzeń końcowych, czyli najczęściej komputerów, smartfonów, tabletów i dronów. Z projektu tegoż aktu prawnego, który jak planowano pierwotnie miał wejść w życie również 25 maja 2018 r., wynika m.in., że: ma on mieć zastosowanie nie tylko do osób fizycznych, ale wszystkich kategorii użytkowników; ponadto wprowadzać będzie odmienne aniżeli RODO warunki wyrażania zgód, w szczególności marketingowych na przetwarzanie danych osobowych. Oczekiwanie na uchwalenie i wejście w życie kolejnych dwóch aktów prawnych z zakresu ochrony danych osobowych nie oznacza, że istniejący obecnie system tworzony przez RODO oraz o.d.o. jest niekompletny. Nowe regulacje stanowić bowiem będą przepisy szczególne względem nich w zakresie niektórych branż bądź sposobów przetwarzania danych osobowych. Uznać zatem należy, że ogólny

system ochrony danych osobowych obowiązuje w Polsce w nowym kształcie od 25 maja 2018 r. Niezależnie zatem od planowanego uchwalenia przepisów szczególnych obecnie każdy z administratorów danych osobowych oraz procesorów zobowiązany jest do stosowania zasad wynikających z RODO oraz o.d.o., o ile te akty prawne nie stanowią wprost inaczej.

W o.d.o. nie odniesiono się do prawa do ochrony danych osobowych, nie odwołano się również w tym zakresie do zasad określonych w RODO, zatem przepisy tego drugiego aktu znajdują zastosowanie na warunkach w nim ustalonych przede wszystkim w zakresie związanych z ochroną prywatności w związku z przetwarzaniem danych osobowych. W szczególności obowiązują w zakresie ustalonym w RODO wszystkie główne zasady ochrony danych osobowych (art. 5-10 RODO) oraz uprawnienia osób, których dane dotyczą (art. 12-22 RODO). Przepisy RODO odnoszą się też do szczegółowych przepisów krajowych jako podstaw przetwarzania danych osobowych, dlatego łącznie z RODO znajdą jednak zastosowanie przepisy ustawy o.d.o., w tym art. 5 ust. 2 tej ustawy, ponieważ na podstawie tych przepisów też będzie dochodziło do przetwarzania (udostępniania) danych osobowych. Jednym z określonych w RODO uprawnień jest prawo do sprzeciwu wobec przetwarzania danych osobowych przez administratora (który jak wskazano może być np. operator drona) z przyczyn związanych ze szczególną sytuacją podmiotu danych (art. 21 ust. 1 RODO). Wniesienie sprzeciwu nie oznacza jego automatycznego uwzględnienia, ale istnieje obowiązek rozpatrzenia go przez administratora, co jest następnie kontrolowane przez organ nadzorczy i sąd. Prawo sprzeciwu przysługuje osobie fizycznej, gdy podstawą przetwarzania danych jest wykonanie zadania w interesie publicznym lub w ramach sprawowania władzy publicznej (art. 6 ust. 1 lit. e RODO). W tym kontekście duże znaczenie ma motyw 154 zdanie drugie preambuły RODO, stanowiący, że: „Publiczny dostęp do dokumentów urzędowych można uznać za interes publiczny”. Nie ma więc przeszkód, aby przedmiotem sprzeciwu było ujawnienie danych osobowych w ramach udostępniania informacji publicznej.

W szczególności osoby fizyczne, których dane są ujawniane (jako informacja publiczna), mogą korzystać z uprawnień ustalonych w RODO, w tym uprawnień procesowych: skargi do niezależnego organu nadzorczego (w Polsce jest nim Prezes Urzędu Ochrony Danych

Osobowych - art. 77 RODO) lub powództwa sądowego (art. 79 RODO), jeżeli uznają, że przyznane im w RODO prawa zostały naruszone. Obowiązkiem organu nadzorczego i sądu jest rozpatrzenie wniesionego środka prawnego poprzez rozstrzygnięcie w przedmiocie realizacji praw określonych w RODO. Odpowiedzialność z tytułu naruszenia przepisów RODO przez operatora drona będzie odpowiedzialnością o charakterze administracyjnym.

3. Obowiązki dostawców nowych technologii (technology providers). Zasady privacy by design i privacy by default (art. 25 RODO)

Propozycje ochrony prywatności jakie formułuje Komisja Europejska w swoim prawodawstwie (m.in. projekt rozporządzenia e-privacy) obejmują również katalog obowiązków, które miałyby zostać nałożone wprost na dostawców nowych technologii (SI). Co ciekawe, projektowane przepisy przedmiotowo w dużej części odpowiadają regulacjom, które obecnie można znaleźć w RODO (m.in. w art. 25). Należy jednak przypomnieć, że RODO dotyczy czynności związanych z obsługą samych danych osobowych. Mechanizmy sztucznej inteligencji (systemy SI) nie zawsze jednak wykorzystają tego typu informacje, a zatem w takich przypadkach nie muszą uwzględniać reguł tego rozporządzenia. Podobnie wygląda sytuacja, jeśli spojrzymy na podmioty, na które RODO nakłada określone obowiązki, a mianowicie są to przede wszystkim administratorzy danych. Tymczasem dostawcy technologii zwykle nie występują w tej roli. Dostarczają narzędzie (np. drony), ale sami z niego nie korzystają, nie zawsze mogą też przewidzieć, jak nabywcy danej technologii będą ją wykorzystywać. Stąd m.in. powstają wątpliwości czy dostawca technologii wykorzystującej dane osobowe może w ogóle ponieść odpowiedzialność na gruncie RODO za realizację zasad privacy by design (zasada prywatności w fazie projektowania) jak i będąca jednym z jej elementów idea privacy by default (zasada prywatności w ustawieniach domyślnych). Zgodnie z założeniami privacy by design narzędzia i usługi powinny być tak konstruowane, by od samego początku uwzględniały potrzebę ochrony prywatności obywateli. Perspektywa ta zakłada więc działania o charakterze proaktywnym i prewencyjnym. Producenci nie mają jedynie odpowiadać na pojawiające się problemy techniczne i prawne, ale również je przewidywać. Ochrona prywatności staje się wówczas nie tylko dodatkiem do produktu, ale jego integralną częścią. Rozwinięciem praktycznych aspektów ochrony prywatności w fazie projektowania jest zaś stosowanie oceny skutków projektu dla ochrony prywatności (privacy impact assessment). By przynosiła ona oczekiwane rezultaty, powinna być przeprowadzana, jeszcze zanim dane urządzenia czy systemy zostaną wprowadzone do faktycznego użycia. Ważne jest, by zakres dokonywanej oceny był szeroki i wykraczający poza problemy ściśle prawne oraz by odbywała się ona w sposób

systematyczny.

Wyrażone w art. 25 (oraz w zw. z motywem nr 32 preambuły) RODO zasady privacy by design i privacy by default, konkretyzują zatem zasadę adekwatności zarówno na poziomie technicznym jak i organizacyjnym. Wdrożenie tych zasad do organizacji może polegać na przykład na możliwie szybkim pseudonimowaniu danych, czyli takim ich przetworzeniu, aby nie było możliwe ich przypisanie konkretnej osobie, bez użycia dodatkowych informacji, czy prowadzeniu na bieżąco analizy i zarządzania ryzykiem. Obowiązki dostawców technologii na płaszczyźnie privacy by design, których wprowadzenie postuluje Komisja Europejska w powołanym projekcie rozporządzenia e-privacy, to przede wszystkim:

1) wdrożenie ogólnych zasad projektowania sztucznej inteligencji (rozwiązanie, które obecnie możemy odnaleźć m.in. w wymogach privacy by design i privacy by default w art. 25 RODO);

2) zapewnienie rozliczalności wdrożenia odpowiednich parametrów projektowych systemów sztucznej inteligencji, w tym ujawnianie odpowiednich metadanych (dostawca technologii miałby być w stanie wykazać podjęcie takich działań, podobnie jak ma to miejsce obecnie na gruncie art. 5 ust. 2 RODO);

3) przeprowadzenie oceny możliwych ryzyk związanych ze stosowaniem sztucznej inteligencji oraz podjęcie działań w celu ich minimalizacji (zasada minimalizacji skutków oraz działanie na wzór obowiązku oceny skutków dla ochrony danych z art. 35 RODO);

4) zapewnienie osobom fizycznym wglądu do systemu automatycznego podejmowania decyzji przez sztuczną inteligencję oraz ewentualny przegląd takich decyzji (rozwiązanie zbliżone do obecnego art. 22 RODO).

Projektowane przepisy mają spowodować, że dostawcy technologii będą musieli spełniać niektóre obowiązki „na wzór RODO” (i ponosić za to odpowiedzialność), również jeśli sami nie przetwarzają danych osobowych, a nawet wtedy, gdy tworzone przez nich narzędzia w ogóle nie przewidują takiej możliwości. Nowe obowiązki wymagają również skutecznego systemu ich egzekwowania, w tym nadzoru publicznego. W tym zakresie Komisja Europejska wstępnie zaproponowała jednak

pozostawienie państwom członkowskim wyboru, czy w tym zakresie będą polegać na istniejących już organach administracji, czy też zdecydują się utworzyć nowe organy zajmujące się wyspecjalizowaną kontrolną przestrzegania regulacji dotyczącej sztucznej inteligencji. Na pewno nowym trendem w obszarze RODO i polityki e-privacy będzie wzmocnienie zasady przenoszalności danych, etyki ich wykorzystania oraz ochrony prywatności.

Dokonując analizy rozwoju ochrony prywatności na płaszczyźnie użytkowania dronów z perspektywy szeroko rozumianych działań legislacyjnych (tj. normatywnych i opiniodawczych) podejmowanych w ostatnim czasie przez Komisję Europejską i organy UE jak również mając na uwadze wytyczne Europejskiej Rady Ochrony Danych (a także uprzednie zalecenia Grupy Roboczej ds. Artykułu 29), należy wskazać, że cele te w omawianym przedmiocie nakierowane są głownie na:

- 👎zagwarantowanie łatwej identyfikacji administratorów danych osobowych (np. poprzez obligatoryjne oznaczanie dronów);
- 👎stworzenie bardziej zorganizowanych systemów informacji na temat operatorów dronów operujących na określonym terenie (opinie Grupy Roboczej ds. Art. 29 sugerowały wręcz stworzenie specjalnych platform informacyjnych, które byłyby łatwo dostępne dla podmiotów, których dane byłyby przetwarzane);
- 👎narzucanie producentom dronów konieczności stosowania zasad privacy by design oraz privacy by default, co w praktyce oznacza fabryczne montowanie w dronach oprogramowania, które maskuje oraz anonimizuje zbierane dane osobowe.

4. Monitoring wizyjny a drony. Wytyczne Europejskiej Rady Ochrony Danych

Do czasu wejścia w życie przepisów RODO w obowiązującym stanie prawnym brak było przepisów regulujących w sposób wyczerpujący zagadnienia nagrywania obrazu i dźwięku (czyli tzw. monitoring) przez różnego rodzaju podmioty, np. szpitale, zakłady komunikacji miejskiej, banki, wspólnoty mieszkaniowe, centra handlowe, ale również osoby fizyczne. Co do zasady istniały jedynie szczątkowe regulacje, odnoszące się do wybranych przez ustawodawcę podmiotów, którymi jest on szczególnie zainteresowany czy to z uwagi na kwestie bezpieczeństwa (imprezy masowe), czy interes fiskalny Skarbu Państwa (kasyna). Tymczasem monitorowanie zachowań osób, uzasadniane najczęściej względami bezpieczeństwa, silnie ingeruje w prywatność i jako takie zasługuje na kompleksową regulację. W mojej ocenie brak stosownej ustawy w tak istotnej kwestii jaką stanowiło uregulowanie monitoringu mógł być nawet traktowany jako zaniechanie legislacyjne uniemożliwiające zapewnienie realnego przestrzegania podstawowych praw i wolności konstytucyjnych. Zagadnienia dotyczące monitoringu należy bowiem postrzegać przez pryzmat zapisów Konstytucji o prawie do ochrony danych osobowych (art. 51), ochrony prywatności (art. 47) oraz prawie do tajemnicy komunikowania się (art. 49). Uregulowanie korzystania z praw konstytucyjnych może nastąpić tylko w ustawie i tylko wtedy, gdy jest to konieczne dla bezpieczeństwa demokratycznego państwa lub porządku publicznego, ochrony środowiska, zdrowia i moralności. Choć przepisy RODO nie zawierają rozwiązań prawnych wprost odnoszących się do czynności związanych z nagrywaniem i rejestrowaniem zdarzeń (filmów, dźwięku) z użyciem drona, to – na zasadzie analogii – można je stosować do adeptów tych rozwiązań technicznych. Przede wszystkim niezwykle ważna będzie w tym przypadku wykładnia przepisów RODO dokonywana przez Europejską Radę Ochrony Danych (EROD) w zakresie dotyczącym zasad postępowania z monitoringiem wizyjnym (wytyczne 3/2019).

EROD, jak zawarto w motywach rozporządzenia RODO, jest niezależnym organem Unii Europejskiej, wyposażonym w osobowość prawną i reprezentowaną przez jej przewodniczącego. Od 25 maja 2018 r. jest następcą prawnym i instytucjonalnym tzw. Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych

Osobowych (motyw 139 preambuły RODO). W skład Rady wchodzą szefowie organów nadzorczych wszystkich państw nadzorczych oraz Europejski Inspektor Ochrony Danych lub ich przedstawiciele. Komisja – jak podkreślono – powinna uczestniczyć bez prawa głosu w działaniach Europejskiej Ochrony Danych, a Europejski Inspektor Ochrony Danych bez praw głosu w niektórych sprawach. Zadania EROD określone w art. 70 RODO stanowią rozwinięcie, poszerzenie i uszczegółowienie zadań, które zostały wskazane w art. 30 dyrektywy 95/46/WE w odniesieniu do Grupy Roboczej Art. 29. Analiza kompetencji przyznanych w art. 70 RODO wskazuje, że Rada otrzymała szerokie uprawnienia, w tym w zakresie: monitorowania i zapewniania właściwego stosowania mechanizmu spójności, współpracy z Komisją Europejską, wydawania wytycznych, zaleceń i określania najlepszych praktyk, a także wspierania w opracowywaniu kodeksów postępowania i mechanizmów certyfikacji. Należy dostrzec, że wydawanie jakichkolwiek interpretacji czy zaleceń co do stosowania ogólnego rozporządzenia o ochronie danych (RODO) przez inne instytucje niż EROD oraz krajowe organy nadzorcze (a więc w Polsce przez Prezesa Urzędu Ochrony Danych Osobowych) jest niezgodne z RODO.

5. Nagrywanie

EROD uznaje, że kamery (np. umieszczone na dronach czy odpowiednio w samochodach) wykorzystywane zarówno w celach służbowych jak i prywatnych nie mogą przetwarzać danych osobowych innych uczestników ruchu. Niedozwolone jest też rozpowszechnianie takich nagrań. Rada uważa przy tym, że kamery nie powinny nagrywać obrazu w trybie ciągłym, ujmować osób postronnych znajdujących się w jej perspektywie, a nawet numerów rejestracyjnych innych pojazdów. Jeżeli przedsiębiorca ma uzasadniony interes w monitorowaniu (np. ze względów bezpieczeństwa) - to powinien odpowiednio informować o stosowaniu urządzeń rejestrujących obraz. Przy czym nie wystarczy specjalna plakietka (zawierająca m.in. rysunek kamery), lecz konieczne jest spełnienie obowiązku informacyjnego wynikającego z RODO. Ponadto materiał z monitoringu wideo powinien być kasowany maksymalnie po kilku dniach, a dłuższe przechowywanie dozwolone jest tylko w przypadku, gdy istnieje ku temu uzasadnienie i to na dodatek tylko wybranych zdarzeń, reszta materiału powinna być usunięta (np. właściciel sklepu czy hotelu powinien usunąć nagranie nawet po 24 godzinach chyba, że doszło do incydentu, ale i wówczas można przechowywać dłużej do celów dowodowych tylko wybrane fragmenty nagrania). W praktyce spełnienie wielu wytycznych EROD może być bardzo trudne do wykonania np. spełnienie wyżej sygnalizowanego obowiązku informacyjnego przy filmowaniu z drona. Nie dość, że EROD w swoich wytycznych stwierdził, iż nagrania z kamer nie mogą być nagrywane w trybie ciągłym (a właśnie w takim trybie bardzo często rejestrują materiał obecne na rynku drony), to w dodatku wideo rejestratory nie powinny przetwarzać danych osób fizycznych. Przy takiej interpretacji należałoby zatem wyposażać drony w urządzenia rejestrujące film jedynie z możliwością automatycznej anonimizacji utrwalanych postaci czy danych w postaci np. tablic rejestracyjnych samochodów bądź numerów posesji (urządzenia pikselujace fragmenty obrazu). EROD zwraca także uwagę, że podmioty profesjonalne (przedsiębiorcy) wykorzystujący wideorejestratory powinni spełniać obowiązek informacyjny z art. 13 RODO. Jest to jednak dosyć problematyczne w sytuacji wykorzystywania do nagrywania obrazu z użyciem drona. Spełnienie obowiązku informacyjnego w klasyczny sposób mogłoby stanowić w takim przypadku nie lada wyzwanie: skoro bezzałogowiec porusza się zazwyczaj ze znaczną prędkością to w jaki sposób można by było z technicznej strony wykonać komentowany

obowiązek? Uważam, że najlepszym sposobem spełnienia obowiązku informacyjnego byłoby zatem wyposażenia drona w urządzenie w postaci piktogramu z kamerą. Biorąc pod uwagę wytyczne EROD i wskazany tam obowiązek szybkiego usunięcia zbędnych nagrań wideo oraz obowiązek powstrzymania się od rejestracji wideo w wypadku sprzeciwu osoby, której dane dotyczą, należałoby generalnie zastanowić się nad dopuszczalnością jakichkolwiek nagrań z drona. Nieprawidłowy (tj. naruszający powyższe wymagania) monitoring w perspektywie wykładni przepisów dokonywanych przez EROD i jego polskiego odpowiednika (UODO) może bowiem prowadzić do nałożenia kary administracyjnej. EROD wyjaśniła, że przepisy RODO w zakresie monitoringu wizyjnego nie będą miały zastosowania w sytuacjach, gdy nagranie lub podgląd nie umożliwiają identyfikacji osób w sposób bezpośredni lub pośredni. W RODO zawarte zostało ograniczenie dotyczące prawa dostępu do takich danych. Z art. 15 ust. 4 RODO wynika, że realizacja tego prawa nie może niekorzystnie wpływać na prawa i wolności innych osób. Przenosząc to ograniczenie na dostęp do nagrań z monitoringu wizyjnego, należy uwzględnić to, że nagrania takie zawierają często wizerunek więcej niż jednej osoby (nie tylko tej, która wnosi o dostęp do danych, lecz także osób postronnych, które w tym samym czasie znajdowały się w zasięgu obiektywu). W takim przypadku wydanie nagrania jednej osobie nie powinno naruszać prawa do prywatności pozostałych nagranych. EROD wskazuje, że zastosowanie tej zasady nie powinno być jednak wymówką dla nieuwzględnienia prawa osoby, która zażądała dostępu do danych. W takiej sytuacji rozwiązaniem dla administratora może być zamaskowywanie wizerunków postronnych osób przed wydaniem kopii nagrań wnioskodawcy.

Wykonując loty dronami marki DJI pamiętaj o tym że:

Autor: ppor. mar. Łukasz Grzyb

1.Wszystkie „LOGi” z przebiegu Twojego lotu zapisują się w kilku lokalizacjach:

a. na karcie micro SD;

b. w pamięci urządzenia mobilnego;

c. w pamięci aparatury sterującej;

d. w pamięci nieulotnej drona;

e. w chmurze producenta.

2. Wszystkie „LOGi” zapisywane są od pierwszego uruchomienia i można odtworzyć każdy lot nawet sprzed kilku lat;

3. „LOGi” zapisują się od razu po włączeniu drona;

4. Jeżeli urządzenie mobilne używane do obsługi lotu posiada dostęp do internetu wszystkie dane będą uploadowane do chmury producenta, który posiada dostęp do tych danych.

Przypisy:

(1) Krajowe orzecznictwo rozwija i wyjaśnia instytucję ochrony prywatności jako dobra osobistego każdego człowieka (np. wyrok I ACa 323/12 – analiza zakresu prawa do prywatności, I CSK 557/16 – naruszenie prywatności przez ujawnienie danych ze sfery życia prywatnego).

(2) Także art. 8 Konwencji o ochronie praw człowieka i obywatela

(3) Babcia publikując zdjęcia wnuczka na Facebooku i Pintereście naruszyła przepisy RODO i została zobligowana do usunięcia takich zdjęć pod groźbą grzywny (50 euro kary za każdy dzień zwłoki w usunięciu danych). Obecnie całość wyroku dostępna w języku niderlandzkim:

https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBGEL:2020:2521

(4) W. Szubert, Zarys prawa pracy, Warszawa 1980, s. 90, T. Zieliński, Prawo pracy. Zarys systemu, cz. I, Warszawa 1986 r. , s. 241, wyrok SN z dnia 25 listopada 2005 r., I UK 68/05, Wokanda 2006, nr 4, poz. 26.

(5) J. Stelina, Komentarz do art. 22, w: Kodeks Pracy. Komentarz, wyd. C.H. Beck 2014r., s. 86.

(6) P. Prusinowski, Komentarz do art. 22 KP, w: Kodeks pracy. Komentarz, wyd. ODDK 2016, s. 148-150.

(7) Zob. np. wyrok SN z dnia 19 lutego 1987 r., I PR 6/87, OSN 1988, Nr 4, poz. 52.

(8) Zob. wyr. SN z dnia 4 kwietnia 2006 r., I PK 161/05, Prawo Pracy 2006, Nr 11, s. 33.

(9)Dz.U.UE.L.2019.152.45 - dalej jako rozporządzenie.

(10)Ustawa z dnia 29 sierpnia 1997 r. o strażach gminnych (miejskich) (Dz.U.1997.123.779 ze zm.) – dalej jako straż.

(11)art. 10-11 ustawy o strażach.

(12) Statki eksploatowane lub przeznaczone do eksploatacji bez pilota na pokładzie.

(13) Dalej jako komendant.

(14) art. 10 ust 2a ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (miejskich) (Dz.U.1997.123.779 ze zm.) – dalej jako ustawy o strażach.

(15) Bezzałogowy statek może poruszać się również pod powierzchnią ziemi, na powierzchnią ziemi, pod powierzchnią wody, na powierzchni wody.

(16) art. 2 ust 1 ustawy z dnia 3 lipca 2002 r. Prawo lotnicze (Dz.U. 2002.130.1112 ze zm.).

(17) art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125) - dalej jako dodo

(18) Dz. U. 2019.125

(19) Dz.U.UE.L.2016.119.1 (dalej jako rodo)

(20) Dz.U.UE.L.2019.152.45

(21) Dz.U. 2001.106.1148 ze zm.

(22) Dz.U. 1971.12.114 ze zm. (dalej jako kodeks wykroczeń)

(23) Dz.U.2019.125

(24)Dane osobowe to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

(25) Lot w określonym celu po spełnieniu wymagań prawnych.

(26) Straże winny prowadzić cykliczne oceny pod kątem skuteczności prowadzonych obserwacji, w celu wykazania niezbędności ich realizowania z wykorzystaniem dronów.

(27) Dowolna osoba prawna lub fizyczna eksploatująca lub zamierzająca eksploatować co najmniej jeden bezzałogowy system powietrzny. W skład bezzałogowego systemu wchodzi bezzałogowy statek i wyposażenie do zdalnego sterowania nim.

(28)Osoba fizyczna odpowiedzialna za bezpieczne wykonanie operacji dronem.

(29) Dz.U. 2001.62.627 ze zm.

(30) Dz.U.1997.88.553 ze zm.

(31) Dz.U. 1964.16.93 ze zm.

(32) Dz.U.1997. 88.555 ze zm.

(33) Dz.U. 2001.112.1198 ze zm.

(34) Dz.U. 1964.16.93 ze zm.

(35)Także Burmistrza lub Prezydenta miasta

(36) Szerz. uchwała 7 sędziów SN z dnia 24 października 2014 r., sygn. akt I KZP 24/12 oraz uchwała SN z dnia 11 czerwca 2019 r., syg. akt I DO 11/19

(37) Działanie straży poza, wyznaczonym przez ustawodawcę, zakresem kompetencji stanowić może, z punktu widzenia osoby, której dane dotyczą, naruszenie RODO. Należy jednak odróżnić taką sytuację od przypadku, gdy straż podejmując, z użyciem drona, działania mieszczące się w ramach swoich uprawnień naruszy warunki ich realizacji. Tylko działanie obejmujące używanie dronów, oczywiście niemające związku z uprawnieniami straży, co wobec prób włączania straży w realizację ogólnych zadań samorządu terytorialnego nie jest wykluczone (choć oczywiście jest co do zasady bezprawne), może generować tego typu skutek.