

RODOmagazyn

NR 21 | grudzień 2021 / styczeń 2022

**DONOS POD OCHRONĄ PRAWA?
NOWE OBOWIĄZKI SEKTORA
PRYWATNEGO I PUBLICZNEGO**

ILE WIE O NAS POLICJA?

**JAK MOŻNA STRACIĆ KLIENTÓW
PRZEZ DANE NA NASZ TEMAT,
KTÓRE PRZETWARZA POLICJA?**

**JAK POKONAĆ BARIERY
WSPÓŁPRACY ADMINISTRACJI?
EUROPEJSKA STRATEGIA
INTEROPERACYJNOŚCI**

**RODO 2021
POLSKA I EUROPA
RAPORT**

Wydawca:

Rzetelna Grupa sp. z o.o.
al. Jana Pawła II 61 lok. 212
01-031 Warszawa

Sąd Rejonowy dla m. st. Warszawy I XIII Wydział Gospodarczy I KRS 0000284065 NIP: 524-261-19-51
REGON: 141022624 Kapitał zakładowy: 50.000 złotych.

ISSN 2544-8897

Numer wpisu do sądowego Rejestru dzienników i czasopism PR20362

Redaktor Naczelny: Rafał Stępniewski

Redakcja i korekta: Monika Świetlińska

Projekt i skład: Monika Świetlińska

Wszelkie prawa zastrzeżone.

Publikacja w całości jak i każdy jej fragment nie mogą być powielane ani rozpowszechniane w żadnej formie i w żaden sposób bez uprzedniego pisemnego zezwolenia Rzetelna Grupa sp. z o.o. z siedzibą w Warszawie. Wszelkie znaki towarowe, nazwy własne, logotypy oraz znaki graficzne i inne treści są chronione prawem autorskim i stanowią własność Rzetelna Grupa sp. z o.o. z siedzibą w Warszawie.

Spis treści:

Donos pod ochroną prawa? Nowe obowiązki sektora prywatnego i publicznego	5
Ile wie o nas Policja?	12
Jak można stracić klientów przez dane na nasz temat, które przetwarza Policja?	18
Jak pokonać bariery współpracy administracji? Europejska Strategia Interoperacyjności	23
RODO 2021 – Polska i Europa. RAPORT	27
O redakcji	31



Drogi Czytelniku,

w Twoje ręce oddajemy grudniowe wydanie "RODOmagazyn". Mamy nadzieję, że sprostaliśmy Twoim oczekiwaniom i tematy, które poruszamy na łamach pisma będą dla Ciebie ciekawą lekturą.

Numer otwiera materiał poświęcony sygnalistom. Czy Twój podmiot musi wcielić je w życie? Co jeśli tego nie zrobi? Jak do zmian przygotowuje się polski ustawodawca?

Od 2 lat stale wprowadzane są poprawki do Ustawy o Policji. Czy wiesz, ile wiedzą o Tobie mundurowi? Które z Twoich danych mogą przetwarzać i w jakich sytuacjach? Przygotowaliśmy przegląd systemów i narzędzi, jakich używa Policja do przetwarzania danych.

Pokażemy Ci przykład przedsiębiorcy, który przez przetwarzanie danych przez Policję, a dotyczących jego samego, stracił klientów. Czy to w ogóle możliwe? Co na ten temat miał do powiedzenia prezes Urzędu Ochrony Danych Osobowych, a co administrator danych? Czy roszczenia przedsiębiorcy były słuszne?

Zostając przy temacie systemów informacyjnych odpowiadających za przetwarzanie danych osobowych, przyjrzelśmy się, na jakim etapie jest wdrażanie ram interoperacyjności. Jak kraje UE współpracują ze sobą, by poprawić skuteczność i wydajność kontroli granicznych na granicach zewnętrznych, zapobiegać nielegalnej imigracji oraz zapewnić wysoki poziom bezpieczeństwa w ramach przestrzeni wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej.

Przygotowaliśmy również raport dotyczący kar RODO w Polsce i w Europie oraz trwających w 2021 roku prac nad prawem chroniącym nasze dane osobowe. Polecamy!

Czy moja firma musi zarejestrować się w BDO?

Obowiązek zarejestrowania się do BDO jest konsekwencją wejścia przepisów dotyczących Rejestru podmiotów wprowadzających produkty, produkty w opakowaniach i gospodarujących odpadami.

Czy muszę się rejestrować?

- jeżeli prowadzisz sklep internetowy
- jeżeli sprowadzasz do Polski baterie, sprzęt elektryczny lub elektroniczny
- jeżeli na skutek Twojej działalności wytwarzane są odpady

Podlegasz pod rejestrację w BDO

Sprawozdawczość

Pomożemy Ci przygotować raporty i sprawozdania do BDO. Możemy to wykonywać za Ciebie przejmując jednocześnie całą komunikację z odpowiednim urzędem.

Szkolenia dla pracowników

Przeszkolimy Twoich pracowników w zakresie BDO. Wiedza z webinarów i e-learningu pozwoli im sprawnie obsługiwać proces i rozwiązywać problematyczne sytuacje mogące wystąpić w trakcie obsługi systemu BDO.



Zapytaj o ofertę



Rzetelny[®]
Regulamin

Donos pod ochroną prawa? Nowe obowiązki sektora prywatnego i publicznego



17 grudnia 2021 – to termin wdrożenia procedur ochronnych sygnalistów przez podmioty z sektora publicznego i większe przedsiębiorstwa. Obowiązek ten wynika z wprowadzenia Dyrektywy Parlamentu Europejskiego i Rady (UE). Co to oznacza dla pracodawcy, a co dla pracownika? Czy każdy musi zgłaszać naruszenia europejskiego prawa w firmie i podmiotach publicznych? Jak wygląda ochrona tożsamości sygnalisty?

Przed czym ma chronić dyrektywa?

Nowe europejskie rozporządzenie dotyczy w tym momencie większych przedsiębiorstw i podmiotów publicznych, ale dokładnie za dwa lata dotyczyć będzie również firm, zatrudniających od 50 do 249 pracowników.

Obecne regulacje dotyczące ochrony sygnalistów nie są wystarczające, stąd nowa Dyrektywa o ochronie sygnalistów w zamierzeniu ma chronić ich przed konsekwencjami takimi jak:

- zwolnienie z pracy,
- degradacja,
- przymusowy bezpłatny urlop,
- zmiana miejsca pracy,

- obniżenie wynagrodzenia,
- wstrzymanie szkoleń,
- zastosowanie jeszcze innego środka dyscyplinarnego.

Istotną częścią nowego prawa ma być również zapewnienie ochrony tożsamości sygnalisty.

Zarówno po dokonaniu samego zgłoszenia, jak i w trakcie toczącego się postępowania, będącym konsekwencją przekazania informacji o naruszeniu unijnego prawa.

Ważna będzie też tymczasowa ochrona prawną, gdy sprawa trafi do sądu. Wszystko po to, by zapobiec ewentualnym groźbom i próbom podjęcia działań odwetowych ze strony pracodawcy.

Donos pod ochroną prawa? Nowe obowiązki sektora prywatnego i publicznego

Sygnalista. Kim jest? Kto i kiedy staje się sygnalistą?

Każdy, kto choć raz dowiedział się o jakichkolwiek naruszeniach europejskiego prawa w firmie i poinformował o tym właściciela lub odpowiednie organy, stał się sygnalistą. W związku z tym podlega pod nowe rozwiązania prawne.

Sygnalista (z ang. whistleblower) jest osobą, która ze względu na to, jakie posiada informacje, zgłasza zauważone nieprawidłowości u swojego pracodawcy. Status ten zyska każdy, kto dokona zgłoszenia różnego rodzaju przekroczeń prawa, które powinny mieć oparcie w faktach.

W interesie publicznym jest, aby w odpowiedni sposób identyfikować i wykrywać takie zachowania, a także przeciwdziałać im w przyszłości. Nieprawidłowości można zgłosić bezpośrednio do swojego pracodawcy albo do organów ścigania.

Aby osobę można było uznać za sygnalistę musi spełnić wszystkie powyższe warunki:

1. posiada ważne w jej rozumieniu informacje, które są dowodem zaistnienia nieprawidłowości związanych z funkcjonowaniem przedsiębiorstwa czy instytucji publicznych
2. jej informacje muszą być oparte na faktach wskazujących, że mogło dojść do powstania nieprawidłowości i mogły zostać naruszone przepisy prawa
3. musi chcieć zgłosić problem i podjąć w tym celu konkretne działania
4. zgłoszenia musi dokonać w dobrej wierze, a co za tym idzie zgłoszenie to służy ważnym celom publicznym, nie jest próbą zemsty czy wyrządzenia krzywdy.

Sygnalista jest anonimową osobą. Może nim być: pracownik, samozatrudniony współpracownik, wspólnik,



Donos pod ochroną prawa? Nowe obowiązki sektora prywatnego i publicznego



stażysta, wykonawca, podwykonawca, dostawca, były pracownik, osoba w trakcie rekrutacji.

Zgłoszenia naruszenia mogą dotyczyć:

- zamówień publicznych,
- usług,
- produktów,
- rynków finansowych,
- zapobiegania praniu pieniędzy
- finansowaniu terroryzmu,
- bezpieczeństwa produktów i ich zgodności z wymogami,
- bezpieczeństwa transportu,
- ochrony środowiska,
- ochrony radiologicznej i bezpieczeństwa jądrowego,
- bezpieczeństwa żywności i pasz,
- zdrowia i dobrostanu zwierząt,
- zdrowia publicznego,
- ochrony konsumentów,
- ochrony prywatności i danych osobowych
- bezpieczeństwa sieci i systemów informacyjnych.

Jak podaje art. 2 ust. 2 Dyrektywy kraje członkowskie mogą rozszerzyć wymieniony zakres naruszeń. Sytuacja taka może się dotyczyć tych dziedzin, które nie są wymienione w Dyrektywie Parlamentu Europejskiego i Rady (UE).

Obowiązki pracodawcy względem sygnalisty

Taka osoba w firmie nie ponosi odpowiedzialności za złamanie obowiązku poufności czy naruszenia tajemnicy przedsiębiorstwa. Od 17 grudnia 2021 roku, po wdrożeniu w życie Dyrektywy do polskiego porządku prawnego, sygnaliści zobowiązani są do składania zgłoszeń za pomocą utworzonych przez pracodawców kanałów informacyjnych.

Przypomnijmy, że pracodawca musi chronić tożsamość i interesy sygnalisty. A dotyczy to sytuacji zarówno po dokonaniu samego zgłoszenia, jak i w trakcie toczącego się postępowania, które może się rozpocząć od złożenia informacji o naruszeniu unijnego prawa.

Donos pod ochroną prawa? Nowe obowiązki sektora prywatnego i publicznego

Osoby odpowiedzialne za weryfikację zgłoszeń sygnalistów

W podmiocie musi być wyznaczona osoba odpowiedzialna za podejmowanie działań wyjaśniających oraz przekazywanie sygnaliście informacji zwrotnych. Nie tylko na temat podjętych w związku z nim działaniach, ale np. o przyjęciu zgłoszenia. Taka osoba będzie miała na to 7 dni.

Przygotowania na nową dyrektywę

W ramach Dyrektywy PE i Rady 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii, na państwa członkowskie został nałożony obowiązek jej wdrożenia. Przy czym ten akt prawny odnosi się jedynie do ogólnych warunków, jakie trzeba spełnić w celu zapewnienia ochrony sygnalistom.

W dokumencie nie ma mowy o konkretnych działaniach. Szczegółowe narzędzia może wdrożyć krajowy ustawodawca, chociaż niekoniecznie tak musi być. Dlatego na przedsiębiorcy będzie spoczywać obowiązek wdrożenia takich rozwiązań, które będą spójne z unijnymi wytycznymi.

Na podstawie samej dyrektywy można wskazać kluczowe i zarazem minimalne wymogi, tj. tworzenie odpowiednich kanałów i regulacji, procedur umożliwiających swobodne zgłaszanie naruszeń oraz zapewnienie ochrony sygnaliście. Kanały te muszą być poufne i bezpieczne, a pracownicy muszą być przez pracodawcę poinformowani o ich wdrożeniu. Takim wewnętrznym kanałem zgłoszeniowym może być np. dedykowana infolinia, formularz na stronie www czy skrzynka na pisemne zgłoszenia.

Sankcje za brak wdrożonych narzędzi

Termin na wdrożenie unijnej dyrektywy upływa:

- 17 grudnia 2021 r. dla podmiotów publicznych (wdrożenie kanałów wewnętrznych i zewnętrznych). Polska, w przepisach krajowych, może podjąć decyzję o zwolnieniu z tego obowiązku gminy mającej mniej niż 10 000 mieszkańców lub zatrudniających mniej niż 50 pracowników;
- 17 grudnia 2021 r. dla podmiotów prywatnych zatrudniających powyżej 249 pracowników;
- 17 grudnia 2023 r. dla podmiotów prywatnych zatrudniających od 50 do 249 pracowników.

Za niedopełnienie tego obowiązku grożą sankcje. Jakże konkretnie? Na razie nie wiemy. Wiemy tyle, że mają być skuteczne, proporcjonalne i odstraszające. Ich zakres oraz wysokość pozostawiono krajom członkowskim. O tym w dalszej części.

Dyrektywa o sygnalistach w Polsce

18 października 2021 w wykazie prac legislacyjnych pojawił się Projekt ustawy o ochronie osób zgłaszających naruszenia prawa na wniosek Ministra Rodziny i Polityki Społecznej.

Planowany termin przyjęcia projektu przez Radę Ministrów to czwarty kwartał 2021 roku i póki co od tamtej pory nie przeprowadzono dalszych czynności. 18 października projekt został skierowany do opiniowania. Kolejne etapy legislacyjne to zewnętrzna konferencja uzgodnieniowa, skierowanie i przyjęcie przez Radę do Spraw Cyfryzacji, skierowanie i przyjęcie przez Krajową Radę Ministrów, skierowanie i przyjęcie przez Komitet do Spraw Europejskich, rozpatrzenie przez komisję prawniczą i na koniec przyjęcie przez Radę Ministrów.

Donos pod ochroną prawa? Nowe obowiązki sektora prywatnego i publicznego

Żadne nie zostały jeszcze zrealizowane. Można więc przypuszczać, że albo intensywne prace ruszą tuż przed 17 grudnia albo ustawa nie wejdzie w życie w terminie wskazanym w Dyrektywie.

Projektowana ustawa ma zapewnić wdrożenie wymaganych Dyrektyw środków ochrony osób zgłaszających oraz osób, których dotyczy zgłoszenie, jak również związanych ze zgłaszaniem rozwiązań organizacyjnych i instytucjonalnych. Co ciekawe, dopiero ta ustawa wprowadzi definicję ustawową określenia "sygnalista".

"Nie istnieją odrębne regulacje na gruncie prawa pracy, które bezpośrednio odnoszą się do sygnalizowania i specyficznie kształtowały sytuację prawną sygnalisty w związku z dokonaniem zgłoszenia lub ujawnieniem" - czytamy w uzasadnieniu projektu ustawy. Podobnie jest w przypadku przepisów procedury karnej lub administracyjnej.

W aktualnym stanie prawnym w Polsce tzw. sygnalizowanie i ochrona osób odpowiadających przytoczonemu wyżej rozumieniu sygnalisty w praktyce podlega przede wszystkim odpowiednim przepisom o powszechnym zakresie zastosowania.

Uzasadnienie wskazuje szereg rozwiązań prawnych, które można zastosować przy sygnalizowaniu,

np. kodeks pracy, gdzie mowa o niedyskryminowaniu w zatrudnieniu, naruszeniu zasady równego traktowania czy przeciwdziałaniu dyskryminacji, mobbingu. Dla przykładu, zgodnie z Kodeksem pracy osoba, wobec której pracodawca naruszył zasadę równego traktowania w zatrudnieniu, ma prawo do odszkodowania w wysokości nie niższej niż minimalne wynagrodzenie za pracę, ustalone na podstawie odrębnych przepisów.

Pracodawca jest także obowiązany przeciwdziałać mobbingowi (art. 943 Kodeksu pracy). Takie działanie pracodawcy jest niezależne od przyczyn, które wywołały mobbing. Dotyczy to więc także mobbingu, który mógłby zaistnieć lub zaistniał wskutek dokonania przez pracownika zgłoszenia lub ujawnienia.

W ramach procedury karnej możliwa jest ochrona świadków w postępowaniu karnym (instytucja świadka anonimowego) czy zapewnienie możliwości anonimowego przekazania zawiadomienia o przestępstwie organom ścigania. Zastosowanie może tu mieć ustawa o ochronie i pomocy dla pokrzywdzonego i świadka. Ponadto według Kodeksu karnego, karze podlega złośliwe lub uporczywe naruszenie prawa pracownika wynikającego ze stosunku pracy lub ubezpieczenia społecznego (zagrożone karą grzywny, ograniczenia wolności albo pozbawienia wolności do lat dwóch) oraz



Donos pod ochroną prawa? Nowe obowiązki sektora prywatnego i publicznego

odmowa ponownego przyjęcia do pracy, o której przywróceniu orzekł właściwy organ.

Sygnalista w Polsce jest też chroniony przepisami Prawa prasowego gwarantującymi swobodę wypowiedzi i wolność prasy, wraz z przewidzianymi w nich gwarancjami ochrony źródeł informacji.

Co ważne, wszystkie powyższe instytucje prawne, jakkolwiek zmierzają bądź do zapewnienia możliwości zgłaszania lub ujawniania nieprawidłowości, bądź służą ochronie osób, które o takich nieprawidłowościach informują, nie są, jako takie, środkami ochrony sygnalistów, których wdrożenia wymaga dyrektywa 2019/1937. Najczęściej nie są też powszechnie uznawane za środki ochrony sygnalistów w ścisłym znaczeniu.

W ostatnich latach utworzono organy, które przeciwdziałają naruszeniom, na przykład, Centralne Biuro Antykorupcyjne czy Urząd Ochrony Konkurencji i Konsumentów (Program dla sygnalistów UOKiK). Związane są one w pierwszym rzędzie z ułatwieniem sygnalizowania (zgłaszania) jako mechanizmu przekazywania informacji i funkcjonują w obowiązujących już ramach prawnych, tj. nie ustanawiają szczególnych środków ochrony, w tym przed nieuzasadnionym niekorzystnym traktowaniem w środowisku pracy. W praktyce, przy braku powszechnych regulacji służących ochronie zgłaszających, środkiem ochrony w ramach takich rozwiązań są przede wszystkim zaoferowane zgłaszającemu określone gwarancje anonimowości bądź poufności.

Rozwiązania ustawy nie modyfikują obowiązujących przepisów ogólnie mogących służyć ochronie osób zgłaszających naruszenia prawa.

Istotą projektowanych rozwiązań jest uzupełnienie istniejących przepisów o środki ochrony związane ze zgłaszaniem lub ujawnianiem naruszeń w trybie przewidzianym w ustawie. Ustanowione są też kanały dokonywania zgłoszeń wewnętrznych i zewnętrznych o naruszeniach, wraz z określeniem zasad ich funkcjonowania, oraz określone zostaną zasady dokonywania ujawnienia publicznego.



OBSŁUGA PRAWNA

E-COMMERCE

CERTYFIKACJA SKLEPÓW

REGULAMINY, RODO, BDO

SYSTEM OPINII KONSUMENCKICH

www.rzetelnyregulamin.pl

Ile wie o nas Policja?

Katalog uprawnień Policji określa Ustawa o Policji z dnia 6 kwietnia 1990 r. o Rozdział 3. Zakres uprawnień Policji. Zgodnie z ustawą Policja w celu realizacji zadań może korzystać z danych o osobie. Mowa nie tylko o danych zebranych przez nią samą, ale też o danych uzyskanych przez inne organy, służby i instytucje państwowe w wyniku wykonywania czynności operacyjno-rozpoznawczych oraz przetwarzać je bez wiedzy i zgody osoby, której dane te dotyczą.

Uprawnienia Policji

Przyjrzyjmy się, co mówi ta część **Ustawy o Policji**, która traktuje o zakresie uprawnień Policji. Kluczowe informacje zawierają się w art. 14.4: "Policja w celu realizacji ustawowych zadań może korzystać z danych o osobie, w tym również w formie zapisu elektronicznego, uzyskanych przez inne organy, służby i instytucje państwowe w wyniku wykonywania czynności operacyjno-rozpoznawczych oraz przetwarzać je w rozumieniu 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), bez wiedzy i zgody osoby, której dane te dotyczą."

Kolejnym ważnym aspektem jest to, że administrator danych, o których mowa we wcześniejszym ustępie, ma obowiązek udostępnić dane osobowe policjantowi wskazanemu w upoważnieniu Komendanta Głównego Policji, Komendanta CBŚP, Komendanta BSWP, komendantów wojewódzkich Policji lub uprawnionego policjanta, po okazaniu tego upoważnienia oraz legitymacji służbowej. Fakt udostępnienia tych danych podlega ochronie na podstawie ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

Ponadto Policja może, w zakresie koniecznym do wykonywania jej ustawowych zadań, korzystać z informacji kryminalnej zgromadzonej w Krajowym Centrum Informacji Kryminalnych.



Ile wie o nas Policja?

W celu wykonywania zadań w zakresie kontroli ruchu drogowego, o których mowa w "Prawie o ruchu drogowym" – może prowadzić wyszukiwania informacji za pośrednictwem Krajowego Punktu Kontaktowego.

W ramach wykonywanych czynności czy obowiązków policjanci mają prawo nawet do tego, by pobierać od osób odcisków linii papilarnych lub wymazu ze śluzówki policzków (w trybie i przypadkach określonych w przepisach Kodeksu postępowania karnego oraz ustawy z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób.

Mogą to zrobić celem identyfikacji osób o nieustalonej tożsamości oraz osób usiłujących ukryć swoją tożsamość, jeżeli ustalenie tożsamości w inny sposób nie jest możliwe.

Źródła danych

Oczywiście Ustawa o Policji nie jest jedynym aktem prawnym, który reguluje zasady pozyskiwania i przetwarzania danych osobowych. Są to również: kodeksy karny i wykroczeń czy kodeksy postępowania karnego i w sprawach o wykroczenie. Co istotne Policja jest w posiadaniu dokumentacji, która szczegółowo opisuje sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Dokumentacja ta zawiera wyszczególnione akty prawne pozwalające na przetwarzanie tych danych osobowych.

Policjanci przechowują dane obywateli zawarte zarówno w zbiorach nieautomatyzowanych – manualnych, tradycyjnych, czyli w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych (zbiory zautomatyzowane). Zbiorami danych są zatem wszelkie materiały gromadzone w formie akt, w tym również sądo-



Ile wie o nas Policja?

we, prokuratorskie, policyjne i inne zawierające dane osobowe. Zbiorami danych są też informacje wprowadzane i wykorzystywane w systemach informatycznych. System informatyczny to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Dane osobowe i dane wrażliwe

Dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. A osobą możliwą do zidentyfikowania jest ta osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny, albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Co ważne, informacji nie uważa się za umożliwiającą określenie tożsamości osoby,

jeżeli wymagałoby to nadmiernych kosztów, czasu czy działań.

Dane osobowe są podzielone na dwie kategorie: takie, które pozwalają na określenie tożsamości konkretnej osoby oraz takie, które nie pozwalają na jej natychmiastową identyfikację, ale są, przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia.

Policja zwraca uwagę na szczególną kategorię danych osobowych zwanych danymi wrażliwymi, sensytywnymi czy po prostu szczególnie chronionymi. Są to informacje o:

- pochodzeniu rasowym,
- pochodzeniu etnicznym,
- poglądach politycznych, religijnych, filozoficznych,
- wyznaniu,
- przynależności partyjnej lub związkowej,
- dane o stanie zdrowia,
- kodzie genetycznym,
- nałogach,
- życiu seksualnym,
- dane dotyczące skazań,
- oraz orzeczeń o ukaraniu i mandatów karnych.

Prawa osoby, której dane dotyczą

Każdy funkcjonariusz wie, jakie prawa przysługują każdej osobie, której dane dotyczą. Są to:

- uzyskania wyczerpującej informacji, czy taki zbiór istnieje oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy,
- uzyskania informacji o celu, zakresie i sposobie przetwarzania danych,
- uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące oraz podania w zrozumiałej formie treści tych danych,



Ile wie o nas Policja?

- uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące,
- uzyskania informacji o sposobie udostępniania danych i o odbiorcach tych danych,
- żądania uzupełnienia, uaktualnienia, sprostowania lub wstrzymania (czasowego lub stałego) przetwarzania danych, jeśli są one niekompletne, nieaktualne, nieprawdziwe, zebrane z naruszeniem ustawy, albo stały się zbędne.

Policja ma obowiązek zgłoszenia zbioru danych do rejestracji organowi nadzorczemu.

Z obowiązku tego są zwolnieni m.in. administratorzy danych, które zostały uzyskane w wyniku:

- czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności
- przetwarzanych przez właściwe organy na potrzeby udziału RP w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym
- przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się.

Bazy danych, z których korzysta Policja

Działanie Policji opiera się na szybkim gromadzeniu, analizie i wykorzystywaniu informacji. Powstają kolejne międzynarodowe i ogólnopolskie bazy danych ułatwiające prowadzenie śledztw, poszukiwania niebezpiecznych przestępców, zdalne sprawdzanie wiarygodności ludzi i dokumentów itp.

Policja, co zostało już wspomniane, korzysta między innymi ze zautomatyzowanych systemów informatycznych.

Wśród krajowych baz danych i systemów informatycznych wykorzystywanych przez Policję znajdują się:



Ile wie o nas Policja?

Krajowy System Informacyjny Policji (KSIP) to centralny system informatyczny Policji, wdrożonym na początku 2003 roku, który stanowi fundament wszystkich systemów informatycznych Policji. Może współdziałać z innymi, udostępnionymi Policji bazami danych. System ten funkcjonuje w Policyjnej Sieci Transmisji Danych (PSTD) wydzielonej siecią nieposiadającą styku m.in. z internetem. Dostęp do niego odbywa się za pomocą komputerów podłączonych do PSTD wyposażonych w zabezpieczenie sprzętowe identyfikujące użytkownika.

KSIP to łącznik patroli, wyposażonych w komputery naręczne, podczas kontroli policyjnych. W ciągu kilku minut dzięki temu narzędziu policjanci otrzymują informacje m.in. o osobach i ich danych. Istotną cechą systemu jest jego bezpieczeństwo, rozumiane, jako kontrola dostępu do określonych funkcji lub danych, lub do pewnych rodzajów informacji zawartych w bazie danych. Działa on w zgodzie ze wszystkimi przepisami dotyczącymi dostępu do danych i bezpieczeństwa obowiązującymi w Polsce i w Unii Europejskiej.

System Wspomagania Dowodzenia Policji do użytkowania w Komendzie Głównej Policji, komendach wojewódzkich, Komendzie Stołecznej Policji, komendach powiatowych i miejskich, a także w niektórych komisariatach. To centralny system teleinformatyczny, który działa na poziomach: powiatowym, wojewódzkim i centralnym.

System ten ma kilka podstawowych funkcjonalności, a wśród nich zarządzanie informacją, tj. możliwość sprawdzenia jej w Krajowym Systemie Informacyjnym Policji (KSIP) przez System Poszukiwawczy Policji (SPP) czy komunikaty.

System Poszukiwawczy Policji (SPP) – system informatyczny, który łączy wszystkie zapytania kierowane do systemów informatycznych – zarówno Policji, jak i wielu zewnętrznych. Podstawowe obszary informacji, które obsługuje SPP, to dane o osobach i pojazdach. Pytania zadawane w SPP kierowane są do takich aplikacji, jak Krajowy System Informacyjny Policji, Schengen Information System, Visa Information System, Centralna Ewidencja Ludności, Centralna Ewidencja Pojazdów i Kierowców, Straży Granicznej, więziennictwa oraz REGON.

Cel SPP to umożliwienie bezpośredniego i sprawnego dostępu funkcjonariuszom do niezbędnego zakresu informacji zawartych w wielu systemach policyjnych i poza-policyjnych. SPP daje możliwość uzyskiwania z nich jednej zbiorczej odpowiedzi.

Krajowe Centrum Informacji Kryminalnych (KCİK) to centralny, ogólnokrajowy rejestr wszystkich danych, jakie mogą być niezbędne instytucjom pilnującym przestrzegania prawa. Jego kluczowym zadaniem jest gromadzenie i przekazywanie instytucjom zwalczającym przestępczość pełnych i bieżących informacji, które przyczyniają się do wykrywania i ścigania przestępstw, a także ich zapobiegania.

KCİK umożliwia błyskawiczną wymianę informacji, dzięki czemu prokuratury: powszechna i woj-skowa, Policja, Straż Graniczna, Inspekcja Celna, organy podatkowe, celne skuteczniej realizują wyznaczone im cele.

Policyjny Rejestr Imprez Masowych (PRIM) jest narzędziem wspomagającym realizowanie zadań powiązanych z przetwarzaniem oraz usystematyzowaniem informacji związanych

Ile wie o nas Policja?



z szeroko rozumianym bezpieczeństwem masowych imprez sportowych. PRIM to wzajemnie powiązane bazy danych m.in. o: klubach, organizacjach, stowarzyszeniach skupiających kibiców, o chuligańskich zachowaniach, związkach i klubach sportowych, organizatorach masowych imprez sportowych. Funkcjonuje jako wyodrębniony moduł Krajowego Systemu Informacyjnego Policji.

Na potrzeby Policji funkcjonuje jeszcze **System Informacji Operacyjnych (SIO)** przeznaczony dla służb: kryminalnej i śledczej m.in. do gromadzenia informacji ważnych dla wykonywania czynności operacyjno-rozpoznawczych. Przetwarzane są tu informacje przydatne do zapobiegania, rozpoznawania, ujawniania i wykrywania przestępstw, ustalania metod ich popełniania oraz wykrywania i zatrzymywania sprawców. SIO składa się z: **Systemu Meldunku Informacyjnego (SMI)** i **Centralnej Bazy Informacji z Ustaleń (CBIU)**.

Meldunek informacyjny tworzy się w każdym przypadku uzyskania przez policjantów ważnych informacji i ustalania metod ich popełniania, a także wykrywania i zatrzymywania sprawców, w tym m.in. informacji o dokumentach, osobach fizycznych i innych podmiotach nie będących osobami fizycznymi.

Z kolei w **Centralnej Bazie Informacji z Ustaleń (CBIU)** gromadzi się i przetwarza informacje zawarte w dokumencie stanowiącym podstawę do prowadzenia obserwacji oraz informacje uzyskane przez policjantów komórek organizacyjnych właściwych w sprawach techniki operacyjnej w ramach prowadzonych obserwacji, zleconych przez jednostki organizacyjne Policji lub ich komórki prowadzące czynności operacyjno-rozpoznawcze.

Policja włączona jest też w **europejski i światowy system** zwalczania przestępczości. Skuteczność funkcjonowania międzynarodowych organizacji zależy m.in. od systemów informatycznych. Są to głównie: System Informacyjny Schengen, Wizowy System Informacyjny, System łączności Interpolu I-24/7, System informacyjny Europolu.

Jak można stracić klientów przez dane na nasz temat, które przetwarza Policja?

Policja ma prawo do przetwarzania danych osobowych każdego obywatela. Skargi na nieprawidłowości w procesie przetwarzania jego danych do Urzędu Ochrony Danych Osobowych zdarzają się dość często. Jednak w zdecydowanej większości przypadków Prezes UODO odmawia ich uwzględnienia. Wachlarz uprawnień Policji jest na tyle szeroki, że nawet utrata klientów przez obywatela (przedsiębiorcę, menedżera, handlowca), która była wynikiem przetwarzania danych w ich obecności, nie jest powodem, dla którego Policja miałaby usuwać jego dane z Krajowego Systemu Informacyjnego Policji (KSIP) oraz w Krajowego Centrum Informacji Kryminalnych (KCIK).

Urząd Ochrony Danych Osobowych publikuje wydane decyzje wniosków, jakie składają skarżący i bardzo często są to sprawy związane z przetwarzaniem danych osobowych przez Policję. Są przypadki, że przetwarzanie to wiąże się z różnymi skutkami dla obywateli.

W przypadku przedsiębiorcy L. M., zamieszkałego w miejscowości S. skończyło się nie tylko na odmowie uwzględnienia skargi przez prezesa UODO i komendanta właściwej jednostki Policji, ale także utracie klientów.

Decyzja organu nadzorczego podyktowana była art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. –

Kodeks postępowania administracyjnego (Dz. U. z 2018 r. poz. 2096 z późn. zm.), art. 12 pkt 2, art. 22 i art. 23 ust. 1 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 z późn. zm.) w związku z art. 100 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. 2019 r. poz. 125).

Sprawa dotyczyła, zdaniem przedsiębiorcy, nieprawidłowości w procesie przetwarzania jego danych osobowych przez Komendanta Głównego Policji w Warszawie polegające na przetwarzaniu jego danych osobowych w Kra-



Jak można stracić klientów przez dane na nasz temat, które przetwarza Policja?

jowym Systemie Informacyjnym Policji (KSIP) oraz w Krajowym Centrum Informacji Kryminalnych (KCIK),

L.M. zawarł w skardze wniosek o nakazanie Komendantowi usunięcie jego danych osobowych z KSIP i KCIK w zakresie informacji uzyskanych w ramach prowadzonego przeciwko niemu postępowania karnego. Jego zdaniem brak było podstaw, dla których organy Policji nadal przechowują i przetwarzają jego dane osobowe w systemach KSIP i KCIK, a konsekwencje istnienia jego danych osobowych w tych systemach odczuwa do dziś.

- *Podczas kontroli drogowej kontrolujący policjanci stwierdzili, że widnieję w ich systemie i zaczęli mnie dopytywać, co zrobiłem (...). Kontrola przebiegała w obecności moich potencjalnych klientów, którzy tego dnia jechali ze mną do miejsca planowanych prac. Wskutek działań policjantów, klienci stracili do mnie zaufanie i wycofali się z transakcji* - opisywał sytuację skarżący, twierdząc, że nie ma przesłanek przemawiających za przydatnością tego rodzaju informacji dla ustawowych działań Policji, w szczególności działań o charakterze wykrywczym oraz zmierzających do zapobiegnięcia popełnienia przestępstwa w przyszłości.

Zażądał więc podjęcia przez Prezesa UODO działań zmierzających do usunięcia jego danych osobowych ze zbiorów KSIP i KCIK.

W odpowiedzi na zapytania Prezesa UODO komendant wyjaśnił, że obywatel, którego sprawa dotyczyła, zwrócił się do niego o usunięcie z KSIP i KCIK jego danych osobowych wprowadzonych w ramach postępowania prowadzonego jeszcze

w 2006 roku. Skarżący był wówczas podejrzany o popełnienie przestępstwa, ale nie został skazany. Wskazano mu podstawy prawne, zwracając uwagę na szczególność tych norm (lex specialis) wobec przepisów ogólnych, jakimi są przepisy ustawy o ochronie danych osobowych oraz art. 51 ust. 5 Konstytucji Rzeczypospolitej Polskiej, który w zakresie zasad i trybu gromadzenia oraz udostępniania informacji o osobie odsyła do regulacji szczególnych.

Skarżący otrzymał też informację, że fakt przetwarzania jego danych osobowych w KSIP i KCIK nie stygmatyzuje jego osoby w świetle prawa.

Dlaczego? Bo informacje, jakimi dysponuje KCIK i KSIP, nie stanowią źródła wiedzy powszechnie dostępnej, gdyż służą wyłącznie realizacji zadań Policji, o których mowa w art. 1 ust. 2 ustawy o Policji.



Jak można stracić klientów przez dane na nasz temat, które przetwarza Policja?



Warto też dodać, że o ile dostęp do informacji o karalności osoby z KRK ma charakter powszechny, to informacje pozyskane i wytworzone przez organy Policji w KSIP i KCIK są zamkniętym, ogólnie niedostępnym zbiorem informacji i danych, służącym jedynie organom Policji dla realizowania ich ustawowych zadań związanych z zapewnieniem bezpieczeństwa i porządku publicznego. Ponadto Policja przetwarza dane osobowe jedynie w podanym zakresie i zgodnie z przytoczonymi przepisami.

Co zdecydował prezes UODO?

Organ nadzorczy zaznaczył, że w dziedzinie przetwarzania różnego rodzaju informacji, w tym danych osobowych, szczególna jest funkcja Policji, bo zbiera ona takie informacje, które podlegają szczególnemu reżimowi i ochronie.

Mówi o tym art. 20 ust. 1 i ust. 2a ustawy o Policji na podstawie którego Policja, z zachowaniem ograniczeń wynikających z art. 19, może uzyskiwać informacje, w tym także niejawne, gromadzić je, sprawdzać oraz przetwarzać (ust. 1).

Policja może pobierać, uzyskiwać, gromadzić, przetwarzać i wykorzystywać w celu realizacji zadań ustawowych informacje, w tym dane osobowe, o osobach, także bez ich wiedzy i zgody. Chodzi tu o:

- osoby podejrzane o popełnienie przestępstw ściganych z oskarżenia publicznego,
- nieletnich dopuszczających się czynów zabronionych przez ustawę jako przestępstwa ścigane z oskarżenia publicznego,
- osoby o nieustalonej tożsamości lub usiłujące ukryć swoją tożsamość,
- osoby stwarzające zagrożenie, o których mowa w ustawie z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób,
- osoby poszukiwane,

Jak można stracić klientów przez dane na nasz temat, które przetwarza Policja?

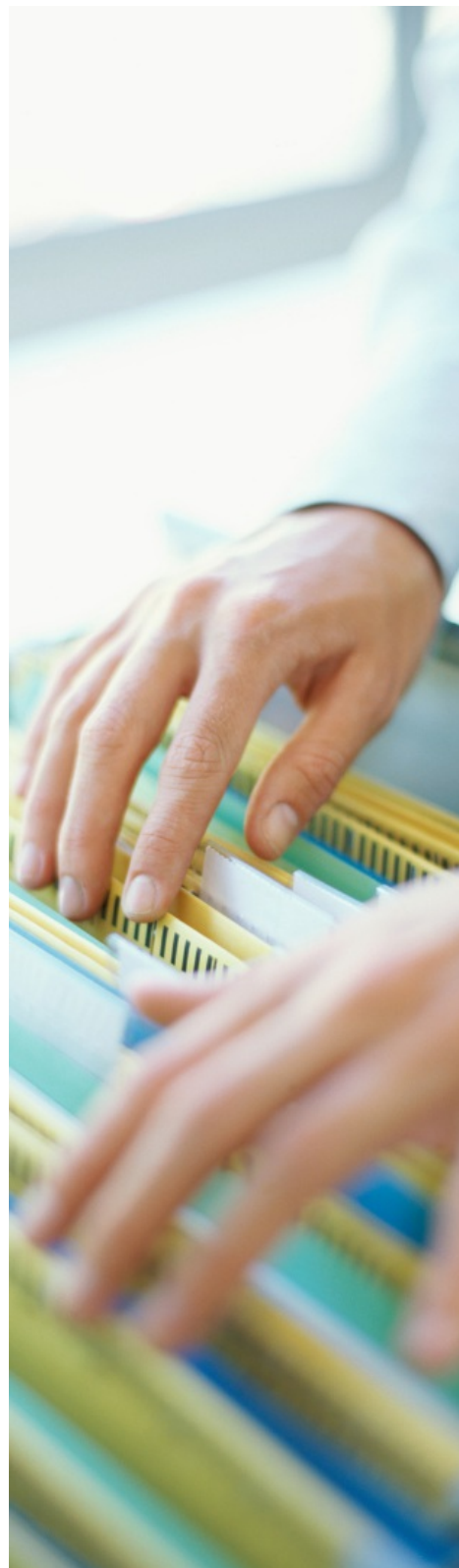
- osoby zaginione,
- osoby, wobec których zastosowano środki ochrony i pomocy, przewidziane w ustawie z dnia 28 listopada 2014 r. o ochronie i pomocy dla pokrzywdzonego i świadka (Dz. U. z 2015 r. poz. 21) (art. 20 ust. 2a ustawy o Policji).

Na zasadach określonych w art. 20 ust. 2a ustawy o Policji funkcjonariusze wprowadzili dane osobowe LM. do zbioru danych KSIP jako o osobie podejrzanej o popełnienie przestępstwa ściganego z oskarżenia publicznego.

Według prawa Policja ma obowiązek dokonywać weryfikacji danych po zakończeniu sprawy, w ramach której te dane zostały wprowadzone do zbioru, a ponadto nie rzadziej niż o 10 lat od dnia uzyskania lub pobrania informacji, usuwając zbędne dane. W tym jednak przypadku, choć dziesięcioletni okres obowiązkowej weryfikacji zgromadzonych danych osobowych minął, to nie zachodziły ustawowe przesłanki do usunięcia danych osobowych Skarżącego z KSIP – nie bez znaczenia pozostaje rodzaj przestępstw, o które był LM. podejrzany. Ponadto informacje kryminalne przechowywane w bazach KCIK są przez 15 lat, nie 10.

Kiedy Policja ma obowiązek usunąć informacje z baz danych KCIK? Określa to art. 25 ustawy o KCIK. Informacje kryminalne podlegają usunięciu z baz danych, jeżeli:

- ich gromadzenie jest zabronione
- zarejestrowane informacje kryminalne okazały się nieprawdziwe
- ustął cel ich gromadzenia
- upłynął okresy, o których mowa w Ustawie o Policji
- jest to uzasadnione ze względu na bezpieczeństwo państwa lub jego obronność
- mogą spowodować identyfikację osób udzielających pomocy przy wykonywaniu czynności operacyjno-rozpoznawczych prowadzonych przez upoważnione do tego podmioty uprawnione.



Jak można stracić klientów przez dane na nasz temat, które przetwarza Policja?

Co istotne, przepis art. 20 ust. 17 ustawy o Policji nie przewiduje usuwania ze zbiorów danych zebranych o osobach podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego, które zostały prawomocnie uniewinnione bądź wobec których postępowanie karne zostało prawomocnie bezwarunkowo umorzone, niezwłocznie po uprawomocnieniu się stosownego orzeczenia.

Prawomocne uniewinnienie konkretnej osoby lub bezwarunkowe umorzenie postępowania karnego wobec konkretnej osoby nie przesądza o tym, czy zgromadzone dane mogą zawierać informacje przydatne dla realizacji ustawowych zadań Policji wobec innych osób.

Ostatecznie?

Czy roszczenia L.M. miały swoje uzasadnienie? Jego dane osobowe zostały pozyskane przez organy Policji w sposób legalny i w taki też są przez nie przetwarzane w KSIP i KCIK. To, że przedsiębiorca utracił klientów nie miało w sprawie znaczenia. Decyzja UODO była ostateczna.

Jak pokonać bariery współpracy administracji? Europejska Strategia Interoperacyjności

Utrzymanie wysokiej pozycji na globalnym rynku wymaga od Unii Europejskiej nieprzerwanego podnoszenia sprawności współpracy międzynarodowej oraz międzydziałowej (w tym między działami administracji). Wszystko po to, by obniżyć koszty funkcjonowania administracji i obsługi potrzeb społecznych, w tym świadczenia usług elektronicznych (e-usług).



Obsługa współpracy międzynarodowej i świadczenia e-usług prowadzona jest różnorodnymi narzędziami informatycznymi, a ich usprawnienie oraz racjonalizacja pracy i ich współpracy w różnych podmiotach wymaga wzajemnego zrozumienia stron. Aby to było możliwe wszyscy powinni stosować te same pojęcia, standardy i – na ile jest możliwość – również narzędzia.

To jest właśnie interoperacyjność przyczyniająca się do eliminacji barier współpracy i jej uproszczenia w wielu dziedzinach życia. To łączenie narzędzi, z których korzysta administracja, przynosi korzyści nie tylko obywatelom, ale i przedsiębiorcom choćby ze względu na oszczędność czasu.

Dla przykładu, osoba chcąc podjąć jednoosobową działalność gospodarczą może skorzystać z funkcjonalności portalu Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG) i zarejestrować działalność bez wychodzenia z domu.

To, co jest wymagane, to znajomość podstawowych osobistych danych oraz posiadanie osobistego podpisu elektronicznego czy Profilu Zaufanego. Cały proces dokonuje się dzięki zautomatyzowanej wymianie informacji między systemami w tym przypadku Zakładu Ubezpieczeń Społecznych czy Kasy Rolniczego Ubezpieczenia Społecznego, Głównego Urzędu Statystycznego i Krajowej Administracji Skarbowej. Po potwierdzeniu rejestracji przedsię-

Jak pokonać bariery współpracy administracji? Europejska Strategia Interoperacyjności



biorca może od ręki prowadzić działalność gospodarczą.

Z kolei np. rolnicy chcąc otrzymać dopłaty, nie muszą odwiedzać biur Agencji Restrukturyzacji i Modernizacji Rolnictwa, bo mogą składać wnioski elektronicznie, a dopłaty są im przekazywane bezpośrednio na ich konta bankowe.

Wymiar europejski

Aby nadać wymiar praktyczny interoperacyjności i wskazać sposób dochodzenia do jej wdrożenia w wymiarze europejskim, zostały opracowane Europejskie Ramy Interoperacyjności (European Interoperability Framework – EIF) ze strategią wdrażania.

Rozporządzenia w sprawie interoperacyjności weszły w życie 11 czerwca 2019 roku. A do końca 2023 roku wszystkie państwa członkowskie, państwa stowarzyszone w ramach Schengen oraz agencji Unii zapewniły pełne wdrożenia rozporządzeń w sprawie interoperacyjności. To termin, do kiedy dostępność nowych i zaktualizowanych systemów IT oraz elementów interoperacyjności ma być już zapewniona.

Połączenie systemów informacyjnych UE wprowadzone zostało, by poprawić skuteczność i wydajność kontroli granicznych na granicach zewnętrznych, przyczynienia się do zapobiegania nielegalnej imigracji oraz zapewnienia wysokiego poziomu bezpieczeństwa w ramach przestrzeni wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej.

Poprawa wdrażania wspólnej polityki wizowej, pomoc w rozpatrywaniu wniosków o udzielenie ochrony międzynarodowej, przyczynianie się do zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i prowadzenia w ich sprawie postępowań przygotowawczych oraz ułatwienie identyfikacji nieznanych osób – to kolejne cele, jakie stoją

Jak pokonać bariery współpracy administracji? Europejska Strategia Interoperacyjności

przed krajami. Co ciekawe, temat jest dziś mocno aktualny i potrzebny, zwłaszcza w czasach kryzysów migracyjnych.

Europejskie systemy informacyjne

Europejskie systemy informacyjne poddano interoperacyjności, by one same, a przede wszystkim zawarte w nich dane mogły wzajemnie się uzupełniać przy jednoczesnym poszanowaniu praw podstawowych obywateli, zwłaszcza prawa do ochrony danych osobowych.

Kiedy przyjęto rozporządzenia związane z interoperacyjnością, już funkcjonowały trzy systemy informacyjne Unii Europejskiej: System Informacyjny Schengen (SIS), Wizowy System Informacyjny (VIS) i system Eurodac.

6 kwietnia 2016 roku Komisja Europejska przedstawiła propozycje, które mają zwiększyć bezpieczeństwo granic zewnętrznych poprzez zastosowanie nowych technologii. Obejmują one:

- unijny System Wjazdu/Wyjazdu (EES) – system z zastosowaniem do wszystkich podróżnych niebędących obywatelami UE, którym zezwolono na pobyt krótkoterminowy w strefie Schengen. Pozwoli na większą automatyzację kontroli granicznych i skuteczniejsze wykrywanie oszustw dotyczących dokumentów i tożsamości; Rozporządzenie weszło w życie w grudniu 2017 roku. Obecnie agencja eu-LISA wraz z państwami członkowskimi rozpoczęła prace wdrożeniowe. Uruchomienie systemu planowane jest na rok 2022.
- stworzenie Europejskiego Systemu Informacji o Podróżach oraz Zezwoleń na Podróż (ETIAS), aby gromadzić informacje na temat podróżnych zwolnionych z obowiązku wizowego, przed ich podróżą. ETIAS pozwoli przeprowadzać kontrole z wyprzedzeniem i w razie



Jak pokonać bariery współpracy administracji? Europejska Strategia Interoperacyjności

potrzeby odmawiać wjazdu do strefy Schengen obywatelom państw trzecich zwolnionym z obowiązku wizowego. Pomoże poprawić bezpieczeństwo wewnętrzne i zapobiegać nielegalnej imigracji, ograniczy zagrożenia dla zdrowia publicznego. Zmniejszy też opóźnienia na granicach, wskazując osoby, które mogą stwarzać ryzyko w jednym z tych obszarów, przed ich przybyciem na granice zewnętrzne. Rozporządzenie weszło w życie we wrześniu 2018 roku. Obecnie agencja eu-LISA wraz z państwami członkowskimi rozpoczęła prace wdrożeniowe.

Po wejściu w życie rozporządzeń Komisja rozpoczęła przygotowanie pierwszego zestawu środków wykonawczych (czterech aktów wykonawczych i dwóch aktów delegowanych), które są konieczne na początkowym etapie procesu projektowania i opracowywania.

W odniesieniu do aktów wykonawczych ustanowiono komitet na podstawie art. 74 rozporządzenia (UE) 2019/817 i art. 70 rozporządzenia (UE) 2019/818. Jeżeli chodzi o przygotowanie niezbędnych aktów delegowanych, ustanowiono grupę ekspertów zgodnie z art. 73 rozporządzenia (UE) 2019/817 i art. 69 rozporządzenia (UE) 2019/818. UE postawiła sobie za cel wdrożenie ram interoperacyjności do końca 2023 roku, choć konieczne jest monitorowanie potencjalnych opóźnień spowodowanych kryzysem związanym z Covid-19.

RODO 2021 – Polska i Europa. RAPORT



2021 rok okazał się w Polsce rekordowy pod względem liczby kar nałożonych przez prezesa Urzędu Ochrony Danych Osobowych w związku z naruszeniem RODO. W 2020 w związku z wybuchem pandemii patrzył na podmioty prowadzące działalność dość pobłażliwie. Ten rok jest zupełnie inny. Kary jednak nie są jedynym ważnym tematem dotyczącym RODO. Przyspieszyły prace nad ważnymi rozporządzeniami, wprowadzono wiele regulacji.

Kary. Coraz więcej i coraz wyższe

W Polsce w porównaniu z innymi krajami Unii Europejskiej kary są stosunkowo niskie. Pod tym względem rekordy bije Francja i Wielka Brytania. Jeśli chodzi o ich liczbę, to na podium nadal stoi Hiszpania.

A jak jest w Polsce? Kary nie są tak wysokie, jednak nie ma co ukrywać, że w 2021 roku wymierzono ich już sporo i prezes UODO wcale nie zwalnia tempa. Co chwilę przypomina podmiotom, dlaczego i w jakich sytuacjach dochodzi do naruszeń oraz jak powinna wyglądać współpraca między podmiotem a Urzędem Ochrony Danych Osobowych, kiedy toczy się postępowanie.

Do końca tego roku prezes UODO ma wydać około 1600 decyzji administracyjnych. Opublikowano ich zaledwie 30, z czego aż 13 (do 6 grudnia) dotyczyło nałożenia kary pieniężnej. Jest to widoczny wzrost w porównaniu do lat ubiegłych. Przypomnijmy, w 2019 roku wydano ich 6, w 2020 – 12 i w 2021 do 6 grudnia – 13.

2021 jest więc kolejnym rekordowym rokiem, jeśli chodzi o liczbę stwierdzonych naruszeń, gdzie podmioty muszą zapłacić kary od kilkudziesięciu do kilkuset złotych. Nieprawidłowości odnotowane zostały w takich branżach jak: ubezpieczenia, pożyczki, finanse, energetyka, doradztwo, platforma satelitarna, jednostki publiczne (uczelnie). Najniższa kara wyniosła 2,2 tys. euro – najwyższa – 245 tys. euro.

RODO 2021 – Polska i Europa. RAPORT

Przegląd kar

2021 rok rozpoczął się nałożeniem kary w wysokości 5,5 tys. euro dla Śląskiego Uniwersytetu Medycznego, w styczniu ukarane zostały również: Enea (30 tys. euro), Anwara (4,6 tys. euro), podmiot nieznany (19 tys. euro). Luty zamknął się jedną karą dla Krajowej Szkoły Sądownictwa i Prokuratury (22,2 tys. euro), marzec – dla spółki Funeda (4,9 tys. euro), kwiecień – dla PNP (5,05 tys. euro) i Cyfrowego Polsatu (245 tys. euro). Dwie kary wymierzone zostały końcem czerwca dla P4 – Play (22 tys. euro) i Sopockiego Towarzystwa Ubezpieczeń ERGO Hestia (34,3 tys. euro).

W lipcu dowiedzieliśmy się o karze dla Fundacji Promocji Mediacji i Edukacji Prawnej Lex Nostra (2,8 tys. euro). Miesiąc później ukarany został Prezes Sądu Rejonowego w Zgierzu (2,2 tys. euro), Następnie prezes UODO zdecydował się na nałożenie kary na Bank Millennium S.A (79 tys. euro). Do 6 grudnia 13 podmiotów publicznych i prywatnych odczuło skutki naruszeń Rozporządzenia o Ochronie Danych Osobowych.

Gdyby przyrzeć się wszystkim nałożonym karom, można wyciągnąć wniosek, że w Polsce średnia grzywna za naruszenie RODO to 86 tys. euro. To i tak nic w porównaniu np. z karą, jaką może zapłacić Amazon. Luksemburg gigantowi e-commerce wymierzył karę w wysokości 746 mln euro. Sprawa jest jeszcze w toku i ostateczna kwota nie jest przesądzona.

Do tej pory najwięcej, bo 50 mln euro, musiało zapłacić Google, któremu nawet odwołania nie pomogły. Francuzi uznali, że nie informował w wystarczającym stopniu o tym, w jaki sposób zbiera ich dane i jak je wykorzystuje, dobierając reklamy. Sąd poparł decyzję organu nadzorczego. Podobnie było w przypadku H&M, który nie informował swoich pracowników, w jaki sposób zbiera dane o nich. To kosztowało spółkę ponad 35 mln euro.

W całej Europie za złamanie przepisów RODO nałożono już kary na 280 mln euro – ta suma to zaledwie 1/3 kary, jaką



RODO 2021 – Polska i Europa. RAPORT

miałby zapłacić wspomniany Amazon. Najczęściej karne są firmy w Hiszpanii – tam organ nadzorujący od 2018 roku ukarał kilkaset firm, dla porównania – w Polsce kar jest około 30.

Za co te kary i dlaczego? Przegląd

Z zasady administracyjna kara pieniężna ma być skuteczna, proporcjonalna i ma odstraszać przed ponownym dokonaniem naruszenia przepisów RODO nie tylko ukarany podmiot, ale i innych.

Niezgłoszenie naruszenia nie oznacza wcale braku odpowiedzialności za nie. To bardzo ryzykowna strategia, którą jednak wiele firm stosuje. Zawsze jednak może znaleźć się osoba, która poinformuje Urząd Ochrony Danych Osobowych o naruszeniu, tak jak w przypadku Towarzystwa Ubezpieczeń i Reasekuracji WARTA S.A. O wystaniu maila z polisą do nieuprawnionego adresata UODO poinformował sam odbiorca wiadomości. Organ nadzorczy dowiedział się przy okazji o braku zawiadomienia o naruszeniu osoby, której dane zostały udostępnione. To skutkowało karą w wysokości 85 tys. złotych. Podobnie było w przypadku sopockiego Towarzystwa Ubezpieczeń ERGO HESTIA S.A. Tam podmiot przetwarzający w wyniku pomyłki adresu mailowego udostępnił dane osobowe. Terminowo zawiadomił prezesa UODO,

czego nie zrobił administrator danych. Ubezpieczyciela kosztowało to 160 tys. złotych.

Karę można dostać również za **niestosowanie obowiązujących procedur i brak kontroli**. Przekonała się o tym Szkoła Główna Gospodarstwa Wiejskiego w czasie rekrutacji na studia. Pracownikowi skradziono prywatny laptop, który zawierał dane osobowe studentów. UODO zarzuciło administratorowi brak aktualizacji dokumentacji ochrony danych oraz audytów wewnętrznych. Okazało się, jak ważna jest inwentaryzacja zasobów.

Przykład spółki Funeda pokazuje, że również **brak współpracy z UODO** w ramach wykonywania przez organ nadzorczy jego zadań również może skutkować nałożeniem kary pieniężnej. Funeda nie przekazała do UODO dostępu do danych, ani nie udzieliła niezbędnych informacji do rozpatrzenia skargi, która wpłynęła do prezesa urzędu. Jakby tego było mało, nie wyjaśniła naruszenia mimo dwukrotnego wezwania. Zignorowanie UODO kosztowało spółkę 20 tys. złotych.

Co ciekawe, karę może dostać firma, która **bezpośrednio naruszenia nie dokonała**, a zrobił to jej współpracownik. Jest to możliwe, gdy to ona jest administratorem danych i ona za nie



RODO 2021 – Polska i Europa. RAPORT

odpowiada. Tak było w przypadku Cyfrowego Polsatu, który nie wdrożył odpowiednich środków technicznych i organizacyjnych przy współpracy z firmą kurierską. Efektem tego były liczne naruszenia identyfikowane z dużym opóźnieniem.

Z powodu tych zaniedbań prezes UODO nałożył na spółkę karę pieniężną w wysokości ponad 1,1 mln zł i jest to najwyższa w tym roku kara za naruszenie RODO. – Pomimo że naruszenia związane były z nieprawidłowościami po stronie firmy kurierskiej, to właśnie ukarany administrator danych nieprawidłowo realizował nadzór nad egzekwowaniem postanowień umownych, przez co dochodziło do późnej identyfikacji naruszeń – przekazał UODO.

RODO 2021. Prace nad prawem UE

Choć pandemia utrudniła i opóźniła prace nad prawem Unii Europejskiej w zakresie ochrony

danych osobowych, to rok 2021 przyniósł kilka istotnych zmian. Mamy tu na myśli w szczególności nowe **Prawo Komunikacji Elektronicznej** czy **rozporządzenie e-privacy, nazywane RODO II**. To pierwsze miało wejść w życie jeszcze w grudniu 2020 roku, prace nad drugim trwają już od 2017 roku. Oba akty prawne zaprezentowaliśmy szczegółowo w poprzednich wydaniach "RODOmagazyn".

Ze względu na pandemię priorytetowymi tematami stały się także: dane osobowe a **ochrona zdrowia, bezpieczeństwo danych oraz usługi IT, cyberbezpieczeństwa, sztucznej inteligencji**. A ostatnio również głośniej mówi się o **umacnianiu granic i systemach informatycznych**.

Pamiętajmy, że w czerwcu Komisja Europejska wydała też decyzję o **przekazywaniu danych osobowych z Unii Europejskiej do Wielkiej Brytanii**. Kwestia transferu danych do UK powstała w wyniku odejścia UK z UE. W tym samym miesiącu odbył się szczyt UE-USA, który na nowo zapoczątkował **partnerstwo transatlantyckie** i ustanowił wspólny program współpracy między UE a USA po pandemii. Przywódcy zobowiązali się do regularnego dialogu w celu podsumowania postępów.

Końcówka 2021 to ostateczny termin wdrożenia **procedur ochronnych sygnalistów** przez podmioty z sektora publicznego i większe przedsiębiorstwa. Obowiązek ten wynika z wprowadzenia Dyrektywy Parlamentu Europejskiego i Rady (UE). Ma również związek z ochroną danych osobowych osób zgłaszających naruszenia w zakładach pracy.

Co przyniesie 2022 rok? Co nas czeka w kolejnych latach? Czego możemy się spodziewać?

ZOSTAŃ AUTOREM EKSPERCKICH ARTYKUŁÓW

Zapraszamy
do współtworzenia
pisma
RODOmagazyn
autorów treści
o tematyce ochrony
danych osobowych
i bezpieczeństwa
w biznesie

redakcja@politykabezpieczenstwa.pl

O redakcji

Rzetelna Grupa

Firma świadcząca kompleksowe usługi doradcze w zakresie prawa gospodarczego, prawa spółek handlowych, prawa konsumenckiego, praw autorskich oraz ochrony danych osobowych. Specjalizuje się w obsłudze podmiotów z branży e-commerce, nowoczesnych technologii IT oraz prowadzących szeroko rozumianą działalność w Internecie. Rzetelną Grupę tworzą **doświadczeni eksperci, radcy prawni, prawnicy oraz menedżerowie**, którzy wspierają przedsiębiorców w prowadzeniu bezpiecznego **e-biznesu**, zgodnego z obowiązującymi przepisami prawa i najlepszymi praktykami.

Rzetelna Grupa posiada w swoim portfolio **sześć marek** – produktów, które precyzyjnie definiują świadczone przez firmę usługi.



Rzetelny Regulamin: platforma certyfikacji sklepów i serwisów internetowych. W ramach Rzetelnego Regulaminu spółka dostarcza przedsiębiorcom, prowadzącym działalność w internecie, usługi związane z audytem e-sklepów i serwisów branżowych, opracowaniem dedykowanego regulaminu oraz opieką prawną pod kątem zgodności prowadzonego e-biznesu z przepisami prawa, spełnienia obowiązków informacyjnych oraz poszanowania praw konsumenta.
www.rzetelnyregulamin.pl



Polityka Bezpieczeństwa: usługa kierowana jest do wszystkich przedsiębiorców przetwarzających dane osobowe w firmie. Polega na opracowaniu dokumentu polityki bezpieczeństwa oraz wdrożeniu procedur przetwarzania i ochrony danych osobowych, zgodnie z aktualnie obowiązującymi przepisami prawa RODO i UODO. Usługa gwarantuje pełną ochronę danych osobowych oraz bezpieczeństwo procesu ich przetwarzania. Eksperti Rzetelnej Grupy pomagają także w zakresie wsparcia w codziennych obowiązkach ADO, a także IOD (Inspektor Ochrony Danych).
www.politykabezpieczenstwa.pl



DziennikPrawny.pl to serwis informacyjny poświęcony biznesowi i prawu. Dedykowany dla konsumentów jak i przedsiębiorców. Jest zbiorem aktualnie obowiązujących przepisów i ich interpretacji dotyczących szeroko rozumianego handlu, zarówno w sklepach stacjonarnych, jak i online, praw konsumentów i obowiązków sprzedawcy. Serwis to także bogata baza eksperckich publikacji z zakresu prawa konsumenckiego, handlowego, prawa pracy i innych obszarów.
www.dziennikprawny.pl

O redakcji



GDP System: to usługa skierowana do Administratorów Danych Osobowych, a także do Inspektorów Ochrony Danych Osobowych. Kompleksowe rozwiązanie do obsługi RODO w firmie, dzięki któremu w jednym miejscu możesz wykazać się rozliczalnością w zakresie prowadzonej dokumentacji, ewidencji zbiorów, umów powierzenia. Możesz również przeszkolić pracowników z zakresu RODO. Ważnym elementem jest pomoc w zakresie analizy ryzyka, a także w zakresie wsparcia przy ocenie konieczności zgłoszenia incydentu do UODO. System wspiera również w odpowiadaniu na żądania osób, których dane są przetwarzane przez ADO.

www.gdpsystem.eu



Rzetelny Prawnik: to usługa skierowana do małych i średnich przedsiębiorstw, które nie posiadają w swoich strukturach działów prawnych, ale potrzebują rzetelnych konsultacji i opinii prawnych na najwyższym poziomie. Usługi świadczone są na jasnych zasadach w ramach abonamentu, który precyzuje zakres doradztwa i jego koszt. Model usługi zapewnia wsparcie dedykowanego doradcy, indywidualnie opracowywane umowy i dokumenty prawne, a także bezpieczeństwo finansowe.

www.rzetelnyprawnik.pl



Rzetelny Konkurs: to kompleksowe doradztwo w zakresie organizacji i obsługi konkursów oraz loterii. Ekspert Rzetelnej Grupy wspierają przedsiębiorców na każdym etapie projektu, począwszy od pomysłu, przez zabezpieczenie prawne i techniczne konkursu oraz zabezpieczenie obsługi uczestników konkursu, na przyznaniu Certyfikatu Rzetelnego Konkursu kończąc. Certyfikat Rzetelnej Grupy podnosi w oczach uczestników wiarygodność organizatora i poczucie bezpieczeństwa.

www.rzetelnykonkurs.pl

Rzetelna Grupa jest współzałożycielem Izby Gospodarki Elektronicznej, której zadaniem jest rozwijanie rodzimego rynku e-commerce.



e-COMMERCE POLSKA
IZBA GOSPODARKI ELEKTRONICZNEJ

Zapraszamy do odwiedzenia naszej strony rzetelnagrupa.pl i bezpośredniego kontaktu. Podczas rozmowy przedstawimy szczegóły dowolnej naszej usługi.