01/2020 CZERWIEC

NEWSLETTER RODO

Temat numeru -

Status i rola IOD w świetle najnowszych decyzji organów nadzorczych

Tematy artykułów:

- Praktyka wykonywania funkcji IOD
- Ochrona danych osobowych w czasach pandemii COVID-19
- Wytyczne EROD dotyczące zgody (cookies)
- Prawo do bycia zapomnianym (wyrok FSK)
- Najnowsze naruszenia ochrony danych

Traple
Konarski
Podrecki
& Wspólnicy

TKP

PRAKTYKA WYKONYWANIA
FUNKCJI IOD

IOD nie może jednocześnie pełnić funkcji kierownika działów zgodności, zarządzania ryzykiem i audytu

Xawery Konarski, Iga Małobęcka-Szwast

Dnia 28 kwietnia 2020 r. Izba Procesowa belgijskiego organu ochrony danych stwierdziła, że spółka Proximus, powierzając funkcję inspektora ochrony danych (IOD) kierownikowi działów zgodności, zarządzania ryzykiem i audytu, dopuściła się naruszenia przepisów RODO, które wymagają, aby dodatkowe zadania wykonywane przez IOD nie powodowały konfliktu interesów (art. 38 ust. 6 RODO).

W swojej decyzji belgijski organ nadzorczy wskazał w szczególności, że:

- Łączenie roli kierownika działów zgodności, zarządzania ryzykiem i audytu z funkcją inspektora ochrony danych powoduje istotny konflikt interesów.
- Do konfliktu dochodzi w sytuacji, gdy IOD – w ramach swoich zadań związanych z danym stanowiskiem pracy – określa cele i środki przetwarzania danych osobowych. Rola IOD powinna być bowiem ograniczona do wewnętrznej konsultacji przetwarzania danych, a nie podejmowania operacyjnej odpowiedzialności za te procesy.
- Brak konfliktu interesów wymaga autonomiczności decyzji IOD, a spełnienie tego warunku powinno być oceniane indywidualnie dla każdego przypadku.
- W zależności od rozmiaru i struktury danej organizacji dobrą praktyką administratorów lub podmiotów przetwarzających powinno być:

  a) zidentyfikowanie stanowisk, które pozostają w „konflikcie" z funkcją IOD;
  b) opracowanie wewnętrznych zasad, pozwalających na uniknięcie konfliktu interesów;
  c) w wewnętrznych regulacjach lub w umowach o świadczenie usług wprowadzenie postanowień zapewniających, że do takiego konfliktu nie dochodzi.

W sprawie Proximus IOD, pełniąc funkcję kierownika działów zgodności, zarządzania ryzykiem i audytu, określał cele i sposoby przetwarzania danych osobowych oraz był odpowiedzialny za czynności przetwarzania w ramach tych działów. Połączenie obu tych ról uniemożliwiało więc wykonywanie przez IOD niezależnego nadzoru nad przetwarzaniem danych w ramach ww. działów, wymaganego przez RODO.

W analizowanej sprawie belgijski organ nadzorczy dopatrzył się również naruszenia art. 38 ust. 1 RODO[1], który wymaga, żeby administrator zapewnił, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych, oraz art. 38 ust. 5 RODO, który zobowiązuje IOD do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.

Za nieprzestrzeganie wymogów określonych w RODO co do wyznaczenia i statusu inspektora ochrony danych belgijski organ nadzorczy nałożył na spółkę karę pieniężną w wysokości 50 000 euro. Wskazał on, że konieczność zapewnienia niezależności IOD oraz tego, by dodatkowe zadania mu powierzane nie powodowały konfliktu interesów, należy co do zasady do obowiązków administratora danych.

Uzasadniając wysokość kary, belgijski organ nadzorczy podkreślił, że spółka dopuściła się w tym zakresie poważnego zaniedbania, w szczególności biorąc pod uwagę, że:

- obowiązek powołania IOD oraz przepisy regulujące jego status nie są nowe;
- podstawowa działalność spółki (administratora) polega na przetwarzaniu danych osobowych (w tym szczególnych kategorii danych) na bardzo dużą skalę;
- naruszenie ochrony danych w takiej spółce może mieć negatywny wpływ na prawa i wolności milionów osób.

Choć jest to jak dotąd najwyższa kara pieniężna nałożona przez belgijski organ nadzorczy, to stanowi ona jedynie mniej niż 0,01% obrotów przedsiębiorstwa.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Jeden organ publiczny – jeden IOD

Iga Małobęcka-Szwast

W ocenie bawarskiego organu nadzorczego organ lub podmiot publiczny nie może wyznaczyć więcej niż jednego IOD. Powołanie przez administratora więcej niż jednego IOD z rożnymi zakresami kompetencji stałoby w sprzeczności ze statusem i zadaniami IOD wynikającymi z RODO.

Obowiązek powołania IOD przez organ lub podmiot publiczny

Zgodnie z art. 37 ust. 1 lit. a RODO[1] organ lub podmiot publiczny zobowiązane są do wyznaczenia inspektora ochrony danych (IOD). Powstała jednak wątpliwość, czy organy lub podmioty publiczne mogą wyznaczyć kilku inspektorów ochrony danych, z których każdy miałby odrębny zakres kompetencji.

Czy organ lub podmiot publiczny może powołać tylko jednego IOD?

Wątpliwość tę rozstrzygnął w swoim stanowisku bawarski komisarz ds. ochrony danych (Bayerischer Landesbeauftragte für den Datenschutz). Zdaniem bawarskiego organu nadzorczego nie jest możliwe wyznaczenie więcej niż jednego IOD przez jednego administratora.

Zdaniem organu przeciwko wyznaczeniu kilku IOD przez tego samego administratora świadczy:

- Samo brzmienie art. 37 ust. 1 RODO, który mówi o wyznaczeniu „inspektora", a nie „inspektorów" ochrony danych.
- Klasyfikacja instytucjonalna i obowiązki IOD. Pełni on funkcję punktu kontaktowego dla osób, których dane dotyczą (art. 38 ust. 4 RODO) oraz organu nadzorczego (art. 39 ust. 1 lit. d i e RODO). Powołanie przez administratora więcej niż jednego IOD z rożnymi zakresami kompetencji przeczyłoby – w ocenie organu – jednolitemu ujęciu statusu i zadań IOD w RODO.

W ocenie bawarskiego organu nadzorczego wyznaczenie przez administratora kilku IOD z różnymi zakresami kompetencji utrudniłoby w szczególności:

- skuteczne egzekwowanie uprawnień przez osobę, której dane dotyczą, w szczególności gdy taka osoba zwróciłaby się z żądaniem najpierw do „niewłaściwego" IOD;
- współpracę IOD z organami nadzorczymi oraz pełnienie przez niego funkcji punktu kontaktowego dla organów nadzorczych.

Taka sytuacja zmuszałaby bowiem osoby, których dane dotyczą, oraz organy nadzorcze do dokonywania wstępnego badania co do tego, który IOD jest właściwy w danej sprawie, i podejmowania dodatkowych czynności w wypadku, gdyby taka osoba lub organ nadzorczy zwrócili się najpierw do „niewłaściwego" IOD.

Jeden IOD dla kilku administratorów – organów lub podmiotów publicznych

Bawarski organ nadzorczy wskazał jednocześnie, że dopuszczalna jest sytuacja odwrotna, tj. wyznaczenie jednego IOD dla kilku administratorów – organów lub podmiotów publicznych, jeżeli są ze sobą ściśle powiązane organizacyjnie. Wprost o takiej możliwości przesądza art. 37 ust. 3 RODO.

Zastępca i zespół IOD

Co istotne, bawarski organ nadzorczy podkreślił, że powyższe stanowisko nie stoi w sprzeczności z powołaniem zastępcy IOD na wypadek, gdyby IOD zachorował lub z innego powodu czasowo nie mógł wykonywać swoich obowiązków. W takim wypadku zastępca IOD wykonuje wszystkie kompetencje IOD i co do zasady organy nadzorcze i podmioty danych nie będą miały wątpliwości odnośnie do zakresu jego kompetencji.

Ponadto powyższe stanowisko organu nie uniemożliwia IOD wsparcia personelu pomocniczego (zespołu IOD) w wykonywaniu jego obowiązków. Bawarski organ zauważa, że powołanie takiego zespołu może się nawet okazać niezbędne, szczególnie w przypadku dużych organizacji – zgodnie bowiem z art. 38 ust. 2 RODO administrator musi zapewnić IOD niezbędne zasoby (w tym zasoby ludzkie) do wykonywania jego zadań, o których mowa w RODO. Wewnętrzne usytuowanie personelu pomocniczego IOD pozostawione jest w gestii administratora – może on utworzyć np. zespół IOD lub ustanowić lokalnych koordynatorów lub osoby kontaktowe ds. ochrony danych, pamiętając, że możliwe jest wyznaczenie wyłącznie jednego IOD.

Choć stanowisko bawarskiego organu nadzorczego dotyczy bawarskich organów i podmiotów publicznych, wydaje się, że ustalenia tam poczynione mają charakter uniwersalny i mogą znaleźć zastosowanie również do podmiotów z sektora prywatnego w innych państwach członkowskich.
Źródło: https://www.datenschutz-bayern.de

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Wiedza fachowa wymagana od IOD a jego odwołanie

Iga Małobęcka-Szwast

Regionalny sąd pracy dla landu Meklemburgia-Pomorze Przednie w wyroku z dnia 25 lutego 2020 r. dookreślił, jakie kwalifikacje musi posiadać inspektor ochrony danych, co należy rozumieć pod pojęciem wiedzy fachowej wymaganej od IOD i jak wpływa to na jego odwołanie.

Sprawa powstała na kanwie sporu między IOD a szpitalem klinicznym (administratorem), w którym IOD był zatrud-niony. Administrator zwolnił (odwołał) IOD, ponieważ uznał, że nie posiada on odpowiedniej wiedzy specjalistycz-nej ani nie wykonuje należycie swoich obowiązków. Sąd odniósł się do pojęcia wiedzy fachowej wymaganej od IOD i uznał, że w niniejszej sprawie odwołanie IOD – wykwalifi-kowanego prawnika – ze względu na rzekome niewykony-wanie przez niego obowiązków oraz brak wiedzy fachowej jest nieskuteczne.

Wymogi wynikające z RODO

Zgodnie z art. 37 ust. 5 RODO[1] inspektora ochrony danych powołuje się na podstawie jego kwalifikacji zawodowych, w szczególności jego wiedzy specjalistycznej w dziedzinie prawa ochrony danych i praktyki ochrony danych, a także na podstawie jego zdolności do wykonywania swoich zadań. RODO nie precyzuje jednak, jakie konkretne kwalifikacje zawodowe wymagane są do pełnienia funkcji IOD.

Pojęcie wiedzy fachowej

Sąd przywołał motyw 97 RODO, zgodnie z którym niezbędny poziom wiedzy fachowej należy ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają dane osobowe przetwarzane przez administratora lub podmiot przetwarzający.

Sąd podkreślił, że wymagana wiedza specjalistyczna zależy od rodzaju i charakteru działalności prowadzonej przez administratora. Przy jej ocenie należy wziąć pod uwagę takie czynniki, jak:

- wielkość organizacji;
- zakres i skomplikowanie czynności przetwarzania danych;
- stosowane procesy informatyczne;
- rodzaj (wrażliwość) przetwarzanych danych osobowych.

Odnosząc się do pojęcia wiedzy fachowej, Sąd stwierdził, że:

- Możliwość wykonywania funkcji IOD nie jest powiązana z żadnym konkretnym wykształceniem ani bliżej określoną wiedzą specjalistyczną. Co do zasady wymagana jest jednak znajomość prawa ochrony danych, technologii przetwarzania danych i procesów operacyjnych.
- Wiedza fachowa IOD musi pozwalać mu na wykonywanie zadań określonych w art. 39 RODO.
- Jeśli IOD posiada specjalistyczną wiedzę jedynie w określonym podobszarze ochrony danych osobowych, może on w pozostałym zakresie polegać na wykwalifikowanym personelu (np. zespole IOD). W ocenie Sądu wymóg wiedzy fachowej nie oznacza zatem, że IOD musi znać się na wszystkim – może on mieć zespół, który wspiera go w wykonywaniu zadań, w zakresie, w jakim IOD takiej specjalistycznej wiedzy nie posiada.
- IOD musi nie tylko posiadać niezbędną specjalistyczną wiedzę, lecz także dawać gwarancję, że będzie wykonywać swoje zadania sumiennie i nie będzie naruszać swoich obowiązków jako IOD, w szczególności obowiązku zachowania poufności.

Ponadto Sąd zwrócił uwagę na konieczność zapewnienia IOD możliwości utrzymania jego wiedzy fachowej, w szczególności poprzez udział w szkoleniach dotyczących nowych osiągnięć technicznych oraz zmian w prawie i orzecznictwie. Proces doskonalenia wiedzy fachowej IOD powinien być wspierany przez administratora.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

IOD jako pracownik administratora

W ocenie Sądu wiarygodność i niezawodność wymagane od wewnętrznego IOD mogą zostać zakwestionowane nie tylko w wypadku naruszenia obowiązków związanych z wykonywaniem tej funkcji, lecz także w sytuacji poważnego naruszenia ogólnych zobowiązań wynikających z umowy o pracę. W wypadku wewnętrznego IOD jego pozycja jako inspektora ochrony danych nie może być całkowicie oddzielona od leżącego u jego podstaw stosunku pracy. Poważne naruszenie zobowiązań umownych może oznaczać, że nie może on już skutecznie wykonywać swoich zadań (w tym w zakresie monitorowania) jako IOD na podstawie przepisów o ochronie danych.

Sąd stwierdził jednak, że w niniejszej sprawie do takiego poważnego naruszenia obowiązków IOD oraz obowiązków wynikających ze stosunku pracy nie doszło.

Specjalna ochrona wewnętrznego IOD przed zwolnieniem

Warto zwrócić również uwagę na specyfikę prawa niemieckiego w zakresie specjalnej ochrony wewnętrznego IOD przed zwolnieniem, przewidzianej w federalnej ustawie o ochronie danych osobowych (Bundesdatenschutzgesetz, BDSG). Zgodnie z § 38 ust. 2 w powiązaniu z § 6 ust. 4 zd. 2 BDSG zwolnienie IOD jest dozwolone tylko na zasadach analogicznych do tych, o których mowa w § 626 niemieckiego kodeksu cywilnego (Bürgerliches Gesetzbuch, BGB), tj. wyłącznie z ważnych powodów. Rozwiązanie stosunku pracy z IOD jest co do zasady niedozwolone, chyba że istnieją fakty, które uprawniają administratora do rozwiązania umowy z ważnego powodu bez zachowania okresu wypowiedzenia. Sąd za takie ważne powody uważa w szczególności te, które uniemożliwiają wykonywanie zadań przez IOD lub poważnie temu zagrażają, takie jak ujawnienie tajemnic lub trwałe naruszenie obowiązków w zakresie monitorowania przez IOD.

Ta szczególna ochrona przed zwolnieniem ma na celu wzmocnienie pozycji IOD i jego niezależności. Sąd podkreślił, że IOD powinien mieć możliwość wykonywania swoich zadań kontrolnych w zakresie ochrony danych osobowych bez obawy, że zostanie odwołany.

Co istotne, specjalna ochrona przed zwolnieniem dotyczy tylko tych inspektorów ochrony danych, których powołanie jest obowiązkowe (tj. ochroną tą nie są objęci inspektorzy wyznaczeni dobrowolnie przez administratora).

Choć brak jest podobnego przepisu na gruncie prawa polskiego, wydaje się, że konieczność zapewnienia szczególnej ochrony IOD przed zwolnieniem może wynikać pośrednio z art. 38 ust. 3 RODO, zgodnie z którym IOD nie może być odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań.

OCHRONA DANYCH OSOBOWYCH
W CZASACH PANDEMII COVID-19

Czy pracodawcy mogą zbierać dane o stanie zdrowia pracowników w związku z epidemią COVID-19? Stanowisko EROD i Prezesa UODO

dr Grzegorz Sibiga, Katarzyna Syska

Zgodnie ze stanowiskiem EROD zbieranie przez pracodawców danych o stanie zdrowia zależy od tego, czy pozwalają na to przepisy krajowe. Natomiast Prezes UODO jako jedyny przepis pozwalający na zbieranie od pracowników danych o stanie zdrowia wskazuje zmieniony specustawą o COVID-19 art. 8a ustawy o Państwowej Inspekcji Sanitarnej, na podstawie którego organy inspekcji sanitarnej mogą wydawać decyzje, wytyczne lub zalecenia w zakresie środków zapobiegawczych.

Stanowisko EROD: kluczowe są przepisy krajowe

Europejska Rada Ochrony Danych (EROD) stwierdziła, że RODO pozwala na przetwarzanie danych o stanie zdrowia, ale kluczowe znaczenie mają przepisy prawa krajowego. Pracodawcy mogą zbierać dane o stanie zdrowia pracowników, o ile wynika to z przepisów prawa krajowego i w zakresie, jaki wskazują te przepisy.

Stanowiska Prezesa UODO

Prezes UODO wydał już trzy oświadczenia dotyczące zbierania danych osobowych w związku z epidemią COVID-19. Wszystkie stanowiska są zbliżone, jednak w ostatnim z nich (z 5 maja br.) Prezes UODO najbardziej jednoznacznie wypowiedział się o dopuszczalności gromadzenia danych o stanie zdrowia pracowników, w tym mierzenia temperatury ciała, i o symptomach choroby.

Po pierwsze Prezes UODO stwierdził, że przepisy o ochronie danych osobowych nie sprzeciwiają się przetwarzaniu danych o temperaturze ciała czy o objawach choroby, o ile wynika to ze szczegółowych przepisów prawa. Podstawą przetwarzania danych jest art. 9 ust. 2 lit. i RODO[1].

Jako przepis szczegółowy Prezes UODO wskazał art. 17 specustawy o COVID-19 z dnia 2 marca 2020 r.[2]. Przepis ten dodaje art. 8a ust. 5 do ustawy o Państwowej Inspekcji Sanitarnej[3]. Na jego podstawie organy inspekcji sanitarnej mogą wydawać:

- decyzje nakładające obowiązek podjęcia czynności zapobiegawczych lub kontrolnych;
- zalecenia i wytyczne określające sposób postępowania w trakcie realizacji przez podmioty, do których kierowane są takie zalecenia lub wytyczne.

Według Prezesa UODO właśnie takie działania organu inspekcji sanitarnej – decyzje, zalecenia lub wytyczne – stanowiłyby podstawę prawną tych działań, a zarazem podstawę do przetwarzania danych osobowych dotyczących stanu zdrowia.

Co istotne, Prezes UODO nie wskazuje żadnych innych przepisów krajowych, które mogłyby pozwalać na zbieranie danych osobowych o stanie zdrowia pracowników w związku z epidemią COVID-19. Warto tu zauważyć, że Prezes UODO nie odnosi się do obowiązków pracodawców z zakresu zapewnienia bezpiecznych i higienicznych warunków pracy oraz ochrony życia i zdrowia pracowników. Ogólne przepisy o BHP są czasem interpretowane w taki sposób, że w okolicznościach epidemii wynika z nich obowiązek chociażby mierzenia temperatury ciała pracowników czy też zbierania informacji o symptomach choroby. Stanowisko Prezesa UODO wydaje się przeczyć takiej interpretacji.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
[2] Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych.
[3] Ustawa z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej.

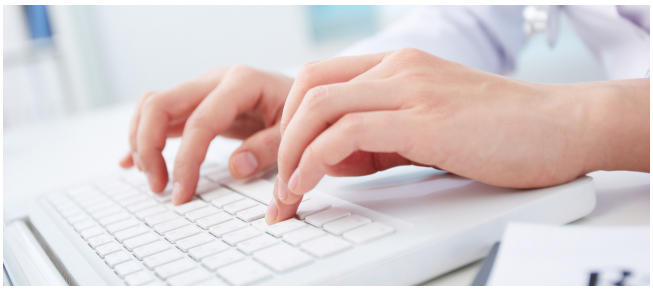
W stanowisku Prezesa UODO podkreślono też, że **zgoda pracownika na zbieranie danych o stanie zdrowia nie byłaby dla pracodawcy właściwą przesłanką przetwarzania tych danych.** Wynika to z faktu, że w relacjach między pracownikiem a pracodawcą występuje brak równowagi, a zatem zgoda pracownika mogłaby nie być dobrowolna.

Co ma zrobić pracodawca, który chciałby zbierać dane o stanie zdrowia pracowników, a taka możliwość nie wynika z wydanych przez GIS zaleceń lub wytycznych, które by go dotyczyły?

W świetle stanowiska Prezesa UODO najbezpieczniejszym rozwiązaniem jest złożenie wniosku do inspekcji sanitarnej o nałożenie na pracodawcę decyzji nakazującej mu dokonywanie pomiarów temperatury czy też dokonywanie innych czynności zapobiegawczych, przy których konieczne jest zbieranie danych o stanie zdrowia pracowników.

Jakie wytyczne GIS pozwalają na zbieranie danych o stanie zdrowia pracowników?

Na podstawie art. 8a ust. 5 pkt 2 ustawy o Państwowej Inspekcji Sanitarnej Główny Inspektor Sanitarny wydał wytyczne dla niektórych branż. W wytycznych dla zakładów fryzjerskich i podmiotów świadczących usługi kosmetyczne GIS zaleca właśnie mierzenie temperatury ciała pracowników oraz gromadzenie w wywiadach innych danych o objawach chorobowych u pracowników. Jednakże z wytycznych GIS wynika, że dane takie powinny być zbierane tylko za zgodą pracowników. W związku z tym wytyczne GIS są sprzeczne ze stanowiskiem Prezesa UODO, według którego zgoda pracownika nie może być w tym wypadku podstawą zbierania danych przez pracodawcę.



Jakie wytyczne innych organów, w porozumieniu z GIS, zalecają zbieranie danych o stanie zdrowia pracowników i jaki jest status tych wytycznych?

Dopuszczenie mierzenia temperatury – za zgodą osoby badanej – znajduje się także w dokumentach innych podmiotów wydawanych w uzgodnieniu z GIS. Do takich wytycznych należą m.in. wytyczne Ministra Rolnictwa i Rozwoju Wsi dla producentów rolnych zatrudniających cudzoziemców przy pracach sezonowych oraz ogólne wytyczne Centralnego Instytutu Ochrony Pracy „Bezpieczeństwo i ochrona zdrowia osób pracujących w czasie epidemii COVID-19" (w tym ostatnim dokumencie badaniem objęto tylko gości w zakładzie pracy).

Warto jednak podkreślić, że dokumenty te nie mają charakteru wytycznych z ustawy o Państwowej Inspekcji Sanitarnej – nie są bowiem wydawane przez organ inspekcji sanitarnej. Zatem zgodnie ze stanowiskiem Prezesa UODO nie mogą one być podstawą prawną zbierania danych osobowych przez pracodawców.

Kierowanie pracowników na badania w kierunku zakażenia SARS-CoV-2 (koronawirusem)

W ostatnim czasie często pojawiają się pytania dotyczące tego, czy pracodawca może skierować pracowników na obowiązkowe badania w kierunku zakażenia koronawirusem (badania genetyczne RT-PCR lub badania serologiczne), a następnie otrzymać wyniki tych badań.

Prezes UODO nie odniósł się do tej kwestii w swoich dotychczasowych stanowiskach.

Natomiast zalecenie kierowania na takie badania w odniesieniu do sezonowych zagranicznych pracowników gospodarstw rolnych wynika z wytycznych MRiRW i GIS dla producentów rolnych zatrudniających cudzoziemców przy pracach sezonowych w związku z rozprzestrzenianiem się wirusa SARS-CoV-2. Jednakże – o czym była mowa wyżej – wytyczne te nie zostały wydane przez organ inspekcji sanitarnej, a zatem nie mają mocy wiążącej.

Jak bezpiecznie pracować zdalnie?

Dominika Nowak

Epidemia COVID-19 postawiła przed pracodawcami i pracownikami wiele wyzwań związanych z bezpieczeństwem informacji, w tym danych osobowych podczas pracy zdalnej.

W niniejszym artykule przedstawiamy wskazówki dotyczące takich obszarów, jak:

- bezpieczeństwo korzystania z urządzeń, służbowej poczty e-mail, sieci oraz chmury;
- bezpieczeństwo korzystania z dokumentacji papierowej;
- bezpieczeństwo korzystania z wideokonferencji.

Ochrona danych osobowych podczas pracy zdalnej

Prezes Urzędu Ochrony Danych Osobowych (UODO) 17 marca 2020 r. opublikował porady dotyczące bezpieczeństwa danych osobowych podczas pracy zdalnej.

Porady te można podzielić na trzy kategorie:

- dotyczące bezpieczeństwa korzystania z urządzeń;
- dotyczące korzystania ze służbowej poczty e-mail;
- dotyczące bezpiecznego korzystania z sieci i chmury.

Więcej informacji: https://uodo.gov.pl/pl/138/1459.

Dokumentacja papierowa zawierająca dane osobowe a praca zdalna

Prezes UODO 4 maja 2020 r. opublikował porady dotyczące korzystania z dokumentacji papierowej podczas pracy zdalnej.

Organ wskazał, że pracodawca może zezwolić na korzystanie z dokumentacji papierowej, lecz musi mieć na względzie większe ryzyko naruszenia bezpieczeństwa danych osobowych. Korzystanie z dokumentacji papierowej przez pracownika musi być uzasadnione.

Przedstawiono również wymogi, które pracodawca powinien spełnić, aby pracownicy bezpiecznie korzystali z dokumentacji papierowej podczas pracy zdalnej od uzyskania dostępu do dokumentów do ich zniszczenia.

Więcej informacji: https://uodo.gov.pl/pl/138/1513.

Jak bezpiecznie korzystać z wideokonferencji?

Dnia 15 marca 2020 r. ENISA (Agencja Unii Europejskiej ds. Cyberbezpieczeństwa) opublikowała dokument zawierający wskazówki dotyczące cyberbezpieczeństwa podczas pracy zdalnej.

ENISA zwraca uwagę na bezpieczeństwo połączenia wifi, aktualizacje oprogramowania antywirusowego oraz zapewniającego bezpieczeństwo danych, wykonywanie kopii zapasowych, blokowanie ekranu w wypadku pracy w pomieszczeniach współdzielonych, zapewnienie bezpiecznego połączenia ze środowiskiem pracy oraz zainstalowanie narzędzi szyfrujących.

Pracodawcy powinni również informować pracowników o tym, jak należy reagować na techniczne problemy związane z pracą zdalną, w tym incydenty bezpieczeństwa. Pracownikom należy także dostarczyć rozwiązania techniczne związane ze zdalnym dostępem (np. szyfrowanie) oraz wirtualne rozwiązania, takie jak podpis elektroniczny, w celu zapewnienia ciągłości działania.

ENISA podkreśla, że należy zachować czujność w związku z podwyższonym prawdopodobieństwem ataków phishingowych.

Więcej informacji: https://www.enisa.europa.eu.

Cyberbezpieczeństwo w czasie epidemii

NASK (Naukowa i Akademicka Sieć Komputerowa) wspólnie z Biurem do Walki z Cyberprzestępczością Komendy Głównej Policji oraz Europolem opublikowała podstawowe zasady cyberbezpieczeństwa, które dotyczą:

- tworzenia kopii zapasowych;
- zabezpieczenia sieci wifi, dostępu do urządzeń, zainstalowania programu antywirusowego, tworzenia silnych i unikatowych haseł oraz sprawdzania ustawień prywatności kont w mediach społecznościowych;
- zachowania czujności podczas pandemii;
- zdalnych zakupów;
- bezpieczeństwa dzieci.

Więcej informacji: https://www.nask.pl/pl/aktualnosci.

Przetwarzanie danych w czasie pandemii COVID-19 – wytyczne EROD

Iga Małobęcka-Szwast

Podczas 23. plenarnego posiedzenia Europejska Rada Ochrony Danych (EROD) przyjęła wytyczne dotyczące ochrony danych w kontekście zwalczania pandemii COVID-19:

1. Wytyczne 03/2020 w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych.
2. Wytyczne 04/2020 w sprawie wykorzystania danych o lokalizacji i narzędzi do śledzenia kontaktów zakaźnych w kontekście pandemii COVID-19.

Wytyczne 03/2020 w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych

Wytyczne 03/2020 w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych mają na celu wyjaśnienie wątpliwości prawnych związanych z wykorzystaniem takich danych. Wytyczne odnoszą się do takich kwestii, jak:

- podstawa prawna przetwarzania;
- dalsze przetwarzanie danych dotyczących zdrowia do celów badań naukowych;
- wdrożenie odpowiednich zabezpieczeń;
- wykonywanie praw osób, których dane dotyczą.

EROD podkreśla, że przepisy dotyczące ochrony danych (w szczególności RODO) nie stoją na przeszkodzie środkom podejmowanym w walce z pandemią COVID-19. Przede wszystkim EROD zauważa, że RODO wprost przewiduje wyjątki od zakazu przetwarzania szczególnych kategorii danych osobowych, takich jak dane dotyczące zdrowia, gdy jest to konieczne do celów badań naukowych.

Art. 4 RODO nie zawiera jasno sprecyzowanej definicji „przetwarzania do celów badań naukowych". „Jak wskazano w motywie 159, przetwarzanie danych osobowych do celów badań naukowych należy interpretować szeroko, obejmując tym pojęciem na przykład rozwój technologiczny i demonstrację, badania podstawowe, badania stosowane oraz badania finansowane ze środków prywatnych. (...) Wyrażenie »do celów badań naukowych« powinno obejmować także badania prowadzone w interesie publicznym w dziedzinie zdrowia publicznego".

W ocenie EROD terminu tego nie należy jednak rozciągać poza powszechne znaczenie i w tym kontekście pojęcie „badania naukowe" powinno się rozumieć jako „projekt badawczy zorganizowany zgodnie z odpowiednimi normami metodycznymi i etycznymi w danym sektorze oraz zgodnie z dobrymi praktykami".

W odniesieniu do podstaw prawnych przetwarzania danych dotyczących zdrowia EROD podkreśla, że musi być ono zgodne z zasadami określonymi w art. 5 RODO oraz z jedną z podstaw prawnych i szczególnymi wyjątkami wymienionymi odpowiednio w art. 6 i art. 9 RODO w celu zgodnego z prawem przetwarzania tej szczególnej kategorii danych osobowych.

Jako dopuszczalną podstawę prawną przetwarzania danych dotyczących zdrowia do celów badań naukowych EROD wskazuje:

- zgodę osoby, której dane dotyczą, uzyskaną zgodnie z art. 6 ust. 1 lit. a i art. 9 ust. 2 lit. a RODO, z zastrzeżeniem, że wszystkie warunki wyraźnej zgody, w szczególności te określone w art. 4 ust. 11, art. 6 ust. 1 lit. a, art. 7 i art. 9 ust. 2 lit. a RODO, muszą być spełnione;
- art. 6 ust. 1 lit. e lub art. 6 ust. 1 lit. f RODO w połączeniu z uchwalonymi wyjątkami na mocy art. 9 ust. 2 lit. j lub art. 9 ust. 2 lit. i RODO.

Wytyczne 04/2020 w sprawie wykorzystania danych o lo-kalizacji i narzędzi do śledzenia kontaktów zakaźnych w kontekście pandemii COVID-19

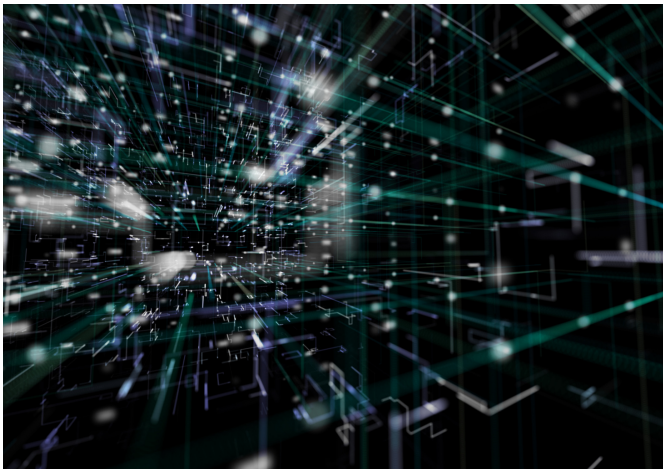
Wytyczne 04/2020, które odnoszą się do geolokalizacji i innych narzędzi ustalania kontaktów zakaźnych w związku z wybuchem pandemii, wyjaśniają natomiast warunki i zasady proporcjonalnego wykorzystania danych dotyczących lokalizacji i narzędzi ustalania kontaktów zakaźnych w celu:

- wykorzystania danych dotyczących lokalizacji w celu wsparcia reakcji na pandemię poprzez modelowanie rozprzestrzeniania się wirusa w celu oceny ogólnej skuteczności środków ograniczających jego rozprzestrzenianie się;
- korzystania z systemu ustalania kontaktów zakaźnych, którego celem jest powiadomienie osób, które mogły znajdować się w bliskiej odległości od osoby, która ostatecznie została uznana za nosiciela wirusa, aby jak najszybciej przerwać łańcuch zakażenia.

W wytycznych podkreślono, że zarówno RODO, jak i dyrektywa 2002/58/WE o prywatności i łączności elektronicznej zawierają szczegółowe przepisy pozwalające na wykorzystanie danych anonimowych lub osobowych w celu wsparcia władz publicznych i innych podmiotów zarówno na szczeblu krajowym, jak i unijnym w ich wysiłkach na rzecz monitorowania i powstrzymania rozprzestrzeniania się COVID-19.

W ocenie EROD stosowanie aplikacji umożliwiających śledzenie kontaktów zakaźnych powinno być dobrowolne i nie powinno opierać się na śledzeniu przemieszczania się poszczególnych osób, lecz na informacjach o bliskości użytkowników.

EROD przypomniał, że ogólne zasady skuteczności, konieczności i proporcjonalności muszą przyświecać wszelkim środkom przyjętym przez państwa członkowskie lub instytucje UE obejmującym przetwarzanie danych osobowych w celu zwalczania COVID-19.



[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
[2] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej).

ORZECZNICTWO SĄDÓW KRAJOWYCH ORAZ
WYTYCZNE I STANOWISKA ORGANÓW NADZORCZYCH

Aktualizacja wytycznych EROD dotyczących zgody

Dominika Nowak

W zaktualizowanej wersji wytycznych Europejska Rada Ochrony Danych wprowadziła dodatkowe wyjaśnienia odnośnie do sposobów wyrażania zgody oraz tzw. cookie walls.

Dnia 4 maja 2020 r. Europejska Rada Ochrony Danych (EROD) przyjęła zaktualizowaną wersję wytycznych dotyczących zgody. Aktualizacji dokonano w dwóch rozdziałach wytycznych:

- warunkowość (paragrafy 38–41);
- jednoznaczne oświadczenie woli (paragraf 86).

Warunkowość

Przede wszystkim EROD zwraca uwagę, że zgody nie można uznać za dobrowolną, jeżeli administrator twierdzi, iż istnieje wybór między jego usługą, która obejmuje zgodę na wykorzystanie danych osobowych do dodatkowych celów (bez której wyrażenia administrator nie będzie świadczył usługi), a równoważną usługą oferowaną przez innego administratora. W takim przypadku swoboda wyboru byłaby uzależniona od działalności innych podmiotów i od tego, czy dla osoby, której dane dotyczą, usługa innego administratora byłaby rzeczywiście równoważna i jednocześnie dostępna. Dodatkowo takie uzależnienie ważności zgody od istnienia usług innego podmiotu oznaczałoby obowiązek monitorowania przez administratorów sytuacji na rynku i zachowań konkurencyjnych usługodawców w celu zapewnienia ważności zgody. Zdaniem EROD zgoda oparta na tym, że istnieją usługi alternatywne oferowane przez inne podmioty, jest niezgodna z RODO. W takim wypadku dostawca usług nie może uniemożliwić osobom, których dane dotyczą, dostępu do swojej usługi na tej podstawie, że nie wyrażą one zgody.

W tym kontekście EROD opisała nowy przykład związany z tzw. cookie walls. Zdaniem Rady w celu zapewnienia swobodnego wyrażenia zgody przez użytkownika dostęp do usług i funkcjonalności nie może być uzależniony od jego zgody na przechowywanie informacji lub uzyskania dostępu do informacji już przechowywanych w urządzeniu końcowym użytkownika, czyli tzw. cookie walls.

EROD wskazuje przykład takiego niedopuszczalnego działania. Dostawca usługi internetowej wprowadza skrypt, który blokuje widoczność treści – widoczna jest jedynie prośba o zaakceptowanie plików cookies oraz informacja o ich ustawieniach i celach przetwarzania danych. W tym wypadku użytkownik nie ma możliwości uzyskania dostępu do treści bez zaznaczenia przycisku „Akceptuj pliki cookies". Zdaniem EROD w tej sytuacji użytkownikowi nie pozostawiono rzeczywistego wyboru, więc zgoda nie była udzielona dobrowolnie.

Jednoznaczne oświadczenie woli

W ocenie EROD takie działania jak przewijanie lub przesuwanie strony internetowej lub podobna aktywność użytkownika nie spełniają wymogu wyraźnego i potwierdzającego działania. Mogą one być trudne do odróżnienia od innych działań lub interakcji użytkownika na stronie internetowej. W takim przypadku ustalenie, czy zebrano jednoznaczną zgodę, jest niemożliwe. EROD zwraca uwagę, że w takiej sytuacji trudno będzie również zapewnić, aby wycofanie zgody było równie łatwe, jak jej udzielenie.

W pozostałym zakresie EROD dokonała wyłącznie zmian edycyjnych.

Podsumowanie

Powyższe zaktualizowane wytyczne EROD mają szczególne znaczenie dla:

- administratorów, którzy zamierzali uzależniać dostęp do usługi od wyrażenia zgody do celów marketingowych lub od zainstalowania plików cookies do celów marketingowych;
- administratorów, który zamierzali uzyskiwać zgodę na pliki cookies poprzez przewijanie lub przesuwanie strony internetowej.

Link do pełnej treści zaktualizowanych wytycznych: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Prawo do bycia zapomnianym w świetle orzeczenia niemieckiego Federalnego Sądu Konstytucyjnego

Iga Małobęcka-Szwast

Niemiecki Federalny Sąd Konstytucyjny (FSK) w wyroku z dnia 25 lutego 2020 r. odniósł się do tzw. prawa do bycia zapomnianym, które wywodzi on z niemieckiej ustawy zasadniczej (Grundgesetz) oraz ujętego tam prawa do samostanowienia informacyjnego i ogólnego prawa osobistego (Persönlichkeitsrecht). Uprawnienia te nie gwarantują jednak prawa do bycia publicznie postrzeganym według własnego uznania.

Prawo do bycia zapomnianym w niemieckiej ustawie zasadniczej

Choć prawo do bycia zapomnianym wynika wprost z RODO (art. 17)[1], to zostało wywiedzione niezależnie przez FSK z prawa do samostanowienia informacyjnego i ogólnego prawa osobistego, które uregulowane są w art. 2 ust. 1 w zw. z art. 1 ust. 1 niemieckiej ustawy zasadniczej. Ustalenia FSK poczynione w wyroku opierają się zatem wyłącznie na prawie krajowym.

Okoliczności sprawy

Skarżący żądał usunięcia z internetowego archiwum prasowego artykułu sprzed ponad 35 lat, z którego wynikało, że skarżący jest synem byłego burmistrza niemieckiego miasta. Ze względu na fakt, że skarżący – jako partner w kancelarii prawnej noszącej jego nazwisko – nie chciał być publicznie kojarzony jako syn byłego burmistrza, próbował on pozwać wydawcę czasopisma o powstrzymanie się od wskazywania jego nazwiska w artykule. Sąd cywilny oddalił pozew skarżącego, więc złożył on skargę konstytucyjną do FSK.

Ustalenia FSK

FSK nie przyjął do rozpoznania skargi konstytucyjnej. Stwierdził, że udostępnienie w wynikach wyszukiwania artykułu prasowego, z którego wynika stosunek pokrewieństwa (filiacja) skarżącego z jego ojcem, nie narusza ogólnego prawa osobistego skarżącego ani jego prawa do samostanowienia informacyjnego.

W ocenie FSK ogólne prawo osobiste chroni swobodny rozwój osobowości i zapewnia ochronę przed rozpowszechnianiem informacji zawierających dane osobowe, które mogą negatywnie wpływać na rozwój osobisty podmiotu danych. Prawo to nie gwarantuje jednak prawa do bycia publicznie postrzeganym według własnego uznania.

Ważenie interesów

W przypadku rozpowszechniania artykułów prasowych ocena w poszczególnych sytuacjach opiera się na wyważeniu sprzecznych interesów chronionych przez prawa podstawowe, przy uwzględnieniu konkretnych okoliczności. Należy zatem określić i wyważyć odpowiednie potrzeby w zakresie ochrony osobistej, w szczególności biorąc pod uwagę okoliczności i przedmiot, a także formę, rodzaj i zakres publikacji oraz jej znaczenie i skutki z perspektywy czasowej, względem interesu prasy w raportowaniu o prawdziwych informacjach ze sfery społecznej.

FSK podkreślił ciągłą wartość informacyjną zarchiwizowanego artykułu oraz ogólny interes prasy w utrzymywaniu publicznej dostępności swoich archiwów w formie możliwie jak najbardziej kompletnej i bez wprowadzania zmian, w szczególności mając na względzie pierwotną dopuszczalność publikacji. FSK zakłada przy tym, że skarżący nie ponosi żadnych znaczących negatywnych konsekwencji wynikających z publicznej wiedzy o jego pokrewieństwie (filiacji) z byłym burmistrzem. Niedogodności, jakie wynikają dla skarżącego z dostępności artykułu i wiedzy o jego pochodzeniu (filiacji), nie są, zdaniem FSK, nieproporcjonalne ani nie przeważają nad podstawowym interesem prasy i ogółu społeczeństwa w ciągłej dostępności artykułów prasowych po ich opublikowaniu. W omawianej sprawie FSK stwierdził, że niezbędne wyważenie praw podstawowych nie skutkuje „prawem do bycia zapomnianym".

Pozycja w wynikach wyszukiwania

FSK zwrócił również uwagę, że po wpisaniu imienia i nazwiska skarżącego kwestionowany artykuł pojawia się dopiero na piątej stronie wyników wyszukiwania (w pozycjach od 40 do 50). Artykuł ten nie widnieje zatem w „priorytetowych" pozycjach wyszukiwarki, które są najczęściej sprawdzane przez użytkowników szukających informacji o skarżącym, i jest mało prawdopodobne, aby osoby te dotarły do wiadomości o filiacji między skarżącym a burmistrzem na kwestionowanej stronie internetowej. Wydaje się zatem, że zdaniem FSK pozycja na liście wyników wyszukiwania jest czynnikiem wpływającym na ocenę legalności udostępniania informacji w wynikach wyszukiwania.

Źródło: decyzja z dnia 25 lutego 2020 r. (1 BvR 1282/17), dostępna pod linkiem.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Naruszenia ochrony danych osobowych w kwietniu i maju 2020 r.

Dominika Nowak

W kwietniu i maju 2020 r. na polskim rynku miało miejsce pięć naruszeń ochrony danych osobowych, które zostały ujawnione i szeroko komentowane. Przedstawiamy ich zestawienie uwzględniające źródła i typy zagrożeń.

Fortum Marketing and Sales Polska S.A.

W dniach od 12 do 16 kwietnia 2020 r. doszło do naruszenia bezpieczeństwa danych osobowych klientów tego administratora – dostawcy energii elektrycznej. Naruszenie dotyczyło następującego zakresu danych: imię, nazwisko, adres, numer telefonu, PESEL lub numer dowodu osobistego.

Zdarzenie polegało na naruszeniu poufności danych osobowych poprzez ich przypadkowe udostępnienie na serwerze zewnętrznego dostawcy świadczącego usługi na rzecz administratora.

Naruszenie ochrony danych zostało zgłoszone do Prezesa UODO oraz do Prokuratury Okręgowej w Gdańsku. Zawiadomiono również Zespół CERT Polska, działający w strukturach NASK, oraz Komendę Wojewódzkiej Policji w Gdańsku (Wydział do Walki z Cyberprzestępczością).

Dnia 18 maja 2020 r. Prezes UODO poinformował o wszczęciu postępowania administracyjnego w sprawie naruszenia przepisów o ochronie danych osobowych.

Więcej informacji:
https://uodo.gov.pl/pl/138/1510
https://uodo.gov.pl/pl/138/1526
https://www.fortum.pl/komunikat-do-klientow-fortum-marketing-and-sales-polska-sa

Krajowa Szkoła Sądownictwa i Prokuratury w Krakowie (KSSIP)

Administrator poinformował, że doszło do nieuprawnionego dostępu do danych osobowych zgromadzonych na platformie szkoleniowej KSSiP, która od lutego 2020 r. była nieaktywna.

Zakres danych osobowych objętych naruszeniem to: nazwa użytkownika, imię, nazwisko, numer lub numery telefonu, adres e-mail, jednostka, wydział, adres jednostki, miasto, adres IP, daty pierwszego i ostatniego logowania oraz zaszyfrowane hasło.

Administrator poinformował, że doszło do nieuprawnionego dostępu do danych osobowych zgromadzonych na platformie szkoleniowej KSSiP, która od lutego 2020 r. była nieaktywna.

Zakres danych osobowych objętych naruszeniem to: nazwa użytkownika, imię, nazwisko, numer lub numery telefonu, adres e-mail, jednostka, wydział, adres jednostki, miasto, adres IP, daty pierwszego i ostatniego logowania oraz zaszyfrowane hasło.

Zdarzenie polegało na naruszeniu poufności danych osobowych poprzez pobranie przez nieuprawnione osoby plików zamieszczonych w lokalizacji publicznej. Zostały one zamiesz-czone w tej lokalizacji przez pracownika podmiotu zewnętrz-nego obsługującego KSSIP.

Naruszenie zostało zgłoszone do Prezesa UODO, Policji, Zespołu Zarządzania Incydentami Biura Cyberbezpieczeństwa w Ministerstwie Sprawiedliwości, Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT NASK oraz Prokuratury Krajowej.

Więcej informacji:
https://uodo.gov.pl/pl/138/1496
https://www.kssip.gov.pl/node/6909
https://www.kssip.gov.pl/sites/default/files/zaktualizowany_komunikat_w_trybie_art._34_rodo.pdf

Panek S.A.

Dnia 17 kwietnia 2020 r. doszło do naruszenia ochrony danych osobowych w spółce Panek S.A. Podczas procesu uruchamiania nowej strony internetowej pliki poprzedniej strony zostały skopiowane do nowego folderu, który został udostępniony, mimo że powinien zostać ukryty.

Naruszenie dotyczy w szczególności następujących danych: imię, nazwisko, adres, numer telefonu, numer PESEL, adres e-mail, haszowane hasła, dane dotyczące wypożyczeń oraz dane dotyczące kont pracowników.

Naruszenie polegało na naruszeniu poufności danych osobowych poprzez ich nieuprawnione udostępnienie przez pracownika zewnętrznej firmy informatycznej.

Naruszenie ochrony danych zostało zgłoszone do Prezesa UODO dnia 5 maja 2020 r.

Więcej informacji:
https://uodo.gov.pl/pl/138/1514

Politechnika Warszawska

Dnia 3 maja 2020 r. na platformie administracyjnej Ośrodka Kształcenia na Odległość PW (OKNO) doszło do naruszenia ochrony danych.

Naruszenie polegało na nieuprawnionym dostępie do informacji poprzez złamanie zabezpieczeń tej platformy.

Naruszenie zostało zgłoszone Prezesowi UODO, Policji oraz Zespołom Reagowania na Incydenty Bezpieczeństwa Komputerowego: CSIRT GOV, CSIRT MON oraz CSIRT NASK.

Dnia 27 maja 2020 r. Prezes UODO poinformował o wszczęciu postępowania administracyjnego w tej sprawie.

Więcej informacji:
https://uodo.gov.pl/pl/138/1518
https://uodo.gov.pl/pl/138/1545
https://www.pw.edu.pl/Aktualnosci/OKNO-i-naruszenie-RODO-najczesciej-zadawane-pytania

SWPS Uniwersytet Humanistycznospołeczny

Administrator zgłosił do Prezesa UODO naruszenie ochrony danych osobowych.

Naruszenie dotyczy studentów, słuchaczy studiów podyplomowych, pracowników oraz współpracowników. Doszło do utraty dostępności danych osobowych.

Incydent polegał na ataku z wykorzystaniem oprogramowania typu ransomware. Do naruszenia ochrony danych doszło w wyniku uzyskania loginu i hasła administratora przez atakującego.

Więcej informacji:
https://uodo.gov.pl/pl/138/1512

Komentarz

Na podstawie opisu tych pięciu naruszeń nasuwają się następujące wnioski. Zasadnicza część naruszeń ochrony danych dotyczy poufności. W większości przypadków źródłem naruszenia jest pracownik administratora lub pracownik podmiotu zewnętrznego obsługującego administratora. Oznacza to, że administratorzy powinni zwracać szczególną uwagę na zapewnienie odpowiednich szkoleń dla swoich pracowników, a przy wyborze dostawców zewnętrznych powinni zbadać kompetencje ich pracowników w zakresie zachowania bezpieczeństwa informacji.

Druga grupa naruszeń dotyczy sytuacji, w których źródłem naruszeń jest podmiot (osoba) z zewnątrz. W tych wypadkach doszło do utraty poufności danych w związku z przełamaniem zabezpieczeń (Politechnika Warszawska), jak również do utraty dostępności ze względu na zainfekowanie systemu oprogramowaniem typu ransomware (SWPS). W tym zakresie należy okresowo przeprowadzać analizę w celu doboru zabezpieczeń adekwatnych do zidentyfikowanego ryzyka.

NADCHODZĄCE WYDARZENIA

#webinar

Status i rola IOD w świetle najnowszych orzeczeń i stanowisk organów nadzorczych i sądów

Prelegenci: adw. Xawery Konarski, adw. dr Grzegorz Sibiga oraz dr Iga Małobęcka-Szwast.

Plan webinarium

Podczas webinarium przedstawimy przegląd najnowszych decyzji dotyczących statusu i roli IOD w organizacji i wnioski płynące z nich dla praktyki wykonywania funkcji IOD. W szczególności skupimy się na następujących sprawach:

1. Belgia: kara pieniężna nałożona na spółkę Proximus, w której wyjaśniono:

- czy IOD może pełnić funkcje compliance officera lub szefa działu audytu i zarządzania ryzykiem;
- jakie dodatkowe zadania i funkcje może pełnić IOD; jakie dodatkowe zadania i funkcje mogą powodować konflikt interesów w rozumieniu art. 38 ust. 6 RODO;
- co należy zrobić, aby uniknąć konfliktu interesów;
- czy konieczne jest posiadanie polityki zapobiegania konfliktowi interesów;

2. Niemcy: stanowisko bawarskiego organu nadzorczego, który wyjaśnia:

- czy organizacja może wyznaczyć więcej niż jednego IOD;
- czy IOD może mieć zastępcę;
- czy konieczne jest powołanie zespołu IOD i jaki jest jego status;

3. Niemcy: orzeczenie niemieckiego regionalnego sądu pracy, w którym rozstrzygnięto:

- co należy rozumieć pod pojęciem wiedzy fachowej wymaganej od IOD;
- czy IOD musi „znać się na wszystkim”;
- kiedy można odwołać IOD;
- kiedy odwołanie IOD będzie zasadne.

Podczas webinarium omówimy również (4) problematykę polis ubezpieczeniowych dla IOD, tj. jakie rodzaje polis są obecnie oferowane na rynku, czy warto posiadać taką polisę i przed czym ona faktycznie chroni.

Rejestracja >>

ZESPÓŁ RODO

Xawery Konarski
Adwokat, Starszy Partner
xawery.konarski@traple.pl

dr Grzegorz Sibiga
Adwokat, Partner
grzegorz.sibiga@traple.pl

Katarzyna Syska
Adwokat
katarzyna.syska@traple.pl

Dominika Nowak
Radca prawny
dominika.nowak@traple.pl

dr Iga Małobęcka-Szwast LL.M.
Prawnik
iga.malobecka@traple.pl

Pytania prosimy kierować na adres:
rodo@traple.pl