JUSTYNA JABŁONKA

Listopad 2023
Nr 9/2023

KANCELARIA WYRZYKOWSCY

Newsletter
INSPEKTORA OCHRONY DANYCH
ADW. JUSTYNY JABŁONKI

Szanowni Państwo,
Listopad jest z pewnością miesiącem refleksji nad przemijaniem. Za chwilę zamkniemy kolejny rok i otworzymy karty następnego. To, co z pewnością czujemy wszyscy to dynamika zmian, z którymi się obecnie spotykamy. Świat przyśpieszył. I to nie tylko ja mam takie wrażenie. Sztuczna inteligencja niesie za sobą wiele wyzwań w kwestii jej regulacji prawnej, pojawiają się również myśli – jak zdążyć za tymi zmianami? Nowych technologii nie zatrzymamy, pozostaje nam podążać. Śledzić. Próbować nowości. W listopadowym Newsletterze odnoszę się do AI Act w kontekście związku między technologią a prywatnością – RODO. Zapraszam również do zapoznania się z pozostałymi tematami, żywiąc nadzieję, że dostarczą Państwu cennych informacji.

Inspektor Ochrony Danych,
adw. Justyna Jabłonka

Tematy na listopad:

I. AI Act, czym jest i jak odnosi się do RODO.
Autor: Justyna Jabłonka, Inspektor Ochrony Danych, adwokat. Str. 2 (czas czytania: 5 min.). (czas czytania: 5 min.).
II. Bądź zgodny z Rodo. Bądź bezpieczny – cyberbezpieczny. Program #CyberbezpiecznySamorząd w JST.
Autor: Justyna Jabłonka, Inspektor Ochrony Danych, adwokat. Str. 5 (czas czytania: 7 min.). (czas czytania: 7 min.).
III. Odpowiedzialność karna za niezgodne z prawem przetwarzanie danych osobowych.
Autor: Grzegorz Lubeńczuk, zespół Inspektora Ochrony Danych, radca prawny. Str. 9 (czas czytania: 10 min.)
IV. Kara dla pracodawcy za inwigilację pracowników, czyli krótka historia o tym, o co pracodawca pytać może, a o co pytać nie powinien?
Autor: Justyna Cybulska, zespół Inspektora Ochrony Danych, adwokat. Str. 14 (czas czytania: 3,5 min.). (czas czytania: 3,5 min.).

I. AI Act, czym jest i jak odnosi się do RODO.

AI Act (ang. Artificial Intelligence Act) to nazwa unijnego aktu prawodawczego, który dotyczy sztucznej inteligencji (AI). Akt ten reguluje i wprowadza nadzór nad jej stosowaniem w Europie.

Główne cele AI Act to:

1. **Ochrona praw konsumentów i użytkowników**: Akt ma na celu zapewnienie, że sztuczna inteligencja jest używana w sposób bezpieczny i zgodny z prawami obywateli Unii Europejskiej. Chodzi o ochronę praw konsumentów i użytkowników przed potencjalnymi skutkami negatywnymi, takimi jak dyskryminacja czy naruszenia prywatności.
2. **Promowanie innowacji**: AI Act ma również na celu wspieranie innowacji i rozwijanie sektora sztucznej inteligencji w Europie, jednocześnie zapewniając, że innowacje te są zgodne z wartościami i normami UE.
3. **Ustanowienie ram prawnych**: Akt ma na celu wprowadzenie jasnych i spójnych ram prawnych dla sztucznej inteligencji na terenie całej Unii Europejskiej, co ma ułatwić zarówno przedsiębiorstwom, jak i organom regulacyjnym stosowanie przepisów dotyczących AI.

W świecie prawnym i technologicznym pojawia się coraz więcej dyskusji na temat AI Act i jej zgodności z obowiązującymi przepisami RODO. Jako adwokat specjalizujący się w ochronie danych osobowych, chciałbym przedstawić kluczowe aspekty tego tematu, które mogą mieć znaczący wpływ na sposób, w jaki firmy i instytucje zarządzają danymi osobowymi w kontekście sztucznej inteligencji.

Potencjalne Sprzeczności między AI Act a RODO

Unijny AI Act, mający na celu regulowanie stosowania sztucznej inteligencji, może nie być w pełni zgodny z RODO, co podkreślono w najnowszym raporcie Grupy Roboczej ds. Sztucznej Inteligencji. Istotne jest zwrócenie uwagi na brak precyzji w AI Act w kontekście przetwarzania danych osobowych. AI Act, choć zakłada współdziałanie z RODO, nie określa dokładnie, w jaki sposób oba akty mają się uzupełniać, co prowadzi do niejasności prawnych.

Zakaz Wykorzystywania Systemów Biometrycznych

AI Act wprowadza zakaz używania systemów zdalnej identyfikacji biometrycznej w przestrzeni publicznej, co może kolidować z RODO. Choć oba akty mają na celu ochronę danych osobowych, ich wzajemne relacje nie są jasno określone, co może stwarzać trudności w praktycznym zastosowaniu.

Wzajemne Zobowiązania Przejrzystości

AI Act rozszerza obowiązki przejrzystości w odniesieniu do systemów AI, szczególnie tych rozpoznających emocje i kategoryzacji biometrycznej. Jednakże brak jest wyraźnego określenia, jak te nowe wymagania wpisują się w ramy RODO.

Zbieg Sankcji Administracyjnych

W przypadku naruszeń, AI Act i RODO przewidują sankcje administracyjne, które mogą się nakładać. Jest to istotne dla przedsiębiorców, którzy muszą mieć świadomość potencjalnego ryzyka związanego z podwójnymi karami.

Specyfika AI i wyzwania dla ochrony danych

Rozwój systemów AI, zdolnych do przetwarzania dużych ilości danych, wymaga specjalnego podejścia. Decyzje podejmowane przez AI mogą być trudne do zrozumienia, co utrudnia kontrolę nad przetwarzaniem danych osobowych i wymaga dodatkowych regulacji.

Rola sądów w rozstrzyganiu sprzeczności

W przypadku wystąpienia sprzeczności między RODO a AI Act, kwestia ta może zostać przekazana do Trybunału Sprawiedliwości Unii Europejskiej. Sądy krajowe będą miały możliwość zwrócenia się z pytaniem prejudycjalnym w celu rozstrzygnięcia ewentualnych wątpliwości.

Obecnie nad AI Act trwają trilogi. Są to tajne rozmowy pomiędzy Parlamentem Europejskim, Komisją Europejską a Radą UE.

Jako Inspektor Ochrony Danych, zalecam wszystkim jednostkom działającym w obszarze sztucznej inteligencji, aby uważnie śledzili rozwój sytuacji prawnej wokół AI Act i RODO. Należy być przygotowanym na ewentualne zmiany w przepisach i zwracać uwagę na to, jak nowe regulacje mogą wpłynąć na przetwarzanie danych osobowych. Pamiętajmy, że ochrona danych osobowych jest kluczowym elementem odpowiedzialnego wykorzystania technologii AI, a zrozumienie i stosowanie się do obowiązujących przepisów jest niezbędne dla zapewnienia zgodności prawnej i ochrony prywatności.

adw. Justyna Jabłonka
Inspektor Ochrony Danych

II. Bądź zgodny z Rodo. Bądź bezpieczny – cyberbezpieczny. Program #CyberbezpiecznySamorząd w JST.

Jak być *zgodnym z RODO* myślę, że już każdy z nas wie. W końcu rozporządzenie – RODO, weszło w życie już ponad 5 lat temu. Znane nam są zasady w jaki sposób dane osobowe muszą być przetwarzane.

(Wstawka z przepisów):

Artykuł 5 RODO:

Zasady dotyczące przetwarzania danych osobowych

1. **Dane osobowe muszą być:**

a) **przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby**, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość");

b) **zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami**; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami ("ograniczenie celu");

c) **adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów**, w których są przetwarzane ("minimalizacja danych");

d) **prawidłowe i w razie potrzeby uaktualniane**; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("prawidłowość");

e) **przechowywane w formie umożliwiającej identyfikację osoby**, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą ("ograniczenie przechowywania");

f) **przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych**, w tym ochronę przed

niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("integralność i poufność").

Z moich spostrzeżeń wynika jednak, że o ustawie o krajowym systemie cyberbezpieczeństwa *(Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa)* nie pamięta każda JST, albo inaczej – pamięta, ale ta pamięć jest bardzo krótka i wiedza o istnieniu obowiązków wynikających z tej ustawy nie przejawia się w działaniu.

Zgodnie z definicją **cyberbezpieczeństwa**, pochodzącą z w/w ustawy, jest to:

odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Jakie są wyzwania bezpieczeństwa informacyjnego w samorządach?

Badania przeprowadzone przez zespół CSIRT NASK w 2020 roku wykazały, że **ponad połowa zbadanych witryn samorządowych była podatna na ataki.**

To alarmujący sygnał, który potwierdza potrzebę działań na rzecz zwiększenia bezpieczeństwa danych osobowych obywateli oraz skutecznego reagowania na incydenty **w systemach informatycznych JST**.

Zgodnie z RODO, każda jednostka, niezależnie od swojego charakteru, jest zobowiązana do zachowania zgodności z przepisami dotyczącymi ochrony danych osobowych. Dlatego też poprzez ten wpis zwracam uwagę na program **#CyberbezpiecznySamorząd**, stanowiący kroki w kierunku pełnej zgodności z RODO.

Czym jest program #CyberbezpiecznySamorząd?

Program ten został stworzony, aby wesprzeć jednostki samorządu terytorialnego, takie jak gminy, powiaty i województwa, w podniesieniu poziomu cyberbezpieczeństwa. Jego celem jest wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych JST.

Warto podkreślić, że program nie tylko ma na celu ochronę danych osobowych, ale także stanowi odpowiedź na coraz bardziej zaawansowane zagrożenia w świecie cyfrowym, takie jak ataki ransomware czy phishing.

Jakie jest wsparcie finansowe dla samorządów?

Program **#CyberbezpiecznySamorząd** przewiduje wsparcie finansowe dla samorządów, które mogą ubiegać się o środki w zakresie od 200 tysięcy złotych do aż 850 tysięcy złotych. Wysokość przyznanej kwoty zależy od liczby mieszkańców oraz wskaźnika podatkowego danego regionu. Całkowita alokacja środków w programie wynosi 1,9 miliarda złotych, co świadczy o skali problemu i potrzebie zabezpieczenia danych w sektorze publicznym.

Jakie są kluczowe obszary finansowania?

Program skupia się na trzech kluczowych obszarach:

1. **Organizacyjnym**: Samorządy będą mogły doskonalić regulacje wewnętrzne, polityki i procedury związane z bezpieczeństwem informacji. Wdrażanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z normą ISO27001 oraz przeprowadzanie audytów SZBI stanowią część tego obszaru.
2. **Technologicznym**: Samorządy mogą sfinansować zakup i wdrożenie narzędzi oraz sprzętu podnoszących poziom cyberbezpieczeństwa. To obejmuje modernizację infrastruktury IT oraz implementację oprogramowania zwiększającego bezpieczeństwo.
3. **Kompetencyjnym**: Program wspiera podnoszenie świadomości pracowników odpowiedzialnych za cyberbezpieczeństwo oraz rozwijanie ich kompetencji poprzez szkolenia, warsztaty, testy socjotechniczne i penetracyjne.

Dzięki programowi **#CyberbezpiecznySamorząd** samorządy mają szansę na zwiększenie poziomu cyberbezpieczeństwa, co przekłada się na ochronę danych obywateli oraz zapewnienie stabilności i bezpieczeństwa funkcjonowania jednostek samorządu terytorialnego. Program ten stanowi krok w kierunku budowy zaufania do sektora publicznego w erze cyfryzacji.

W mojej opinii jako Inspektora Ochrony Danych w szeregu JST, warto skorzystać z programu **#cyberbezpiecznysamorząd**, w celu zapewnienia bezpieczeństwo informacji w samorządach.

Termin na składanie wniosków został przedłużony do 30 listopada 2023 r.!

adw. Justyna Jabłonka
Inspektor Ochrony Danych

III. Odpowiedzialność karna za niezgodne z prawem przetwarzanie danych osobowych

Sankcje administracyjne i karne za naruszenie zasad przetwarzania danych osobowych

Podstawowymi sankcjami za naruszenie przepisów o ochronie danych osobowych są nakładane przez organ nadzorczy administracyjne kary pieniężne. Kary te sięgają 10 000 000 EUR, a w przypadku przedsiębiorstwa 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. W przypadku naruszenia podstawowych zasad przetwarzania danych osobowych mogą być nawet dwukrotnie wyższe. W niektórych przypadkach naruszenia zasad przetwarzania danych osobowych, polski ustawodawca, bazując na treści upoważnienia zawartego w art. 84 ust. 1 RODO, które daje państwom członkowskim podstawę do przyjęcia przepisów określających inne sankcje za naruszenia przepisów rozporządzenia, wprowadza także odpowiedzialność karną. Przykładem takiej regulacji jest art. 107 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (dalej: u.o.d.o.), który przewiduje odpowiedzialność karną za przetwarzanie danych osobowych w sytuacji, gdy ich przetwarzanie nie jest dopuszczalne albo przez osobę nieuprawnioną do ich przetwarzania. Sprawca, który dopuszcza się przetwarzania danych osobowych w takich okolicznościach podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch. Niezgodne z prawem przetwarzanie danych osobowych może także wyczerpywać znamiona innych czynów zabronionych, w tym w szczególności, określonych w przepisach Kodeksu karnego z dnia 6 czerwca 1997 r. (dalej k.k.), przestępstw przeciwko ochronie informacji. W takim przypadku sankcje karne występują równocześnie z sankcjami administracyjnymi, a sprawca niezgodnego z prawem przetwarzania danych osobowych naraża się zarówno na odpowiedzialność za delikt administracyjny, jak i za przestępstwo.

Przestępstwo niedopuszczalnego przetwarzania danych osobowych lub przetwarzania danych osobowych przez osobę nieuprawnioną

Podstawę odpowiedzialności za przestępstwo z art. 107 ust. 1 u.o.d.o. stanowi ustalenie, że dane osobowe są przetwarzane pomimo, że nie jest to dopuszczalne albo, że przetwarza je osoba nieuprawniona.

Przetwarzanie danych osobowych jest dopuszczalne tylko wtedy i tylko w takim zakresie, w jakim spełniony jest co najmniej jeden z warunków określonych w art. 6 RODO, a w przypadku tzw. danych wrażliwych w art. 9 RODO. Jeżeli administrator danych nie dysponuje żadną spośród wymienionych w tych przepisach podstawą przetwarzania danych osobowych to ich przetwarzanie jest niedopuszczalne. Niedopuszczalność przetwarzania danych może mieć miejsce także w innych przypadkach, np. w sytuacji, gdy osoba, której dane dotyczą, zgłosi na podstawie art. 21 RODO skuteczny sprzeciw wobec ich przetwarzania.

Przetwarzanie danych osobowych bez uprawnień ma miejsce, gdy osoba podejmuje czynności przetwarzania pomimo, że nie jest do tego upoważniona na podstawie przepisów prawa powszechnie obowiązującego, nie otrzymała polecenia lub upoważnienia do ich przetwarzania.

Mając na względzie treść art. 4 pkt 2 RODO, zgodnie z którym przetwarzanie danych osobowych może obejmować różne czynności, w tym: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie, rozpowszechnianie, udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie oraz niszczenie danych osobowych, należy wskazać, że do popełnienia przestępstwa z art. 107 ust. 1 u.o.d.o. wystarczające jest dokonanie bez odpowiedniej podstawy prawnej lub przez osobę nieuprawnioną którejkolwiek z tych czynności.

Spełnienie znamion przestępstwa z art. 107 ust.1 u.o.d.o. wymaga działania sprawcy i nie jest możliwe jego popełnienie przez zaniechanie. Jednocześnie należy podkreślić, że przestępstwo z art. 107 ust. 1 u.o.d.o. ma charakter formalny i do jego zaistnienia nie jest wymagane wystąpienie jakiegokolwiek skutku niezgodnego z prawem przetwarzania danych osobowych (por. B. Kurzępa, Przestępstwa z ustawy o ochronie danych, s. 47). W szczególności nie jest wymagane, żeby przetwarzanie danych osobowych doprowadziło do wystąpienia jakiegokolwiek skutku po stronie osoby, której dane dotyczą, bądź też jakiejkolwiek ingerencji w prywatność tej osoby, poza przetwarzaniem jej danych osobowych (P. Litwinski (red.), Ustawa o ochronie danych osobowych. Komentarz [w:] P. Litwinski (red.) Ogólne rozporządzenie o ochronie danych osobowych.

Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz). Podstawą odpowiedzialności z art. 107 u.o.d.o. jest już sam fakt usiłowania popełnienia określonego w nim przestępstwa.

Zachowanie spenalizowane w art. 107 u.o.d.o. jest przestępstwem powszechnym i może je popełnić każdy, kto nie posiada podstawy prawnej do przetwarzania określonych danych osobowych albo nie jest uprawniony do ich przetwarzania. Należy jednak pamiętać, że zgodnie z zasadami, na których opiera się regulacja polskiego prawa karnego, odpowiedzialność karną za przestępstwo może ponieść wyłącznie osoba fizyczna. Jeżeli dane osobowe są przetwarzane przez podmiot niebędący osobą fizyczną, nie ma możliwości pociągnięcia go do odpowiedzialności karnej. Podmiot taki, nie będzie również ponosił odpowiedzialności za przestępstwo popełnione przez osobę fizyczną działającą w jego imieniu. Zgodnie bowiem z założeniami ustawy z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (t.j. Dz. U. z 2023 r. poz. 659 z późn. zm.), podmiot zbiorowy podlega odpowiedzialności na podstawie ustawy tylko za przestępstwa enumeratywnie wskazane w art. 16 tej ustawy, tymczasem przepis ten nie wymienia przestępstwa z art. 107 ust. 1 u.o.d.o.

Z uwagi na treść art. 18 k.k. odpowiedzialność karną ponosi także ten kto: kieruje przetwarzaniem danych osobowych w sytuacji, gdy nie jest to dopuszczalne lub przetwarzaniem danych osobowych przez osobę nieuprawnioną; ten kto wykorzystując uzależnienie innej osoby od siebie, poleca jej przetwarzanie danych osobowych, gdy nie jest ono dopuszczalne lub, gdy nie ma ona uprawnień do ich przetwarzania oraz ten, kto nakłania lub ułatwia takie przetwarzanie. Początek formularza

Przestępstwo określone w art. 107 u.o.d.o. jest ścigane z urzędu. Podlega ono zatem ściganiu niezależnie od woli pokrzywdzonego. Kwalifikowaną postacią przestępstwa określonego w art. 107 ust. 1 RODO jest przestępstwo uregulowane w ust. 2 tego artykułu, dotyczące bezprawnego przetwarzania danych osobowych, które ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej. Zasady odpowiedzialności za to przestępstwo są takie same jak w

przypadku przestępstwa z art. 107 ust. 2 RODO. Jedną różnicą jest podniesiona do 3 lat górna granica kary pozbawienia wolności, która może być orzeczona za to przestępstwo.

Przestępstwa przeciwko ochronie informacji obejmujących dane osobowe

Art. 107 u.o.d.o. nie jest jedyną podstawą, która pozwala na ściganie niezgodnego z prawem przetwarzania danych osobowych. W niektórych przypadkach podstawę taką mogą stanowić także przepisy k.k. Szczególną uwagę należy zwrócić na treść art. 266 i 267 k.k. Art. 266 § 1 k.k. penalizuje ujawnienie lub wykorzystanie wbrew przepisom ustawy, bądź przyjętemu zobowiązaniu, informacji, z którą sprawca zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową. Z kolei art. 267 § 1 k.k. uznaje za przestępstwo uzyskanie bez uprawnienia dostępu do informacji, która nie była przeznaczona dla sprawcy, poprzez otwarcie zamkniętego pisma, podłączenie się do sieci telekomunikacyjnej lub przełamanie albo ominięcie zabezpieczeń. W przypadku popełnienia każdego z tych przestępstw sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Celem wskazanych przepisów jest zapewnienie ochrony przed nieuprawnionym uzyskaniem, wykorzystywaniem lub ujawnianiem informacji. Oba przepisy mają pełne zastosowanie w sytuacji, gdy informacje będące przedmiotem ich ochrony obejmują dane osobowe. W tym przypadku możliwy jest zbieg z art. 107 ust.1 u.o.d.o.

Warunkiem odpowiedzialności za przestępstwo z art. 266 § 1 k.k. jest istnienie ustawowego obowiązku zachowania przez sprawcę w tajemnicy określonych informacji lub przyjęcie na siebie takiego obowiązku w drodze oświadczenia. Przykładem obowiązku ustawowego może być art. 30a ust. 2 w zw. z ust. 1 Prawa oświatowego z dnia 14 grudnia 2016 r., który stanowi, że nauczyciele oraz inne osoby pełniące funkcje lub wykonujące pracę w szkole są obowiązani do zachowania w poufności informacji uzyskanych w związku z pełnioną funkcją lub wykonywaną pracą, dotyczących zdrowia, potrzeb rozwojowych i edukacyjnych, możliwości psychofizycznych, seksualności, orientacji seksualnej, pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub światopoglądowych uczniów. Przyjęcie zobowiązania do zachowania poufności przetwarzanych danych osobowych może polegać w szczególności na zobowiązaniu się przez pracownika do zachowania w tajemnicy danych osobowych,

z którymi zapozna się on w związku z wykonywaniem obowiązków zawodowych (w niektórych przypadkach zapewnienie, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy jest wymogiem prawnym, por. art. 28 ust. 2 lit. b). Zakres regulacji art. 266 § 1 k.k. obejmuje wyłącznie wykorzystanie lub ujawnienie (udostępnienie) chronionych informacji wbrew zobowiązaniu. Co za tym idzie nie może on być podstawą odpowiedzialności w przypadku podejmowania innych czynności przetwarzania danych osobowych określonych w art. 4 pkt 2 RODO.

Istotą występku spenalizowanego w art. 267 § 1 k.k. jest uzyskanie bez uprawnienia dostępu do informacji, która nie była przeznaczona dla sprawcy, przy czym do popełnienia przestępstwa dochodzi tylko wtedy, gdy sprawca dążąc do uzyskania informacji przełamuje lub omija zabezpieczenia zastosowane w celu ich ochrony. Jeżeli informacje te obejmują dane osobowe to każdorazowo dochodzi do zbiegu z art. 107 ust. 1 lub 2 u.o.d.o., w zakresie w którym przewiduje on karalność przetwarzania danych osobowych przez osobę nieuprawnioną. W tym przypadku zasady wymiaru kary określa art. 11 § 3 w zw. z § 2 k.k.

Przestępstwa określone art. 266 i 267 k.k. są ścigane na wniosek pokrzywdzonego. Co za tym idzie, jeśli pokrzywdzony nie wyrazi woli ścigania sprawcy, organy ścigania nie podejmą w tym zakresie działania. Brak woli pokrzywdzonego nie wyłącza jednak ścigania sprawcy za pozostające w zbiegu przestępstwa z art. 107 u.o.d.o., które w każdym przypadku są ścigane z urzędu.

Na co zwrócić uwagę

Przetwarzanie danych osobowych niezgodnie z zasadami określonymi w RODO może skutkować nałożeniem przez organ nadzorczy dotkliwej kary pieniężnej. Dodatkowo jednak może ono skutkować odpowiedzialnością karną. Należy przy tym pamiętać, że skazanie za przestępstwo oznacza nie tylko konieczność poddania się wymierzonej przez sąd karze, ale skutkuje też utratą przymiotu niekaralności, wymaganego np. do zajmowania niektórych stanowisk. Co przy tym istotne, ściganie, określonego w art. 107 u.o.d.o., przestępstwa niedopuszczalnego przetwarzania danych osobowych lub przetwarzania danych osobowych przez osobę nieuprawnioną następuje z urzędu a do jego popełnienia dochodzi już przez sam fakt niezgodnego z prawem przetwarzania danych osobowych, nawet wtedy, gdy nie skutkuje ono żadnymi negatywnymi konsekwencjami po stronie osoby, której dane dotyczą.

r. pr. Grzegorz Lubeńczuk Zastępca IOD

Zespół Ochrony Danych Osobowych

IV. Kara dla pracodawcy za inwigilację pracowników, czyli krótka historia o tym, o co pracodawca pytać może, a o co pytać nie powinien.

Drodzy Państwo,

Kontynuując serię wpisów RODO w HR, przedstawię dzisiaj pewną ciekawą sprawę związaną z naruszeniem danych osobowych, jaka miała miejsce u jednego z pracodawcy – sieci znanych sklepów H&M.

Na sieć sklepów H&M niemiecki organ nadzorczy nałożył karę – ponad 35 milionów euro, a głównym powodem tak wysokiej kary miała być nieznajdująca w przepisach uzasadnienia ingerencja H&M w dane swoich pracowników, obejmująca również dane dotyczące życia osobistego.

Organ podczas kontroli ustalił, że znaczna część pracowników H&M była poddawana pewnego rodzaju „obserwacji", a wnioski z nich, były dokładnie notowane i przechowywane przez osoby dokonujące tychże obserwacji (przełożonych).
W firmie panowała – jak się wydawało – miła zasada, przeprowadzania z pracownikami, czy to po urlopie, czy to po nieobecności z powodu choroby, rozmów powitalnych. Rozmowy takie pracownik przeprowadzał ze swoim przełożonym.

Miały one zawsze przebieg grzecznościowy, w luźnej atmosferze i wydawały się nie być w żaden sposób zobowiązujące. Pracownicy mieli wrażenie troski ze strony pracodawcy.

Jak się jednak okazało, przedmiotem rozmów była nie tyle miła, koleżeńska pogawędka o wakacjach, czy o stanie samopoczucia po przebytej chorobie, ale też ustalenie szczegółów, takich jak np. kosztów podróży, liczby uczestników urlopu, objawów choroby, diagnozy lekarskiej itp. Niejednokrotnie rozmowy obejmowały także sytuację rodzinną pracowników, przekonania religijne czy polityczne.
Co bardziej zaskakujące, dane z rozmów były dokładnie notowane i przechowywane, a dostęp do nich miała dość duża kadra kierownicza firmy (szacuje się, że około 50 osób). Notatki, według przeprowadzonej przez organ kontroli, były szczegółowe i przechowywane bez ustalenia terminu końcowego, co z kolei umożliwiało przełożonym „pisanie dalszej historii", czyli dopisywanie dalszych wątków.

Obserwowano na przykład czy pracownik, który miał problemy rodzinne, rozwiązał je, czy też doszło do rozwodu, podziału władzy rodzicielskiej, utraty dzieci, a w konsekwencji jaki jest stan psychiczny pracownika.
Po co takie dane były gromadzone? Jak się wyjaśniło na etapie postępowania kontrolnego, wykorzystywano je do bardzo szczegółowej oceny pracownika (jego wydajności, możliwości zaangażowania), ale też i analizy co do dalszej kariery (czy dany pracownik nadaje się np. na stanowisko kierownicze).

Organ nadzorczy w trakcie kontroli uznał, że doszło do szczególnie poważnego naruszenia praw pracowników sieci H&M.
Kto o tym doniósł?
To był zupełny przypadek. Dane przechowane były jako notatki w systemie i z powodu błędu tego systemu, folder został udostępniony wszystkim pracownikom. Sprawą zainteresowała się prasa, a organ wszczął postepowanie na skutek tych właśnie informacji.
Firma współpracowała z organem, nie utrudniła kontroli i udostępniła wszystkie zebrane dane.
Po przeprowadzonej kontroli przyznała się do popełnionego błędu i zagwarantowała wdrożenie całego systemu naprawczego ochrony danych swoich pracowników. Przełożeni przeprosili pracowników i podjęto rozmowy w przedmiocie wypłaty zadośćuczynienia.

Mimo że RODO wprost przewiduje, że administracyjna kara pieniężna, która grozi za naruszenie kluczowych przepisów RODO może sięgać 20 000 000 euro, a w przypadku przedsiębiorstwa nawet 4% jego całkowitego rocznego światowego obrotu, to kary przekraczające pułap 20 milionów zawsze wywołują duże emocje, tym bardziej, że są rzadkie.

Reasumując
Muszę przyznać, że chyba w swoim kilkuletnim doświadczeniu w ochronie danych osobowych, nie spotkałam się z tak daleko idącym i jawnym naruszeniem przepisów RODO.
Pracodawca naruszył fundamentalne zasady przetwarzania danych. Brak było podstaw prawnych do przetwarzania danych osobowych, brak było zachowania jakiejkolwiek rozliczalności przetwarzanych danych. Naruszone zostały dobra osobiste pracowników oraz ich konstytucyjne prawo do prywatności.

Powyższą historię przedstawiam Państwu jako ciekawostkę, ale wyciągnąć z niej można kilka ważnych, tak myślę przynajmniej, wniosków.

Szanujmy dane osobowe i prywatność innych.

Zbierajmy tylko te dane, które są konieczne, tym bardziej, że nigdy nie wiemy, kiedy zainicjowana zostanie kontrola (choćby wskutek błędów techniki, a nie koniecznie wskutek skargi człowieka),

I ostatni – podawajmy innym nasze dane ostrożnie. Bo przecież dane osobowe każdego z nas są przetwarzane z jakiegoś powodu.

adw. Justyna Cybulska
Zastępca IOD
Zespół Ochrony Danych Osobowych

JUSTYNA JABŁONKA

KANCELARIA WYRZYKOWSCY

Inspektor Ochrony Danych,
adw. Justyna Jabłonka

www.justynajablonka.pl
www. kancelariawyrzykowscy.pl

BLOG dla JST:
https://kancelariawyrzykowscy.pl/pl/blog-jst/
FB:
https://www.facebook.com/kancelariawyrzykowscy