Jak przygotować się do kontroli

RODO PORADNIK

Dla przedsiębiorców

Spis treści

Patron poradnika

ODO 24 sp. z o.o. oferuje kompleksowe rozwiązania w zakresie ochrony danych osobowych i bezpieczeństwa informacji. Dzięki doświadczonemu zespołowi ekspertów z dziedziny m.in. prawa, informatyki, zarządzania kryzysowego oraz ciągłości działania dostarcza organizacjom praktyczne rozwiązania, pozwalające skutecznie zabezpieczyć posiadane zasoby informacyjne.

Autorzy poradnika

Damian Gąska – audytor i konsultant w obszarze bezpieczeństwa informacji. Zajmuje się weryfikacją infrastruktury informatycznej, wykonuje testy i audyty bezpieczeństwa, tworzy procedury oraz dokumentacje. Przeprowadza analizy incydentów naruszenia bezpieczeństwa usług i procesów biznesowych. Specjalizuje się w bezpieczeństwie usług w chmurze obliczeniowej (ISO/IEC 27017) oraz zarządzaniu ryzykiem (ISO 31000). Posiada certyfikat „Bezpieczeństwo sieci komputerowych".

Agata Kłodzińska – aplikant adwokacki. Swoje zainteresowania koncentruje na prawie nowych technologii i prawie medycznym, w szczególności w kontekście zagadnień związanych z ochroną danych osobowych. W ODO 24 zajmuje się przeprowadzaniem audytów, prowadzeniem projektów wdrożeniowych, tworzeniem dokumentacji związanej z przetwarzaniem danych osobowych oraz doradztwem prawnym. Audytor wiodący systemu zarządzania bezpieczeństwem informacji (ISO/IEC 27001).

Barbara Matasek – doktorant w Kolegium Prawa Akademii Leona Koźmińskiego w Warszawie. Swoje zainteresowania skupia wokół prawa handlowego i prawa cywilnego, ze szczególnym uwzględnieniem zagadnień dotyczących ochrony danych osobowych. Doświadczenie zawodowe zdobywała podczas pracy w kancelariach prawnych oraz jako asystent sędziego. Odpowiada za przeprowadzanie audytów, przygotowanie dokumentacji w zakresie ochrony danych osobowych oraz doradztwo prawne.

Ilustracje Karol Banach (karolbanach.com)

Projekt i skład Radosław Zbytniewski (zbytniewski.pl)

Redakcja i korekta Ewa Walewska

ISBN: 978-83-943435-7-6

Wydanie I – Warszawa, październik 2019 r.

Wstęp

Ogólne rozporządzenie o ochronie danych (RODO) obowiązuje już kolejny rok. Wydawać by się mogło, że po takim czasie emocje, które początkowo towarzyszyły stosowaniu nowych przepisów, już dawno opadły, a praktyka związana z wdrożeniem RODO i utrzymaniem systemu ochrony danych osobowych, wymiana doświadczeń między przedsiębiorcami oraz bieżące wskazówki Urzędu Ochrony Danych Osobowych (UODO) zaprowadziły porządek i harmonię. Nic bardziej mylnego. Po okresie względnego spokoju UODO ruszył z ofensywą, rozpoczynając kontrole przedsiębiorców, a nawet nakładając pierwsze kary, w tym jedną w wysokości niemal miliona złotych.

Tymczasem trwały prace nad nowelizacją przepisów sektorowych, której celem było dostosowanie ich do RODO (zmiany, które ostatecznie objęły 162 ustawy, weszły w życie 4 maja 2019 r.). Dodatkowo UODO wydał poradniki mające rozjaśnić najbardziej niezrozumiałe kwestie (w tym poradnik „Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców"), opublikował instrukcje i opinie w zakresie stosowania przepisów RODO w praktyce, zorganizował konferencje i szkolenia (m.in. dla inspektorów ochrony danych). Mimo to obowiązujące przepisy nadal powodują dużą niepewność i pozostawiają szerokie pole do interpretacji, przez co mało która organizacja może spać spokojnie. To, czym dysponujemy na tę chwilę, zdecydowanie nie pozwala czuć się bezpiecznie. W obliczu grożących kar trudno dziwić się tej atmosferze strachu i niepewności.

CO ZNAJDZIESZ W NASZYM PORADNIKU?

W Twoje ręce przekazujemy materiał, który – mamy nadzieję – **rozwieje wątpliwości**, które nagromadziły się przy codziennym stosowaniu RODO i przepisów sektorowych. Pomoże on **skorygować błędy czy niedociągnięcia**, które mogą pojawić się w procesach przetwarzania danych osobowych w Twojej organizacji, a przede wszystkim – **przygotować się do ewentualnej kontroli** Prezesa UODO. Podręcznik jest skierowany do inspektorów ochrony danych, koordynatorów ds. ochrony danych oraz właścicieli procesów, a także wszystkich osób odpowiedzialnych za respektowanie przepisów RODO i nadzorowanie operacji przetwarzania danych osobowych.

W pierwszej części poradnika omawiamy kluczowe i przede wszystkim praktyczne kwestie związane z kontrolą przeprowadzaną przez pracowników UODO, w tym: kiedy kontrola może zostać wszczęta, jak przygotować się do wizyty kontrolerów, jakie dokumenty przedstawić, jakie prawa przysługują kontrolowanym i jakie obowiązki się z tym wiążą. **Druga część** poradnika obejmuje omówienie najważniejszych i najczęściej występujących procesów przetwarzania danych. Poruszane zagadnienia poprowadzą Cię krok po kroku w kierunku zapewnienia zgodności tych procesów z RODO, ze szczególnym uwzględnieniem aspektów, które zazwyczaj przysparzają administratorom najwięcej problemów. Natomiast **w ostatniej, trzeciej części** tłumaczymy, jak dostosować organizację do wymogów RODO, tak aby być przygotowanym na ewentualną kontrolę UODO od strony zabezpieczeń fizycznych, technicznych i organizacyjnych, w tym szeroko pojętych kwestii IT.

Mamy nadzieję, że nasz poradnik pomoże Ci dostosować procesy i zabezpieczenia do wymogów RODO, a wiedza, którą dzięki niemu nabędziesz, usprawni system ochrony danych osobowych w Twojej organizacji tak, że żadna kontrola organu nie będzie Ci straszna.

I CZĘŚĆ. KONTROLA UODO

Prezes UODO jako organ uprawniony do przeprowadzania kontroli

Wraz z rozpoczęciem stosowania RODO – od 25 maja 2018 r. – na mocy art. 51 ust. 1 (który nakazuje, by za monitorowanie stosowania RODO odpowiadał co najmniej jeden niezależny organ nadzorczy) Prezes UODO zastąpił funkcjonującego przez ponad 20 lat Generalnego Inspektora Ochrony Danych Osobowych. Aby skutecznie realizować swoje zadania, Prezes UODO został wyposażony w szereg narzędzi i uprawnień (o których mowa przede wszystkim w art. 58 RODO), w tym możliwość:

- **nałożenia administracyjnej kary pieniężnej (w wysokości do 20 milionów euro lub do 4% rocznego światowego obrotu),**
- **wprowadzenia czasowego lub całkowitego zakazu przetwarzania danych osobowych,**
- **nakazania usunięcia danych,**
- **wydania upomnienia,**
- **nakazania poinformowania osoby, której dane dotyczą, o naruszeniu ochrony jej danych,**
- **uzyskania wszelkich informacji potrzebnych organowi nadzorczemu do realizacji swoich zadań,**
- **zawiadomienia administratora lub podmiotu przetwarzającego o podejrzeniu naruszenia RODO.**

Ponadto ustawa o ochronie danych osobowych (u.o.d.o.) w art. 78 ust. 1 stanowi, że Prezes UODO przeprowadza kontrolę przestrzegania przepisów o ochronie danych osobowych, która – zgodnie z art. 58 ust. 1 lit. b RODO – może przybrać postać audytu ochrony danych.

Rodzaje kontroli

Wyróżniamy dwa główne rodzaje kontroli (art. 78 ust. 2 u.o.d.o.):

- **kontrolę planową – na podstawie zatwierdzonego planu kontroli organu nadzorczego,**
- **kontrolę doraźną – na podstawie informacji uzyskanych przez Prezesa UODO.**

Dodatkowo organ nadzorczy może przeprowadzić kontrolę w ramach monitorowania przestrzegania RODO (tzw. kontrola wyrywkowa, zależna od swobodnego wyboru Prezesa UODO).

Kontrola planowa odbywa się na podstawie rocznego planu kontroli sektorowych na dany rok, publikowanego przez UODO. Może ona dotyczyć wybranej kategorii podmiotów lub zagadnień. W 2019 r. kontrolami planowymi objęto:

- **sektor prywatny w zakresie telemarketingu, profilowania,**
- **sektor bankowy i ubezpieczeniowy,**
- **działalność brokerów danych.**

W planowanych działaniach kontrolnych zwrócono również uwagę na aspekt prowadzenia monitoringu wizyjnego przez pracodawców, placówki oświatowe i szkoły, a także podmioty udzielające świadczeń zdrowotnych w zakresie prowadzonej dokumentacji medycznej. Plan kontroli objął także sektor publiczny, ze szczególnym uwzględnieniem organów ścigania i sądów.

Drugi rodzaj kontroli, czyli tzw. **kontrola doraźna**, ma swoje źródło w informacjach pozyskanych przez Prezesa UODO lub wynika z monitorowania zgodności z RODO. Przykładowo kontrola może zostać wszczęta w wyniku skargi osoby fizycznej (lub niepokojąco dużej liczby takich skarg) na niezgodne z prawem przetwarzanie danych osobowych przez administratora. Podobne w skutkach może być regularne zgłaszanie przez administratorów naruszeń ochrony danych osobowych – jako jasny sygnał, że skoro naruszenia są w danej organizacji na porządku dziennym, to system ochrony danych osobowych może w niej funkcjonować nie do końca prawidłowo. W szczególnym przypadku kontrolę doraźną może spowodować głośna sprawa medialna, dotycząca np. podejrzenia wycieku danych. Tak było w przypadku szpitala w Hadze, gdzie zbyt szerokie grono personelu medycznego zapoznało się z dokumentacją medyczną leczonej tam celebrytki, a tym samym pozyskało informację o przedawkowaniu przez nią narkotyków i próbie samobójczej. Holenderski organ nadzorczy na skutek wszczętego postępowania nałożył na szpital karę w wysokości niemal 2 milionów złotych za niewłaściwe zabezpieczenie danych pacjentów.

W powyższego wynika, że nawet gdy roczny plan kontroli zatwierdzony przez Prezesa UODO nie dotyczy naszej działalności, nie oznacza to, że możemy głęboko odetchnąć i wykluczyć możliwość wszczęcia kontroli właśnie w naszej organizacji.

Kary pieniężne nakładane przez Prezesa UODO

WIĘCEJ

Jednym z celów reformy przepisów o ochronie danych była poprawa skuteczności egzekwowania przepisów. Uznano, że zagrożenie w postaci wysokiej kary pieniężnej będzie skutkować wzrostem poszanowania przepisów, nakładanie kar zaś będzie stanowić środek zniechęcający innych do ich naruszania. Wydaje się, że cel ten osiągnięto.

Przede wszystkim podkreślenia wymaga, że decyzja administracyjna (lub postanowienie) Prezesa UODO dotycząca ukarania administratora (podmiotu przetwarzającego), stwierdzenia naruszenia itp. nie zawsze musi być następstwem przeprowadzonej wcześniej kontroli zgodności przetwarzania danych osobowych przez organizację z przepisami o ochronie danych osobowych. Można ukarać podmiot bez kontroli. I odwrotnie – kontrola może zakończyć się bez wszczynania postępowania administracyjnego z uwagi na brak uprawdopodobnienia naruszenia ochrony danych w toku kontroli. Najczęściej jednak wszczęcie postępowania administracyjnego będzie skutkiem przeprowadzonej kontroli.

Do czasu wydania tego poradnika UODO opublikował na swojej stronie internetowej (www.uodo.gov.pl) w zakładce „Prawo" łącznie 133 decyzje administracyjnye, z czego trzy o nałożeniu administracyjnej kary pieniężnej. Warto wskazać, że znaczna część tych decyzji dotyczy trzech obszarów:

- **podstaw prawnych przetwarzania,**
- **realizacji praw osób, których dane dotyczą,**
- **udostępnienia danych osobowych.**

Niektóre z tych decyzji nadal nie są prawomocne, natomiast analiza stanu faktycznego oraz (w niektórych przypadkach) stwierdzone naruszenia po stronie administratorów i dokładne przyjrzenie się charakterowi przewinienia pozwolą zidentyfikować kwestie, na które kładziony jest szczególny nacisk, stanowiące główny przedmiot zainteresowania UODO.

Warto odnotować, że art. 73 u.o.d.o. określa, że po zakończeniu postępowania organ, jeśli uzna, że przemawia za tym interes publiczny, może poinformować o wydaniu decyzji na swojej stronie w Biuletynie Informacji Publicznej. Oznacza to, że pełne wyniki postępowania w sprawie naruszenia przepisów o ochronie danych osobowych mogą być dostępne publicznie.

Przykładowe postępowania i kary

WIĘCEJ

MILION ZA NIEZGODNOŚĆ

Prezes UODO na podstawie ustaleń poczynionych w toku kontroli ukarał warszawską spółkę tworzącą bazy danych przedsiębiorców, oparte na ogólnodostępnych źródłach, takich jak CEiDG, KRS czy GUS. Powód? Niespełnienie obowiązku informacyjnego w stosunku do osób prowadzących jednoosobowe działalności gospodarcze (JDG), których dane znalazły się w bazach ukaranej spółki. Sprawa byłaby oczywista, gdyby spółka nie podjęła żadnych działań zmierzających do spełnienia obowiązku informacyjnego. W przywołanej sytuacji istotny natomiast jest fakt publikacji stosownej klauzuli na stronie i masowa wysyłka mailowa z informacjami na temat przetwarzania danych (do wszystkich osób, których adresami e-mail spółka dysponowała – w liczbie ok. 680 tysięcy rekordów). Wskazuje to jasno, że administrator podjął pewne, choć zdaniem UODO niewystarczające kroki w kierunku zapewnienia zgodności z RODO. W tej sprawie UODO dokonał interpretacji pojęcia niewspółmiernie dużego wysiłku, stwierdzając, że wysyłka ok. 6 milionów listów poleconych (bo w odniesieniu do tylu osób spółka dysponowała wyłącznie adresem prowadzenia działalności) takim niewspółmiernie dużym wysiłkiem wcale nie jest, gdyż nie chodzi o skalę wysiłku dla podmiotu, a raczej o wysiłek związany z jednostkowym poinformowaniem osoby. Przykładowo niewspółmiernie dużym wysiłkiem byłoby ustalanie adresów kontaktowych osób, które podały jedynie imię, nazwisko i numer PESEL, bez adresu zamieszkania, korespondencji czy numerów telefonów.

Powyższe pozwala wysnuć wniosek, że UODO przywiązuje szczególną wagę do spełniania obowiązku informacyjnego, a nałożenie tak surowej kary należy odczytywać jako przestrogę dla organizacji, które często z wygody czy nadmiernych oszczędności część obowiązków wynikających z RODO traktują po macoszemu. Tak wysoka kara (a intencją unijnego ustawodawcy było przecież ustanowienie kar „skutecznych i odstraszających") każe każdemu dobrze się zastanowić, zanim zrezygnuje z realizacji obowiązku informacyjnego, nawet gdyby chodziło o najbardziej problematyczne przypadki.

NIEUPRAWNIONE UJAWNIENIE DANYCH WARTE 55 TYSIĘCY ZŁOTYCH

Powodem nałożenia przez Prezesa UODO drugiej z kar pieniężnych były nieskuteczne próby usunięcia naruszenia polegającego na upublicznieniu zbyt szerokiego zakresu danych osobowych. W omawianej sprawie

jeden ze związków sportowych opublikował na swojej stronie internetowej dane osobowe sędziów, którym przyznano licencje sędziowskie. W takim działaniu nie byłoby nic niewłaściwego, gdyby nie fakt, że wśród upublicznionych danych osobowych oprócz imion i nazwisk sędziów znalazły się również ich adresy zamieszkania oraz numery PESEL. Jak wskazuje UODO, taka sytuacja stworzyła potencjalne ryzyko bezprawnego wykorzystania danych osobowych, np. do podszycia się pod osoby, których te dane dotyczą, w celu tworzenia tzw. kolekcjonerskich dokumentów tożsamości, by za ich pomocą zaciągać pożyczki i inne zobowiązania.

Przy ustalaniu wysokości kary organ nadzorczy wziął pod uwagę m.in. czas trwania naruszenia oraz to, że dotyczyło ono 585 osób (sędziów). Okolicznością łagodzącą była dobra współpraca administratora z organem nadzorczym, brak dowodów na powstanie szkody po stronie osób, których dane dotyczyły, a także to, że związek sam dostrzegł swój błąd i zgodnie z RODO zgłosił naruszenie Prezesowi UODO. Pomimo tych działań nieskuteczne próby usunięcia naruszenia przesądziły o nałożeniu kary.

Mimo że postępowanie w tej sprawie nie było wynikiem przeprowadzonej kontroli, to przypadek ten jest bezcenną lekcją dla każdego administratora i podmiotu przetwarzającego, że należy dokładnie upewniać się, czy naruszenie ochrony danych zostało skutecznie naprawione.

WIĘCEJ

MORELE.NET I PRAWIE 3 MILIONY ZŁOTYCH KARY ZA NIEWYSTARCZAJĄCE ZABEZPIECZENIA

Największa z nałożonych dotychczas kar to skutek naruszenia w postaci uzyskania nieuprawnionego dostępu do bazy danych klientów Morele.net. Podczas postępowania administracyjnego organ nadzorczy stwierdził, że wśród danych wykradzionych z Morele.net znajdowały się imiona, nazwiska, numery telefonw i adresy do doręczeń (które posłużyły potem do ataków phishingowych), dotyczące ok. 2,2 mln osób. Natomiast w przypadku 35 tys. osób zakres wykradzionych danych był znacznie szerszy. Dane pochodziły z ich wniosków ratalnych i obejmowały m.in. nr PESEL, serię i nr dokumentu tożsamości.

Zdaniem Prezesa UODO zastosowane przez Morele.net środki organizacyjne i techniczne ochrony danych osobowych nie były adekwatne do istniejącego ryzyka, czym spółka naruszyła m.in. określoną w art. 5 ust. 1 lit. f RODO zasadę poufności. Jako nieskuteczne określono środek uwierzytelniania dostępu do danych oraz system „monitorowania sieciowego" organizacji, przede wszystkim z uwagi na brak odpowiednich procedur reagowania na wypadek pojawienia się nietypowego ruchu w sieci.

INNE DECYZJE PREZESA UODO – CZEGO MOŻEMY SIĘ Z NICH DOWIEDZIEĆ O KONTROLACH?

Decyzje Prezesa UODO nie dotyczą jednak wyłącznie kar nakładanych na podmioty, które przetwarzają dane, ale również np. odmowy uwzględnienia wniosków skarżących o realizację praw przysługujących im na gruncie RODO, nakazania administratorom określonego zachowania (np. realizacji wniesionych żądań praw osób fizycznych) czy umorzenia postępowania. Spośród mających największe przełożenie na codzienne funkcjonowanie organizacji z wydanych dotychczas decyzji można wyróżnić dwie:

- **decyzję dotyczącą sposobu realizacji prawa dostępu do danych, w której Prezes UODO wskazuje, że zgodnie z art. 15 ust. 3 RODO udostępnienie kopii danych zawartych w dokumentach (np. w pismach urzędowych) nie jest równoznaczne z obowiązkiem udostępnienia kopii dokumentów.** Administrator nie ma bowiem obowiązku udostępniania osobie zainteresowanej nośnika, na którym przetwarzane są dane osobowe, oraz danych, które nie stanowią danych osobowych. Realizując to prawo, administrator może poprzestać na wskazaniu treści danych dotyczących osoby, z wyłączeniem pozostałych informacji zawartych na nośniku (decyzja z 22 marca 2019 r., sygn. akt: ZSZZS.440.660.2018);
- **decyzję, w której poruszono kwestię zasady rozliczalności w kontekście przekazania informacji o przetwarzaniu danych. Organ nadzorczy uznał, że samo potwierdzenie nadania listu zwykłego zawierającego treść klauzuli informacyjnej nie jest wystarczającym dowodem na to, że osoba została skutecznie poinformowana** – administrator powinien dysponować zwrotnym potwierdzeniem odbioru lub innym dokumentem potwierdzającym odbiór korespondencji przez osobę, której dane przetwarza (decyzja z 12 grudnia 2018 r., sygn. akt: ZSPR.440.195.2018). W tym miejscu trzeba jednak podkreślić, że komentowana decyzja dotyczyła interpretacji art. 105a ust. 3 ustawy – Prawo bankowe, natomiast zdecydowanie rzutuje ona również na interpretację słowa „podaje" użytego w art. 13 i 14 RODO. Kwestia ta nie jest jednoznaczna, ponieważ w uzasadnieniu decyzji, w której nałożono milion złotych kary, organ zaznacza, że realizacja obowiązku informacyjnego przez przesłanie stosownych informacji listem poleconym to nie jedyne możliwe rozwiązanie.

ABC kontroli

Niniejsza część poświęcona kontroli ma za zadanie przybliżyć to, jak organ nadzorczy przeprowadza kontrole, jakie zagadnienia są przedmiotem jego szczególnego zainteresowania, jak w możliwie przystępny sposób pozyskać podstawowe informacje związane z praktycznymi aspektami kontroli, a także jak się do niej przygotować oraz czego się spodziewać. Bazując na dotychczasowym doświadczeniu ODO 24, prezentujemy odpowiedzi na najczęściej zadawane pytania oraz wskazówki, które pomogą przejść proces kontroli jak najsprawniej.

CZY UODO INFORMUJE O PLANOWANEJ KONTROLI?

Co do zasady organ powinien poinformować o planowanej kontroli. Nie mówi nic o tym RODO, natomiast wynika to z ustawy – Prawo przedsiębiorców (p.p.). Zgodnie z art. 48 ust. 1 p.p. organ przystępujący do kontroli zawiadamia przedsiębiorcę o zamiarze wszczęcia kontroli. Najczęściej takie zawiadomienie przyjmuje formę pisemną, choć organ nadzorczy dodatkowo kontaktuje się w tej sprawie telefonicznie, aby kontrola przebiegła jak najsprawniej. Samo wszczęcie kontroli powinno zaś nastąpić nie wcześniej niż po upływie 7 dni i nie później niż przed upływem 30 dni od dnia doręczenia zawiadomienia (art. 48 ust. 2 p.p.).

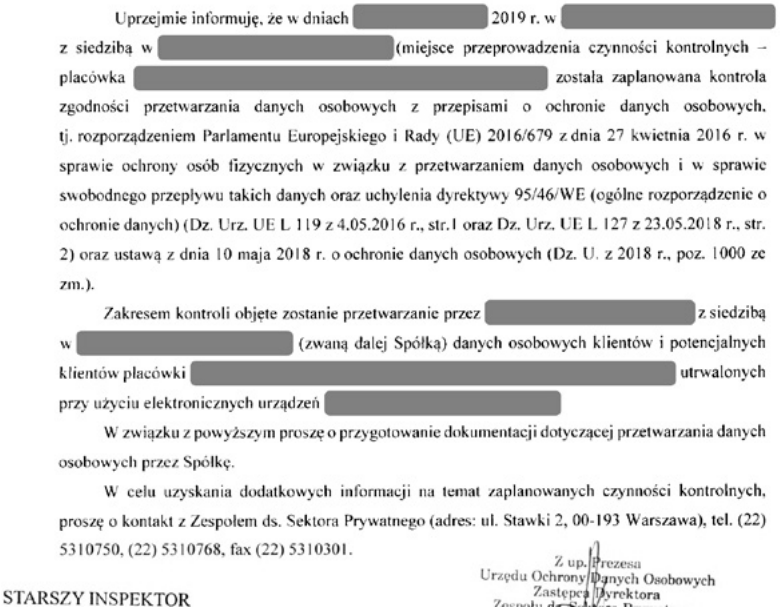
Art. 48 ust. 11 p.p. określa wszystkie dozwolone wyjątki, gdy nie zawiadamia się o kontroli. Obejmują one przykładowo następujące sytuacje:

- **przeprowadzenie kontroli jest niezbędne dla przeciwdziałania popełnieniu przestępstwa lub wykroczenia, przeciwdziałania popełnieniu przestępstwa skarbowego lub wykroczenia skarbowego lub zabezpieczenia dowodów jego popełnienia,**
- **przedsiębiorca nie ma adresu zamieszkania lub adresu siedziby lub doręczanie pism na podane adresy było bezskuteczne lub utrudnione.**

SKĄD WIADOMO, JAKI OBSZAR BĘDZIE PRZEDMIOTEM KONTROLI?

Zakres kontroli, którym objęte zostanie przetwarzanie danych osobowych w danej organizacji, najczęściej jest wskazany w treści zawiadomienia o kontroli. Zazwyczaj możemy liczyć na ogólne wskazanie procesu, który ma zostać poddany kontroli, np. przetwarzanie danych osobowych pracowników, proces związany z marketingiem czy monitoring stosowany przez organizację. Równie dobrze przedmiot kontroli może dotyczyć całości czynności przetwarzania podejmowanych przez organizację albo pewnego aspektu rozpatrywanego w ramach kilku (lub wszystkich) procesów przetwarzania (np. prowadzenie monitoringu wizyjnego w organizacji czy realizacja obowiązku informacyjnego). Warto skontaktować się z urzędnikiem, żeby spróbować pozyskać bardziej precyzyjne informacje w tym zakresie (numer telefonu powinien zostać podany w treści zawiadomienia).

WIĘCEJ



Uprzejmie informuję, że w dniach [redacted] 2019 r. w [redacted] z siedzibą w [redacted] (miejsce przeprowadzenia czynności kontrolnych – placówka [redacted] została zaplanowana kontrola zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, tj. rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016 r., str.1 oraz Dz. Urz. UE L 127 z 23.05.2018 r., str. 2) oraz ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000 ze zm.).

Zakresem kontroli objęte zostanie przetwarzanie przez [redacted] z siedzibą w [redacted] (zwaną dalej Spółką) danych osobowych klientów i potencjalnych klientów placówki [redacted] utrwalonych przy użyciu elektronicznych urządzeń [redacted]

W związku z powyższym proszę o przygotowanie dokumentacji dotyczącej przetwarzania danych osobowych przez Spółkę.

W celu uzyskania dodatkowych informacji na temat zaplanowanych czynności kontrolnych, proszę o kontakt z Zespołem ds. Sektora Prywatnego (adres: ul. Stawki 2, 00-193 Warszawa), tel. (22) 5310750, (22) 5310768, fax (22) 5310301.

Z up. Prezesa
Urzędu Ochrony Danych Osobowych
Zastępca Dyrektora

STARSZY INSPEKTOR

Drugim dokumentem, z którego wynika, jakie zagadnienia zostaną poddane sprawdzeniu przez kontrolerów, jest imienne upoważnienie pracownika UODO.

Uwaga: Zakres kontroli nie może wykraczać poza zakres wskazany w upoważnieniu.

Typowe upoważnienie do kontroli obejmuje ustalenie:

- **podstaw prawnych przetwarzania danych osobowych,**
- **źródeł pozyskiwania danych,**
- **kategorii osób, których dane dotyczą, oraz kategorii przetwarzanych danych osobowych,**
- **celów, w jakich dane są przetwarzane,**
- **odbiorców, którym dane są ujawniane, oraz szczegółów udostępniania (podstawy prawnej, celu, zakresu i sposobu),**
- **sposobu spełnienia obowiązku informacyjnego,**
- **sposobu realizacji praw osób, których dane dotyczą,**
- **zasad powierzenia przetwarzania,**
- **upoważnień do przetwarzania danych,**
- **wdrożenia polityk i procedur ochrony danych (w tym ich formalnego obowiązywania oraz świadomości i przeszkolenia członków personelu),**
- **czy wyznaczono inspektora ochrony danych,**
- **czy dane osobowe nie są przechowywane przez zbyt długi okres,**
- **czy wdrożono środki techniczne i organizacyjne, aby zapewnić odpowiedni stopień bezpieczeństwa danych,**
- **czy prowadzony jest rejestr czynności przetwarzania oraz rejestr wszystkich kategorii czynności przetwarzania,**
- **czy odpowiednio dokumentowane są wszystkie naruszenia ochrony danych.**

Wskazówka: UODO ostrzega przed fałszywymi kontrolerami, dlatego warto zweryfikować legitymację kontrolujących, zanim przystąpią oni do działań kontrolnych. Legitymacja zawiera m.in. informacje o imieniu, nazwisku, stanowisku służbowym oraz fotografię. W razie wątpliwości co do wiarygodności osoby podającej się za kontrolera UODO zachęca do telefonicznego zweryfikowania, czy rzeczywiście jest ona tą, za którą się podaje, i czy jest upoważniona przez Prezesa UODO do przeprowadzenia kontroli. Zalecamy, aby ze względów bezpieczeństwa zawsze telefonicznie potwierdzić kontrolę, gdyż zdarzały się przypadki, że złodzieje podszywali się pod kontrolerów. Sama legitymacja i upoważnienie nie są wystarczającym zapewnieniem.

Ze wzorem legitymacji możesz zapoznać się pod adresem: https://uodo.gov.pl/pl/131/463 (dostęp: 12.09.2019 r.).

JAKI JEST SKŁAD ZESPOŁU PRZEPROWADZAJĄCEGO KONTROLĘ?

Najczęściej kontrola jest przeprowadzana w składzie kilkuosobowym: w większych organizacjach trzy osoby, w mniejszych dwie osoby, przy czym jeden z kontrolerów odpowiada za obszar prawny, a drugi – za kwestie zabezpieczeń technicznych, fizycznych i organizacyjnych, w tym szeroko pojęte zagadnienia związane z IT. W przypadku dość dużych organizacji albo skomplikowanych zagadnień kontrolę mogą przeprowadzać dwa zespoły kontrolujące – każdy po trzy osoby. Bywają też kontrole jednoosobowe – odbywają się one przeważnie wtedy, gdy przedmiotem kontroli są kwestie wyłącznie prawne.

JAK DŁUGO TRWAJĄ CZYNNOŚCI KONTROLNE?

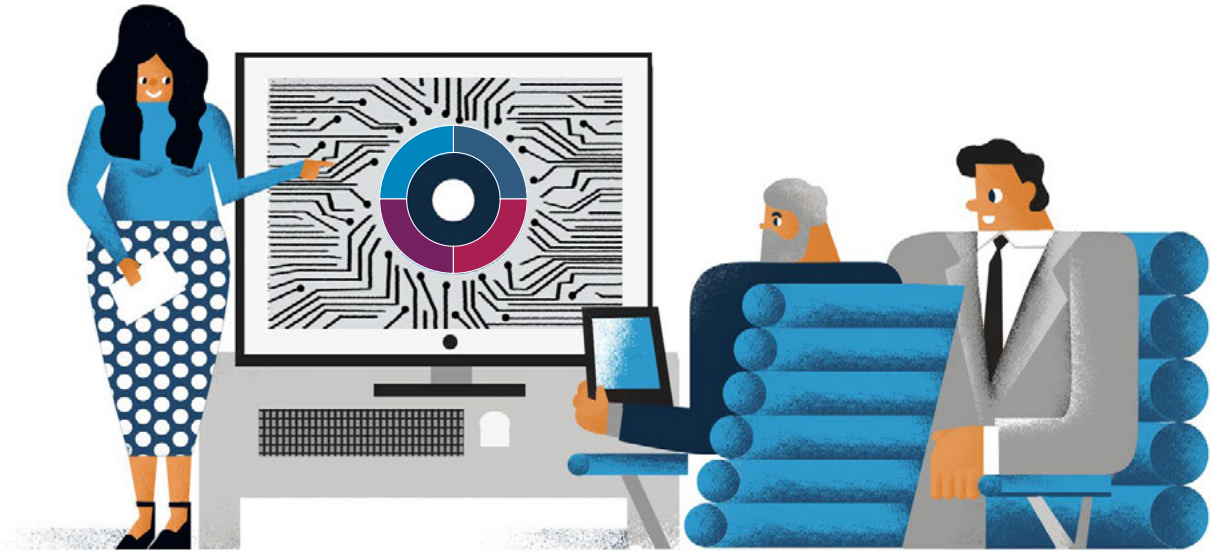
Zgodnie z art. 89 u.o.d.o. cała kontrola ma trwać nie dłużej niż 30 dni od dnia okazania kontrolowanemu upoważnienia do przeprowadzenia kontroli. Faktycznie na miejscu kontrola może trwać dzień do kilku dni. Pozostałe czynności odbywają się już telefonicznie, mailowo i korespondencyjnie.

Za termin zakończenia kontroli uznaje się dzień podpisania protokołu kontroli przez kontrolowanego (albo dzień dokonania wzmianki w protokole, że kontrolowany odmówił podpisania protokołu).

KTO POWINIEN BYĆ OBECNY PRZY KONTROLI PO STRONIE KONTROLOWANEGO?

Kontrola powinna być przeprowadzana co do zasady w obecności kontrolowanego (a raczej przedstawiciela reprezentującego go organu, np. zarządu) lub osoby przez niego upoważnionej, tj. posiadającej pełnomocnictwo. W pełnomocnictwie należy wyszczególnić dokładnie umocowanie osoby, zwłaszcza wskazać, że jest umocowana do podpisania protokołu kontroli w imieniu podmiotu kontrolowanego. Pełnomocnictwo powinno mieć formę pisemną. Osoba legitymująca się nim musi liczyć się z tym, że kontrolujący mogą żądać jego okazania.

Jeśli w organizacji powołano inspektora ochrony danych, będzie on najodpowiedniejszą osobą do wsparcia przy kontroli. Ale uwaga – inspektor ochrony danych powinien zostać do tego upoważniony przez kierownictwo. Samo bycie inspektorem ochrony danych takim upoważnieniem nie jest.



WIĘCEJ

JAKIE UPRAWNIENIA PRZYSŁUGUJĄ KONTROLEROWI UODO? JAKIE OBOWIĄZKI CIĄŻĄ NA KONTROLOWANYM?

Co do zasady czynności kontrolne podejmowane przez pracowników UODO polegają na:

- **wywiadzie osobowym,**
- **wizji lokalnej,**
- **ocenie dokumentacji ochrony danych osobowych funkcjonującej w kontrolowanej organizacji (np. rejestrów czynności przetwarzania, listy podmiotów przetwarzających, przyjętych polityk i procedur, stosowanych kodeksów) oraz sprawdzeniu funkcjonowania przyjętych przez organizację procedur w praktyce.**

W ramach prowadzonych czynności kontrolnych kontrolujący ma prawo (art. 84 ust. 1 u.o.d.o.):

- **wstępu od 6:00 do 22:00 na teren organizacji oraz do jej budynków, lokali i innych pomieszczeń,**
- **wglądu do dokumentów mających bezpośredni związek z przedmiotem kontroli,**
- **przeprowadzenia oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych,**
- **żądania złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwania świadków (np. pracowników kontrolowanego),**
- **zlecania sporządzenia ekspertyz i opinii.**

Uprawnienia organu nadzorczego określa także samo RODO (art. 58). Obejmują one m.in. nakazanie dostarczenia informacji potrzebnych organowi nadzorczemu do realizacji jego zadań lub uzyskiwanie dostępu do takich informacji.

Uwaga: Kontrolerzy mogą rejestrować przebieg kontroli, np. za pomocą kamery. Muszą jednak o tym wcześniej poinformować. Zgoda kontrolowanego podmiotu nie jest konieczna (art. 84 ust. 4 u.o.d.o.).

Z kolei kontrolowany ma obowiązek umożliwić kontrolerom UODO sprawne przeprowadzenie kontroli, w związku z czym oprócz aktywnego w niej udziału i odpowiedzi na pytania zadawane w trakcie czynności kontrolnych może być zobowiązany do sporządzania kopii lub wydruków zarówno dokumentów, jak i informacji zgromadzonych na nośnikach, urządzeniach i w systemach. Dodatkowo organ nadzorczy może żądać przetłumaczenia sporządzonej w języku obcym dokumentacji, przedłożonej przez organizację w trakcie kontroli – niestety na koszt kontrolowanego.

KWESTIONOWANIE WYNIKÓW KONTROLI

Podczas kontroli może się zdarzyć, że w interesie kontrolowanego podmiotu będzie interwencja i zakwestionowanie czynności podejmowanych przez kontrolerów. Do takiej sytuacji może dojść, kiedy pracownik UODO w trakcie czynności kontrolnych przekracza zakres wskazany w upoważnieniu do kontroli. Co prawda utrudnianie pracownikom UODO czynności kontrolnych (przez co należy rozumieć m.in. niszczenie lub ukrywanie dokumentów, odmowę kontrolującym wstępu na teren mający podlegać kontroli, odmowę składania zeznań, udzielanie nieprawdziwych informacji) jest zagrożone karą nawet do dwóch lat pozbawienia wolności, jednak nikt nie powiedział, że są oni nieomylni.

Przykład: Zgodnie z upoważnieniem kontrola ma dotyczyć danych klientów placówki handlowej przetwarzanych w ramach stosowanego monitoringu wizyjnego. W związku z tym na prośbę kontrolera o przedstawienie regulaminu pracy funkcjonującego w organizacji powinno się wskazać, że taki dokument nie jest bezpośrednio związany z przedmiotem kontroli, a to oznacza, że nie powinien być poddany tej kontroli. Jeśli kontrolerzy nie podzielą argumentacji, warto poprosić ich o poczynienie odpowiedniej adnotacji w tym zakresie w protokole kontroli.

Warto również wskazać, że jeśli w postępowaniu w sprawie naruszenia przepisów o ochronie danych osobowych przedsiębiorca uzna, że kwestie mające stanowić przedmiot kontroli dotyczą tajemnicy przedsiębiorstwa, to ma on prawo zastrzec informacje, dokumenty lub ich fragmenty, które według jego opinii tę tajemnicę stanowią, i jednocześnie dostarczyć dwie wersje dokumentu: zawierającą informacje objęte zastrzeżeniem i niezawierającą takich informacji (zgodnie z art. 65 u.o.d.o.). Zastrzeżenie jest skuteczne z chwilą jego wniesienia, przy czym Prezes UODO może wydać decyzję o uchyleniu zastrzeżenia.

ROZLICZALNOŚĆ A UDOKUMENTOWANIE USTALEŃ PRZEZ KONTROLERÓW

RODO opiera się na zasadzie rozliczalności, zgodnie z którą to na administratorze danych spoczywa obowiązek wykazania, że przestrzega on przepisów o ochronie danych osobowych. Ta zasada odegra kluczową rolę podczas czynności kontrolnych, ponieważ kontrolerzy UODO bardzo rzadko poprzestają na ustaleniach ustnych. Co do zasady praktycznie wszystkie ustalenia starają się bardzo dokładnie udokumentować (np. przez załączenie do protokołu oryginałów lub poświadczonych kopii żądanych dokumentów).

Przykład: Organ nadzorczy przeprowadzający kontrolę w formie audytu osobowego prawdopodobnie nie poprzestanie na deklaracji organizacji, że pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych. Z pewnością konieczne będzie przedstawienie ich oświadczeń o zapoznaniu się z funkcjonującą w organizacji dokumentacją, a także certyfikatów poświadczających ukończenie szkolenia z tematyki ochrony danych osobowych.

Uwaga: Od pewnego czasu w przepisach o ochronie danych osobowych istnieje kara za utrudnianie lub udaremnianie kontroli. Przepis ten znalazł się też w nowej u.o.d.o. (art. 108). Uporczywe zwodzenie kontrolerów poprzez umawianie się na kontrolę i niestawianie się na nią dla organu będzie stanowić utrudnianie kontroli. Na pewno jednak za utrudnianie kontroli nie można uznać dyskomfortu inspektorów w związku z zaoferowaniem im niezbyt wygodnego pomieszczenia czy przeniesieniem ich do innego pomieszczenia w trakcie kontroli.

ZADBAJ O DOKUMENTACJĘ

Jedną z zalet RODO jest wyrażone w nim podejście do ochrony danych bazujące na ryzyku. Administratorzy mają dość dużą dowolność przy dobieraniu środków mających zapewnić przetwarzanym danych osobowym odpowiedni do ryzyka poziom bezpieczeństwa. Podobnie jest z dokumentacją ochrony danych – RODO nie określa katalogu elementów, z których powinna się ona składać, aby zapewnić pełną zgodność z przepisami. Wyjątkami są:

- **rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania,**
- **dokumentacja naruszeń ochrony danych.**

Zgodnie z zasadą rozliczalności musimy być w stanie wykazać, że organizacja wdrożyła zasady RODO. Mając to na względzie oraz zważywszy na stanowisko UODO w zakresie wymaganych dokumentów, przedstawione na jego oficjalnej stronie (https://uodo.gov.pl/pl/138/273, dostęp: 12.09.2019 r.), każda organizacja powinna posiadać następujące elementy dokumentacji:

- **rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania**, o których mowa w art. 30 RODO,
- **wytyczne dotyczące klasyfikacji naruszeń i procedurę zgłaszania naruszeń ochrony danych do organu nadzorczego (UODO)** – art. 33 ust. 3 RODO,
- **procedurę na wypadek wystąpienia naruszeń mogących powodować wysokie ryzyko naruszenia praw i wolności osób, w zakresie ich informowania o działaniach, jakie powinny wykonać, aby ryzyko to ograniczyć** – art. 34 RODO,
- **procedurę prowadzenia wewnętrznej dokumentacji stanowiącej rejestr naruszeń ochrony danych,** o którym mowa w art. 33 ust. 5 RODO,
- **raport z przeprowadzonej analizy ryzyka,**
- **raport z oceny skutków dla ochrony danych** – art. 35 ust. 7 RODO – jeśli dotyczy,
- **procedury związane z pseudonimizacją i szyfrowaniem** – jeśli dotyczy,
- **plan ciągłości działania** – art. 32 ust. 1 lit. b RODO,
- **procedury odtwarzania systemu po awarii oraz ich testowania** – art. 32 ust. 1 lit. c i d RODO.

Wskazówka: Kluczowe jest zgromadzenie w jednym miejscu dokumentów, o które mogą prosić kontrolujący. Dzięki temu będziemy w stanie udzielić dokładniejszych wyjaśnień oraz sprostować ewentualne nieścisłości. Ze względu na to, że nie sposób przewidzieć wszystkich materiałów, o które kontrolujący będą się zwracać, warto zadbać o stały dostęp do drukarki, aby na bieżąco drukować potrzebne dokumenty. Najlepiej jednak dostarczać wymagane dokumenty pocztą elektroniczną, aby nie wpływać negatywnie na środowisko.

WIĘCEJ

PRZEDKONTROLNY „COACHING" PRACOWNIKÓW

Nawet najlepiej przygotowana organizacja i najlepsze zabezpieczenia nie zapewnią zgodności z RODO, jeśli personel uczestniczący w operacjach przetwarzania nie zda egzaminu i podczas kontroli nie wykaże się wiedzą na temat tego, jak faktycznie przetwarza się dane osobowe – o niektórych kwestiach zapomni, o innych nie wyrazi się wystarczająco jasno w rozmowie z kontrolerem albo okaże się, że nie został w ogóle poinformowany o nich przez administratora lub źle je zrozumiał. Dlatego przed kontrolą zalecamy przeprowadzić symulację. W jej trakcie można zadać personelowi odpowiedzialnemu za przetwarzanie danych pytania, które prawdopodobnie padną ze strony kontrolerów UODO (przy uwzględnieniu omówionego wcześniej zakresu upoważnienia do kontroli), a także przypomnieć podstawowe zasady dotyczące przetwarzania danych osobowych oraz stosowanych technicznych, organizacyjnych i fizycznych zabezpieczeń przy codziennej pracy na danych. Warto również podnieść kwestie związane z bezpieczną budową haseł i postępowaniem z nimi (np. temat współdzielenia haseł z innymi), przechowywaniem i niszczeniem dokumentów papierowych, sposobem blokowania konta systemowego, zasadą czystego ekranu itp. Dodatkowo należy zwrócić uwagę na zasady postępowania w razie utraty sprzętu, kluczy, karty dostępowej czy na reguły dotyczące zamykania pomieszczeń, okien oraz szafek.

ZAKOŃCZENIE KONTROLI

Do formalnego zakończenia kontroli dochodzi po sporządzeniu i podpisaniu protokołu kontroli. Taki protokół zawiera przebieg czynności kontrolnych i dokumentuje wszystkie działania podjęte w toku kontroli, mające znaczenie dla sprawy. Elementy, które w protokole obligatoryjnie muszą się znaleźć, są wskazane w art. 88 u.o.d.o. Są to m.in.:

- **nazwa i adres podmiotu kontrolowanego,**
- **imię i nazwisko osoby reprezentującej kontrolowanego oraz nazwa organu reprezentującego kontrolowanego,**
- **imię i nazwisko, stanowisko służbowe, numer legitymacji służbowej oraz numer upoważnienia kontrolera,**
- **data rozpoczęcia i zakończenia kontroli,**
- **określenie przedmiotu i zakresu kontroli,**
- **opis stanu faktycznego stwierdzonego w toku kontroli oraz inne informacje mające istotne znaczenie,**
- **opis załączników do protokołu,**
- **omówienie dokonanych w protokole poprawek, skreśleń i uzupełnień,**
- **data i miejsce podpisania protokołu przez inspektora oraz przez podmiot kontrolowany.**

Kontrolujący przekazuje protokół do podpisu kontrolowanemu, przy czym ten, w terminie 7 dni od dnia przedstawienia mu protokołu, może albo podpisać protokół (jeśli nie ma zastrzeżeń co do jego treści), albo złożyć pisemne zastrzeżenia do treści protokołu. Brak którejkolwiek z wymienionych czynności uznaje się za odmowę podpisania protokołu, o czym kontrolujący czyni wzmiankę w protokole.

Wskazówka: Może się zdarzyć, że w protokole nie zostaną zawarte wszystkie korzystne dla nas ustalenia – np. o stosowaniu polityki czystego biurka i ekranu – lub że pojawią się ustalenia, z którymi się nie zgadzamy. Wówczas w ciągu 7 dni możemy skorzystać z przysługującego nam uprawnienia do złożenia pisemnych zastrzeżeń do treści protokołu.

Co istotne, w samym protokole kontroli nie znajdziemy rozstrzygnięcia merytorycznego w zakresie tego, czy przepisy o ochronie danych osobowych zostały naruszone, czy też kontrolowany podmiot jest zgodny z nimi. Protokół stanowi jedynie ustalenie stanu faktycznego – opis tego, jak organizacja stosuje się do przepisów. Ocenę tego i decyzję w tym zakresie na podstawie ustaleń kontrolnych podejmuje Prezes UODO, a w przypadku gdy uzna, że mogło dojść do naruszenia przepisów, wszczyna postępowanie administracyjne w sprawie naruszenia przepisów o ochronie danych osobowych, o którym kontrolowana organizacja jest powiadomiona. W takim wypadku postępowanie administracyjne stanowi kolejny, odrębny od kontroli etap działań podejmowanych przez organ nadzorczy. Jeśli organ nadzorczy nie dostrzega naruszeń, wykonywane przez niego czynności kończą się z chwilą zakończenia kontroli.

W niektórych sytuacjach po zakończonym postępowaniu administracyjnym, w którego wyniku w drodze decyzji stwierdzono naruszenie, może zostać przeprowadzona dodatkowa kontrola w celu sprawdzenia, czy kontrolowany zrealizował decyzję Prezesa UODO.

Uwaga: Jeśli w trakcie kontroli, a później postępowania okaże się, że zawinił pracownik, organ nadzorczy ma prawo żądać jego ukarania (art. 58 u.o.d.o.).

II CZĘŚĆ. PROCESY PRZETWARZANIA DANYCH

Dzięki znajomości podstawowych założeń kontroli i schematu działania kontrolerów wiadomo, jak zachować się przed kontrolą i podczas niej. W ferworze wszystkich czynności związanych z kontrolą nie można zapomnieć o tym, co jest głównym przedmiotem zainteresowania kontrolerów UODO, czyli o procesach przetwarzania danych osobowych realizowanych przez administratorów. W szczególności zaś powinniśmy mieć na względzie to, w jaki sposób zapewnić, aby w ramach przetwarzania dokonywanego w poszczególnych procesach respektować zasady wyrażone w RODO i (co ważniejsze) być w stanie to wykazać. Poniżej przedstawiamy opracowanie kluczowych procesów wraz z gotowymi rozwiązaniami, które możesz zaimplementować w swojej organizacji. Obejmuje ono następujące procesy: rekrutacji, zatrudnienia, marketingu, sprzedaży i obsługi klienta, przetwarzania danych kontrahentów i ich przedstawicieli. Zapoznanie się z tą częścią poradnika pozwoli szybko ocenić, na ile organizacja jest zgodna z wymaganiami RODO.

Rekrutacja

JAK ZAPEWNIĆ PODSTAWĘ PRAWNĄ PRZETWARZANIA DANYCH OSOBOWYCH W PROCESIE?

Zasadniczym punktem kontroli jest ustalenie, czy dane zebrano zgodnie z prawem. Dane osobowe mogą być przetwarzane wyłącznie wtedy, gdy istnieje podstawa prawna ich przetwarzania. Oznacza to, że administrator może przetwarzać niemal dowolne dane osobowe, o ile jest w stanie wykazać, że przetwarza je na podstawie przesłanek wymienionych w art. 6 ust. 1 RODO – jeśli mowa o danych zwykłych – lub na podstawie art. 9 ust. 2 RODO, gdy mowa o danych szczególnych kategorii („danych wrażliwych").

Jednym jest więc zidentyfikowanie danych osobowych jako zwykłych lub wrażliwych, a drugim – zapewnienie, aby do ich przetwarzania dochodziło zgodnie z prawidłową prawną przesłanką przetwarzania. Jakie zatem przesłanki znajdą zastosowanie przy przetwarzaniu danych osobowych kandydatów do pracy, zawartych w nadsyłanych dokumentach aplikacyjnych?

Obowiązek prawny ciążący na administratorze

Nowelizacja Kodeksu pracy obowiązująca od 4 maja 2019 r., którą przyniosła ustawa o zmianie niektórych ustaw w związku z RODO, dostosowała brzmienie obowiązujących przepisów prawa pracy do art. 6 ust. 1 lit. c RODO, czyli do przesłanki obowiązku prawnego jako podstawy prawnej zbierania danych osobowych przez pracodawcę – zarówno na etapie rekrutacji, jak i w trakcie zatrudnienia.

W art. 22^1 § 1 Kodeksu pracy (k.p.) znajdujemy katalog danych osobowych, których pracodawca żąda od osoby ubiegającej się o zatrudnienie, obejmujący:

- **imię (imiona) i nazwisko,**
- **datę urodzenia,**
- **dane kontaktowe wskazanych przez kandydata,**
- **wykształcenie,**
- **kwalifikacje zawodowe,**
- **przebieg dotychczasowego zatrudnienia.**

We wcześniejszej wersji przywołanego przepisu pracodawca jedynie „mógł żądać" wymienionych danych osobowych, teraz zaś jest do tego zobligowany.

Wskazówka: Ministerstwo Rodziny, Pracy i Polityki Społecznej opublikowało na swojej stronie WWW pomocnicze wzory dla pracodawców, w tym kwestionariusz osobowy dla osoby ubiegającej się o zatrudnienie, zgodny z wymogami k.p.

Błędem często popełnianym przez administratorów jest zbieranie takich danych kandydatów jak imiona rodziców, miejsce urodzenia czy zdjęcie w CV. Czy w związku z tym pracodawcy mogą przetwarzać w toku rekrutacji inne dane osobowe kandydatów? Tak – pracodawcy żądają podania dodatkowych danych, jeśli taki **wymóg wynika wprost z przepisów szczególnych**. Przykładowo pracownik ochrony nie może być skazany za przestępstwo umyślne (zgodnie z art. 26 ust. 3 ustawy o ochronie osób i mienia), tak samo jak nauczyciel, detektyw czy członek organów spółek handlowych (taki wymóg każdorazowo będzie wynikał z przepisów). W związku z tym kandydatów na takie stanowiska można prosić o przedłożenie zaświadczenia o niekaralności z Krajowego Rejestru Karnego (KRK). Co więcej obowiązek prawny podania danych nie jest jedyną podstawą prawną przetwarzania danych osobowych w procesie, ponieważ przetwarzanie możemy także oprzeć na podstawie, jaką jest zgoda.

Zgoda osoby, której dane dotyczą

Dane kandydata biorącego udział w rekrutacji można przetwarzać w zakresie szerszym niż skromny katalog z k.p., natomiast dodatkowe dane można przetwarzać wyłącznie na podstawie dobrowolnej zgody kandydata

(art. 6 ust. 1 lit. a RODO). Co ważne, RODO zezwala na wyrażenie zgody w formie oświadczenia lub wyraźnego działania potwierdzającego. Oznacza to, że nie zawsze trzeba posługiwać się klauzulą zgody – czasem wystarczy zachowanie kandydata, które jednoznacznie wskazuje na jego wolę przekazania pracodawcy swoich danych osobowych.

Dobrowolność (i zarazem wyraźne działanie) łatwo wykazać, kiedy dane są przekazywane w toku rekrutacji z inicjatywy kandydata, np. gdy ten umieszcza w CV informację o swoich zainteresowaniach, mimo że taki wymóg nie wynika z treści ogłoszenia. Nie wyklucza to sytuacji, w której to potencjalny pracodawca pyta kandydata o zgodę na przetwarzanie jego danych, natomiast odmowa wyrażenia takiej zgody lub jej wycofanie nie może skutkować negatywnymi konsekwencjami (np. przez to, że kandydat nie umieścił w CV swojego zdjęcia, nie powinien być automatycznie odrzucany na wstępnym etapie rekrutacji).

Jakie dane kandydata do pracy można przetwarzać na podstawie jego zgody? Najczęściej będą to:

- **wizerunek (zdjęcie kandydata),**
- **referencje od byłych pracodawców,**
- **informacje o zainteresowaniach, działalności dodatkowej itp.**

Uwaga: W niektórych sytuacjach mogą pojawić się również dane wrażliwe, np. informacje o przynależności do związków zawodowych, partii politycznych czy wyznaniu religijnym. Przetwarzanie takich danych będzie ryzykowne dla pracodawcy. Rekomendujemy, aby administrator zanonimizował takie nadmiarowe dane lub zniszczył przesłane dokumenty i poprosił kandydata o ponowne przesłanie dokumentów w wersji bez takich informacji.

Zgoda musi być nie tylko dobrowolna, lecz także konkretna, świadoma i jednoznaczna. Przede wszystkim kandydat musi mieć możliwość udzielenia jej na każdy z celów przetwarzania odrębnie.

Przykład: Nie będziemy mogli w ramach jednej klauzuli zebrać zgody na przetwarzanie danych na cele rekrutacji obecnej i rekrutacji przyszłych.

KLAUZULE ZGODY W REKRUTACJI

Skoro zgodę można wyrazić poprzez działanie, warto rozważyć zaprzestanie zbierania pisemnych zgód na przetwarzanie danych do celów bieżącej rekrutacji. Kandydat, odpowiadając na ogłoszenie o pracę, zgadza się na przetwarzanie danych, które (dobrowolnie) zawarł w dokumentach aplikacyjnych. Zamiast zbierać standardowe zgody w treści ogłoszenia można zamieścić informację:

Przykład: *Zawarcie przez Ciebie w dokumentach aplikacyjnych danych osobowych, które swoim zakresem wykraczają poza wymogi przepisów prawa pracy, rozumiemy jako Twoją dobrowolną zgodę na ich przetwarzanie w celach przeprowadzenia procesu rekrutacyjnego.*

Natomiast „tradycyjne" zgody można odbierać jak niżej:

Przykład:

☐ *Tak, chcę, aby moje dane zawarte w dokumentach aplikacyjnych były przetwarzane przez ABC sp. z o.o. w celach rekrutacji przyszłych.*

☐ *Wyrażam zgodę, aby moje CV i dane osobowe w nim zawarte były przekazane innym spółkom z grupy kapitałowej w celach przeprowadzenia przez nie rekrutacji na własną rzecz, tj.: DEF sp. z o.o., GHI sp. z o.o.*

Warto w tym miejscu zwrócić uwagę na stanowisko Grupy Roboczej Art. 29, wyrażone w wytycznych dotyczących zgody[1]. Zgodnie z nim zgoda na przekazanie danych (tu: innym podmiotom z grupy) w konkretnym celu (prowadzenia przez nie działań rekrutacyjnych) zostanie uznana za ważną w odniesieniu do każdego z podmiotów, o którego tożsamości poinformowano osobę, której dane dotyczą, w chwili wyrażania zgody, o ile zostanie mu ona przekazana w tym samym celu.

Podstawowe zasady konstruowania klauzul zgód:

- **Należy wskazać administratora danych i cel przetwarzania.**
- **Osoba udzielająca zgody musi znać zakres danych, których zgoda dotyczy (np. „dane zawarte w przesłanym CV" lub „dane z formularza rekrutacyjnego").**
- **Każdy cel przetwarzania danych osobowych = odrębna zgoda.**

[1] Wytyczne Grupy Roboczej Art. 29 dotyczące zgody na mocy rozporządzenia 2016/679 (17/PL, WP259 rev.01), przyjęte 28 listopada 2017 r., ostatnio zmienione i przyjęte 10 kwietnia 2018 r., przykład nr 7, s. 11.

WIĘCEJ

JAK I KIEDY SPEŁNIAĆ OBOWIĄZEK INFORMACYJNY W REKRUTACJI?

Wielu myli sformułowanie „uzyskanie podstawy prawnej przetwarzania danych osobowych" z wyrażeniem „spełnienie obowiązku informacyjnego". Nie można jednak zakładać, że jeżeli uzyskaliśmy zgodę kandydata na przetwarzanie jego danych, to jesteśmy uprawnieni do wykorzystywania danych osobowych w określonych celach. Zwracamy uwagę, że są to kwestie całkowicie od siebie niezależne, a tylko ich równoległe występowanie pozwoli na stwierdzenie, że dane osobowe są przetwarzane zgodnie z RODO.

Obowiązek informacyjny (wynikający z art. 13 RODO) względem kandydata spełnia się w momencie zbierania jego danych osobowych. Sytuacja komplikuje się, gdy organizację w rekrutacji wspierają podmioty zewnętrzne (np. agencje rekrutacyjne) lub gdy dane zbierane są w sposób inny niż bezpośrednio od kandydata. Poniżej przedstawiamy najczęstsze przykłady pozyskiwania danych kandydatów ze wskazówkami, w jaki sposób najlepiej spełnić obowiązek informacyjny z art. 13 czy 14 RODO.

Pozyskanie kandydatur przez ogłoszenie na portalu rekrutacyjnym lub na stronie WWW administratora

Niezależnie od tego, czy kandydat przekazuje swoje dane osobowe przez udostępnienie swojego CV lub przesłanie go na adres e-mail pracodawcy, czy przez wypełnienie formularza internetowego, musi on mieć możliwość zapoznania się z klauzulą informacyjną przed kliknięciem w przycisk „Wyślij" lub „Aplikuj". Musi to więc nastąpić przed udostępnieniem danych osobowych potencjalnemu pracodawcy. Treść klauzuli z art. 13 RODO można zawrzeć np. w treści ogłoszenia o pracę czy pod formularzem aplikacyjnym.

Pozyskanie danych za pośrednictwem podmiotu działającego w imieniu i na rzecz pracodawcy, np. agencji rekrutacyjnej

Jeśli pracodawca powierza podmiotowi zewnętrznemu przeprowadzenie rekrutacji na swoją rzecz, to zbieranie danych kandydatów przez ten podmiot traktujemy, jak gdyby to administrator pozyskiwał te dane. W świetle przepisów RODO *de facto* tak właśnie jest, ponieważ agencja pozyskuje dane osobowe kandydatów, działając w imieniu i na rzecz administratora. W związku z tym obowiązek informacyjny należy spełnić analogicznie, tj. tak, jakby dane zbierał administrator. Naturalne w tej sytuacji jest, że z takim podmiotem należy zawrzeć umowę powierzenia w formie pisemnej (w tym elektronicznej) lub uregulować przetwarzanie danych innym instrumentem prawnym zgodnie z art. 28 RODO.

Skoro jesteśmy przy powierzaniu przetwarzania danych, to warto nadmienić, że rekomendowanym rozwiązaniem jest prowadzenie przez administratora wykazu wszystkich podmiotów, którym powierzył przetwarzanie danych osobowych, a jeśli te podmioty dalej powierzają przetwarzanie danych osobowych – wykazu całego łańcucha dalszych podmiotów przetwarzających. W trakcie kontroli taki wykaz ułatwi objaśnienie cyklu życia oraz przepływów danych osobowych.

Dane kandydata udostępniane przez innego administratora

Jeśli dane kandydata udostępnia inny administrator, np. inna spółka z grupy kapitałowej, która uprzednio uzyskała zgodę na przekazanie danych kandydata, albo agencja zatrudnienia, która udostępnia dane z własnej bazy potencjalnych kandydatów, to obowiązek informacyjny aktualizuje się po stronie każdego z administratorów z osobna. W takiej sytuacji dane pozyskuje się w sposób inny niż bezpośrednio od kandydata, w związku z czym spełnia się obowiązek informacyjny z art. 14 RODO (w stosunku do klauzuli z art. 13 RODO rozszerzony o źródło pozyskania danych i kategorie danych, jakie administrator pozyskał, a ograniczony o kwestie dobrowolności/obligatoryjności podania danych, bo przecież to nie kandydat nam je podaje, a inny administrator). Wówczas – w zależności od dalszych działań na pozyskanych danych osobowych – administrator powinien spełnić obowiązek informacyjny co do zasady przy pierwszym kontakcie z kandydatem, ale najpóźniej w ciągu miesiąca od pozyskania danych.

Administrator powinien spełnić obowiązek informacyjny w sposób, na który pozwalają mu dane kontaktowe kandydata, którymi dysponuje. Kandydat w tym zakresie ma pełną dowolność – może wskazać swój adres e-mail, numer telefonu i adres do korespondencji, ale również może zdecydować się na podanie np. tylko jednej z tych informacji.

Przekazanie danych kandydata przez stronę trzecią, np. innego pracownika biorącego udział w firmowym programie poleceń

Jeżeli dane pozyskuje się za pośrednictwem osoby trzeciej, to obowiązek informacyjny należy spełnić na zasadach określonych w art. 14 RODO.

Wskazówka: W procesie rekrutacji często dochodzi do przetwarzania danych osób innych niż kandydaci, tj. udzielających referencji. W takiej sytuacji dane pozyskuje się za pośrednictwem kandydata, w związku z czym wobec takiej osoby w teorii powinno spełnić się obowiązek informacyjny z art. 14 RODO, wskazując jako podstawę prawną przetwarzania art. 6 ust. 1 lit. f RODO,

w którym prawnie uzasadnionym interesem administratora jest weryfikacja prawdziwości złożonych referencji.

PODMIOTY ZEWNĘTRZNE W REKRUTACJI – JAK ODPOWIEDNIO UREGULOWAĆ Z NIMI WSPÓŁPRACĘ?

Administratorzy często przeprowadzają proces rekrutacyjny przy wsparciu zewnętrznych podmiotów. Przed podjęciem współpracy w tym zakresie należy określić stosunek prawny, na podstawie którego będzie dochodziło do przepływu danych między administratorem a zewnętrznym podmiotem, odpowiednio: powierzenie danych osobowych podmiotowi przetwarzającemu lub udostępnienie danych między odrębnymi administratorami.

Powierzenie danych kandydatów

Administrator, czyli pracodawca chcący zatrudnić nowych pracowników, co do zasady powierza dane osobowe **agencjom rekrutacyjnym**, które zgodnie z poleceniem administratora (czyli „w imieniu i na rzecz") poszukują dla niego pracowników. Przykładami działań wykonywanych przez agencje mogą być: publikowanie ogłoszeń o pracę, wyszukiwanie kandydatów i ich wstępna selekcja czy umawianie rozmów rekrutacyjnych. Takie podmioty co do zasady nie korzystają z własnych baz kandydatów, a wyszukują ich na potrzeby danej, określonej przez administratora rekrutacji. Wówczas niezbędne jest zawarcie umowy powierzenia przetwarzania danych osobowych zgodnie z art. 28 RODO.

Udostępnienie danych kandydatów przez odrębnego administratora

Inaczej sytuacja przedstawia się przy współpracy pracodawcy z agencjami zatrudnienia, których działalność jest uregulowana prawnie i które będą pełnić funkcję odrębnych administratorów danych. Dlaczego? Agencje zatrudnienia najczęściej działają w schemacie, w którym prowadzą działania w swoim imieniu i na własną rzecz, mające na celu zbudowanie własnej bazy kandydatów, z której poszczególne rekordy byłyby udostępniane na potrzeby innych administratorów, czyli pracodawców. Pracodawca stanie się administratorem danych kandydata dopiero w momencie ich udostępnienia przez agencję – tylko wówczas, gdy kandydat wyraził odpowiadającą przepisom RODO zgodę na takie udostępnienie.

OKRES PRZECHOWYWANIA DANYCH

Zgodnie z rekomendacjami UODO dane osób biorących udział w rekrutacji powinny zostać usunięte niezwłocz-

nie po jej zakończeniu. Naszym zdaniem dane powinno się jeszcze móc przechowywać przez **3 miesiące po zakończeniu rekrutacji** – jest to praktyczne, bo jeśli osoba wyłoniona w trakcie rekrutacji nie sprawdzi się na nowo objętym stanowisku i pracodawca nie zdecyduje się przedłużyć z nią współpracy po okresie próbnym, to mógłby on wznowić prowadzony proces rekrutacyjny zamiast zbierać dane od nowa.

W przypadku kandydatów, którzy wyrazili zgodę na **rekrutacje przyszłe**, kwestia również nie jest jasno rozstrzygnięta. Decyzja administratora co do terminu przechowywania danych powinna zostać podjęta po wnikliwej analizie faktycznych potrzeb i prawdopodobieństwa skutecznego wykorzystania CV kandydata w danym okresie, przy czym jako taki bezpieczny termin rekomendujemy okres 1 roku. W uzasadnionych przypadkach można go wydłużyć, np. do 2 lat, jeśli rotacja na danym stanowisku jest spora i istnieje duże prawdopodobieństwo, że potencjalni kandydaci raczej nie stracą całkowicie zainteresowania ewentualną ofertą.

UMOWY CYWILNOPRAWNE

W dużej części do przetwarzania danych potencjalnych współpracowników (kandydatów, którzy docelowo mają zostać zatrudnieni na podstawie umowy cywilnoprawnej, w tym np. umowy-zlecenia, umowy o dzieło, umowy o świadczenie usług) powinno dochodzić w sposób analogiczny do tego, który jest stosowany przy rekrutacji pracowników – przede wszystkim jeśli chodzi o okres przechowywania danych i sposoby spełniania obowiązku informacyjnego. Natomiast różnice pomiędzy tymi rodzajami rekrutacji można zaobserwować w dwóch poniżej wskazanych aspektach.

Podstawa prawna przetwarzania

W przypadku rekrutacji na stanowisko współpracownika właściwe będą inne podstawy prawne przetwarzania danych osobowych, ponieważ k.p. nie znajdzie tu zastosowania. Zamiast art. 6 ust. 1 lit. c RODO (czyli przetwarzania niezbędnego do wykonania obowiązku prawnego ciążącego na administratorze) dane osobowe niezbędne do przeprowadzenia rekrutacji zawarte przez kandydata na współpracownika w CV będziemy przetwarzać na podstawie art. 6 ust. 1 lit. b RODO. Oznacza to, że przetwarzanie jest niezbędne do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (bo ewentualna umowa cywilnoprawna na etapie rekrutacji nie jest przecież zawierana). Jeśli zaś którekolwiek z danych osobowych wykraczają poza zakres „niezbędności", będziemy przetwarzać je na podstawie zgody kandydata (art. 6 ust. 1 lit. a RODO), wynikającej z faktu samego przesłania dokumentów.

Zakres przetwarzanych danych

Zakres, czyli to, jakie dane kandydata ubiegającego się o zatrudnienie na podstawie umowy cywilnoprawnej możemy przetwarzać, nie wynika wprost z przepisów prawa cywilnego. Oznacza to, że podmiot zatrudniający powinien samodzielnie dokonać analizy, jakie dane powinien zbierać i jakie będą adekwatne do celu. Do takich danych osobowych bez wątpienia można zaliczyć imię i nazwisko, dane kontaktowe, dane o wykształceniu, kwalifikacjach i doświadczeniu, czyli dane podobne do tych wskazanych w art. 22^1 k.p. Oczywiście kandydat może podać dane wykraczające poza ten zakres.

REKRUTACJE UKRYTE

Przeprowadzanie rekrutacji ukrytych (tzw. ślepych), zakładających utajenie tożsamości pracodawcy na wstępnym etapie procesu rekrutacyjnego, to zjawisko coraz powszechniejsze. Powody, dla których pracodawcy decydują się na rekrutacje ukryte, mogą być różne, choć do najczęstszych zalicza się planowane zastąpienie obecnych pracowników i tym samym uniemożliwienie im uzyskania informacji o nadchodzących zmianach.

RODO jednoznacznie rozstrzyga tę kwestię w art. 13, regulującym sposób spełniania obowiązku informacyjnego. Zgodnie z tym przepisem klauzulę informacyjną (wskazującą m.in. tożsamość administratora danych) należy przedstawić osobie fizycznej **podczas pozyskiwania** jej danych osobowych. Skoro zatem rekrutacja ukryta zakłada brak wskazania tożsamości pracodawcy, to tym samym potencjalny kandydat przy przesła-

niu swoich dokumentów aplikacyjnych nie zostanie poinformowany o tym, kto jest administratorem jego danych osobowych.

Natomiast UODO sugeruje, aby w sytuacji gdy pracodawcy zależy na dyskrecji, skorzystać z usług agencji rekrutacyjnych (patrz część „Podmioty zewnętrzne w rekrutacji…") i tworzonych przez nie baz kandydatów. Wówczas agencja może dokonać wstępnej selekcji na podstawie profilu stworzonego przez pracodawcę, a obowiązek informacyjny zaktualizuje się po stronie pracodawcy dopiero w momencie przekazania mu danych kandydata przez agencję.

ZAŚWIADCZENIE O NIEKARALNOŚCI Z KRK

Argument, że pracodawca chce zatrudnić osobę o nieposzlakowanej opinii, która nigdy nie miała zatargów z prawem, ponieważ darzyłby ją większym zaufaniem, nie przekonuje UODO. Zasada jest prosta: dane o niekaralności kandydata/pracownika przetwarzamy wyłącznie wtedy, gdy taki obowiązek wynika z przepisów prawa. Dostęp do zawodu jest ograniczony ze względu na wymóg niekaralności w przypadku m.in. nauczycieli, detektywów, osób ubiegających się o zatrudnienie w podmiotach sektora finansowego czy osób mających pełnić funkcje w określonych organach spółek prawa handlowego.

KONTAKT Z BYŁYMI PRACODAWCAMI

Samo dostarczenie przez kandydata do pracy w toku prowadzonej rekrutacji referencji wystawionych przez byłe podmioty zatrudniające nie uprawnia pracodawcy do kontaktu z tymi podmiotami. Taki kontakt może nastąpić dopiero na podstawie zgody kandydata. Co ważne, kontakt z byłym pracodawcą powinien być nawiązany w celu weryfikacji informacji podanych przez kandydata i znajdujących odzwierciedlenie w wystawionych referencjach, a nie w celu zebrania o nim dodatkowych danych.

REKRUTACJA W GRUPIE KAPITAŁOWEJ

Modeli rekrutacji prowadzonych przez spółki należące do grupy kapitałowej jest na tyle dużo, że można by napisać o nich oddzielny poradnik. Dlatego w tym miejscu chcielibyśmy raczej zwrócić uwagę na występowanie problemu i konieczność jego analizy niż wskazać gotowe rozwiązanie. Możliwości jest mnóstwo, ale najpowszechniejsze formy rekrutacji w grupie kapitałowej to:

- **przeprowadzanie rekrutacji przez jedną spółkę na rzecz innych podmiotów z grupy,**
- **udział jednej ze spółek (np. spółki matki) na jednym z etapów rekrutacji, np. przy podjęciu ostatecznej decyzji co do zatrudnienia kandydata,**
- **korzystanie przez spółki z grupy z tych samych programów rekrutacyjnych, administrowanych przez jedną ze spółek (np. spółkę matkę).**

Standardowo można wyróżnić trzy modele zarządzania przepływem danych osobowych pomiędzy przywołanymi podmiotami, mianowicie:

- **udostępnienie danych pomiędzy niezależnymi administratorami (relacja ADO – ADO),**
- **powierzenie danych (ADO – podmiot przetwarzający) lub**
- **współadministrowanie danymi przez co najmniej dwa podmioty.**

WIĘCEJ

Do administratora należy rzetelna ocena stanu faktycznego i odpowiednie uregulowanie kwestii przepływu danych osobowych kandydatów pomiędzy spółkami z grupy.

Zatrudnienie

PODSTAWY PRAWNE PRZETWARZANIA DANYCH OSOBOWYCH W ZATRUDNIENIU

W procesie zatrudnienia rysuje się wachlarz możliwości, jeśli chodzi o podstawy prawne przetwarzania danych osobowych. Posiadanie ważnych podstaw prawnych do przetwarzania danych podczas zatrudnienia jest kluczowe z punktu widzenia pracodawcy. UODO bowiem w czasie badania konkretnego obszaru przetwarzania danych osobowych w organizacji w pierwszej kolejności zwróci uwagę, czy pracodawca przetwarza tylko takie dane osobowe swoich pracowników, co do których legitymuje się odpowiednią podstawą prawną. Poniżej omawiamy kolejno przesłanki przetwarzania, które najczęściej pojawiają się w niniejszym procesie, odwołując się do wymienionych zarówno w art. 6 ust. 1 RODO, jak i w art. 9 ust. 2 RODO.

Przepis prawa

Podobnie jak w przypadku danych osobowych kandydata do pracy w k.p. znajdziemy katalog danych, których pracodawca żąda od pracownika. Katalog ten zgodnie z art. 22^1 § 1 i 3 k.p. obejmuje:

- **adres zamieszkania,**
- **numer PESEL, a w przypadku jego braku – rodzaj i numer dokumentu potwierdzającego tożsamość,**
- **inne dane osobowe pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych**

jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy,

- **wykształcenie i przebieg dotychczasowego zatrudnienia, jeżeli nie istniała podstawa do ich żądania od osoby ubiegającej się o zatrudnienie,**
- **numer rachunku płatniczego, jeżeli pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych.**

Zgodnie z postanowieniami k.p. udostępnianie pracodawcy powyższych danych następuje w formie oświadczenia pracownika, niemniej pracodawca może żądać od pracownika odpowiednich dokumentów celem potwierdzenia konkretnych informacji, np. dyplomu ukończenia deklarowanego kierunku studiów czy wymienionych kursów bądź świadectwa pracy.

Należy mieć na uwadze również to, że na podstawie przepisu prawa pracodawca przetwarza dane pracowników oraz członków ich rodzin w przypadku prowadzenia i obsługi przez pracodawcę zakładowego funduszu świadczeń socjalnych (ZFŚS), jak również wykonywania obowiązków względem Zakładu Ubezpieczeń Społecznych (ZUS), urzędu skarbowego czy Narodowego Funduszu Zdrowia.

Zgoda pracownika

Kolejną przesłanką, z którą spotykamy się, analizując proces zatrudnienia, jest zgoda osoby, której dane dotyczą. Dane osobowe, które pracodawca będzie przetwarzał na podstawie zgody pracownika, będą przetwarzane zgodnie z art. 6 ust. 1 lit. a RODO, a w przypadku danych szczególnych kategorii – art. 9 ust. 2 lit. a RODO.

Praktyka pokazuje, że na podstawie zgody przetwarzany jest najczęściej wizerunek pracownika. Wynika to w szczególności z powszechności stosowania **identyfikatorów ze zdjęciem pracownika**, które często jednocześnie pełnią funkcję karty dostępowej do siedziby pracodawcy. Z uwagi na fakt, że wizerunek nie jest objęty katalogiem danych wskazanych w k.p., pracodawca zobligowany jest uzyskać zgodę pracownika na zamieszczenie wizerunku na identyfikatorze. W poradniku dotyczącym zatrudnienia UODO zaznacza jednak, że istnieją sytuacje, w których wizerunek pracownika jest ściśle związany z wykonywanym przez niego zawodem czy charakterem pracy, a wskazywanie wizerunku pracownika przewidują wprost przepisy prawa. Jako przykład UODO przywołuje pracownika ochrony, który jest zobligowany posiadać legitymację zawierającą jego zdjęcie[2]. Innymi przykładami mogą tu być pracownicy urzędów, np. inspektor kontroli ZUS czy też pracownik UODO.

Często spotykaną sytuacją jest również zamieszczanie **zdjęcia pracownika na stronie internetowej** pracodawcy. Przed umieszczeniem zdjęcia pracownika na stronie internetowej pracodawca musi pozyskać jego zgodę. W tym zakresie zwykle nie pojawiają się żadne wątpliwości. Również stanowisko UODO jest bezsporne. Problematyczna może jednak pozostawać kwestia rozpowszechniania wizerunku. Z rozpowszechnianiem wizerunku mamy do czynienia wtedy, gdy wizerunek pracownika dociera do nieograniczonego grona odbiorców, co wiąże się nierozerwalnie z umieszczeniem takiego wizerunku na stronie internetowej. Oprócz przepisów RODO zastosowanie znajdzie w tym przypadku również ustawa o prawie autorskim i prawach pokrewnych (u.p.a.p.p.). Zgodnie z art. 81 u.p.a.p.p. rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej, chyba że osoba ta otrzymała umówioną zapłatę za pozowanie. W związku z tym pracodawca, który chce upublicznić wizerunek swojego pracownika na firmowej stronie internetowej, powinien posiadać zgodę pracownika wynikającą z u.p.a.p.p. Ta sama zgoda będzie stanowić jednocześnie zgodę na przetwarzanie wizerunku i danych osobowych.

Przykład: *Wyrażam zgodę na przetwarzanie mojego wizerunku utrwalonego podczas pikniku integracyjnego przez ……* [nazwa pracodawcy].

Przyjmuję do wiadomości, że:

- *mój wizerunek zostanie zamieszczony na stronie internetowej pracodawcy w terminie tygodnia od zakończenia pikniku,*
- *mój wizerunek może zostać zestawiony z treścią dotyczącą przedmiotu działalności pracodawcy i oferowanych przez niego usług,*

[2] Urząd Ochrony Danych Osobowych, „Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców. Poradnik RODO", październik 2018, s. 24.

- mój wizerunek może zostać zestawiony z wizerunkami innych pracowników i osób biorących udział w pikniku,

- mój wizerunek nie będzie wykorzystywany w celach marketingowych.

Powyższa zgoda może zostać odwołana w każdym czasie, jednakże odwołanie niniejszej zgody pozostanie bez wpływu na przetwarzanie danych dokonane przed jej odwołaniem.

Kolejnym przykładem jest zamieszczanie **zdjęcia pracownika w gazetce firmowej**. W pierwszej chwili może się wydawać, że skoro co do zasady gazetka rozprowadzana jest wewnątrz organizacji, to pracodawca nie jest zobligowany do pozyskiwania dodatkowo zgody od pracownika. Ponadto często zdjęcie pracownika wiąże się z wykonywaniem przez niego obowiązków czy zadań wynikających ze stosunku pracy, np. spotkania biznesowe, konferencje, targi. Rzeczywiście, rozpatrując powyższe, można dojść do wniosku, że pracodawca może przetwarzać dane pracownika, opierając się na innej niż zgoda podstawie prawnej, tj. art. 6 ust. 1 lit. f RODO – prawnie uzasadnionym interesie administratora, rozumianym jako komunikowanie wewnątrz organizacji bieżących wydarzeń, w których pracownicy biorą udział. Można również wyobrazić sobie sytuację, że konkretne stanowisko wiąże się z systematycznym udziałem pracownika w różnych wydarzeniach, konferencjach, targach, z których relacja dla pozostałych pracowników jest zamieszczana w wewnętrznej gazetce, publikowanej np. w intranecie. Należy jednak mieć na uwadze, że zdjęcia pracownika zamieszczane w gazetce nie zawsze są bezpośrednio związane z realizacją stosunku pracy. Mogą to być bowiem zdjęcia z imprez firmowych bądź wyjazdów integracyjnych. Ponadto często gazetka firmowa jest również drukowana i dostęp do niej może mieć znaczne szersze grono odbiorców, np. klienci pracodawcy odwiedzający firmę, rodziny pracowników itd. Wówczas zgodę pracownika na utrwalenie i rozpowszechnianie jego wizerunku należy uznać za konieczną. Przedmiotowa zgoda powinna przyjąć tożsamą formę z opisywaną powyżej zgodą dotyczącą zamieszczania zdjęcia pracownika na stronie WWW.

Prawnie uzasadniony interes administratora

Na wstępie warto zaznaczyć, że prawodawca unijny bardzo szeroko definiuje „prawnie uzasadniony interes administratora", kładąc nacisk na to, że jego istnienie należy w każdym przypadku ważyć i oceniać. Przykładowym narzędziem, które może posłużyć do takiej oceny, jest tzw. **test równowagi**. Jego wynik może stanowić materiał dowodowy spełnienia wymagań RODO przez administratora. Na czym polega test równowagi? Jest to nic innego jak porównanie wagi interesów administratora realizowanych w związku z podejmowanymi czynnościami przetwarzania danych osobowych z podstawowymi prawami i wolnościami osoby, której dane dotyczą. Dokonując tego porównania, administrator musi zdecydować, który z dwóch interesów postawionych na szali ma większy priorytet. Jeżeli w konkretnym przypadku okaże się, że ważniejsze są interesy osoby fizycznej lub w wyniku podjęcia konkretnej czynności przetwarzania zagrożone byłyby jej podstawowe prawa i wolności, administrator nie może oprzeć przetwarzania danych na omawianej podstawie prawnej.

Przekładając to na grunt relacji pracodawca – pracownik, prawnie uzasadnionym interesem pracodawcy zazwyczaj jest dochodzenie roszczeń lub obrona przed roszczeniami, które wynikają z umowy łączącej pracodawcę oraz pracownika. Stosowanie przez pracodawcę różnych form monitoringu (monitoring wizyjny, monitoring poczty służbowej) również stanowi jego prawnie uzasadniony interes, przez który należy rozumieć kolejno zapewnienie: bezpieczeństwa pracowników, ochrony mienia, kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, jak również organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwe użytkowanie udostępnionych pracownikowi narzędzi (art. 22^2 § 1 oraz 22^3 § 1 k.p.).

Prawnie uzasadnionym interesem dla przetwarzania danych pracowników jest często także potrzeba zapewnienia prawidłowej realizacji umów zawieranych przez pracodawcę, co wiąże się z koniecznością udostępnienia klientom i kontrahentom pracodawcy danych osobowych pracownika. W tym miejscu warto jednak zaznaczyć, że w literaturze podnosi się, iż przy udostępnianiu klientom i kontrahentom danych pracowników pracodawca może opierać się na art. 6 ust. 1 lit. b RODO – przetwarzanie danych osobowych jest niezbędne do realizacji umowy. Bez udostępnienia przedmiotowych danych osobowych pracownik może nie być w stanie wykonywać swoich obowiązków, zwłaszcza gdy w zakresie tych obowiązków leży np. kontakt z klientem i tworzenie/utrzymywanie relacji z klientem.

Dane szczególnych kategorii (dane wrażliwe)

Odrębnie należy omówić kwestię podstawy przetwarzania tzw. danych wrażliwych pracowników. Przetwarzając np. dane o stanie zdrowia, dane o przynależności do związków zawodowych czy też dane biometryczne, pracodawca musi zadbać, aby spełniony został jeden z warunków wskazanych w art. 9 ust. 2 RODO. Spośród obszernej listy zawartej we wskazanym artykule w stosunku do pracodawców zazwyczaj znajdą zastosowanie pierwsze dwie przesłanki przetwarzania danych osobowych wrażliwych, tj.:

- **pracownik wyraził wyraźną zgodę na przetwarzanie jego danych osobowych, np. zgodę na prze-**

twarzanie danych biometrycznych celem zabezpieczenia dostępu do pomieszczeń szczególnie istotnych (takich jak serwerownia),

- **przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez pracodawcę lub osobę fizyczną w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, np. przeprowadzenie badań pracowników, które są konieczne w ramach stosunku pracy, przetwarzanie danych zawartych w zaświadczeniach o stopniu niepełnosprawności (jeśli dotyczy) czy przetwarzanie danych o stanie zdrowia na potrzeby ZFŚS.**

W kontekście danych wrażliwych należy zwrócić uwagę na art. 22^{1b} k.p., zgodnie z którym pracodawca powinien zadbać o to, aby do przetwarzania takich danych zostały dopuszczone jedynie osoby posiadające pisemne upoważnienie do przetwarzania danych wrażliwych. Dodatkowo pracodawca, opierając przetwarzanie danych wrażliwych na zgodzie osoby fizycznej, musi mieć na względzie, że jest to możliwe wyłącznie w przypadku, gdy przekazanie tych danych osobowych następuje z inicjatywy pracownika. Wyjątkiem jest przetwarzanie danych biometrycznych, gdyż jest ono dopuszczalne także wtedy, gdy ich podanie jest niezbędne ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę, lub dostępu do pomieszczeń wymagających szczególnej ochrony.

ZAKRES ZBIERANYCH DANYCH W KONTEKŚCIE ZASADY MINIMALIZACJI – JAKIE DANE PRACOWNIKA MOŻNA POZYSKAĆ?

WIĘCEJ

Zgodnie z zasadą minimalizacji danych pracodawca powinien pozyskiwać jedynie dane osobowe adekwatne i stosowne do celów, w których są przetwarzane, czyli do realizacji procesu zatrudnienia. Pierwszy dokument, który przychodzi na myśl w zakresie pozyskiwania danych osobowych pracownika, to kwestionariusz osobowy. W wyniku zmiany rozporządzenia Ministra Pracy i Polityki Socjalnej w sprawie dokumentacji pracowniczej nie obowiązuje już oficjalny wzór kwestionariusza osobowego, lecz na stronie internetowej Ministerstwa opublikowano pomocniczy wzór.

Gromadząc więc informacje w kwestionariuszu osobowym, należy opierać się na art. 22^{1} k.p., zawierającym katalog danych, których pracodawca żąda od pracownika. Pracodawca często jednak staje przed dylematem, co zrobić, gdy potrzebuje innych danych pracownika niż te wymienione w powyższym artykule. Jakie inne dane mogą mu być potrzebne? Przede wszystkim dane osobowe niezbędne do zgłoszenia pracownika do ubezpieczeń społecznych. Pracodawca do wypełnienia zgłoszenia (ZUS ZUA), którego wzorzec jest określony przepisami prawa, musi uzyskać w szczególności takie informacje, jak:

- **numer PESEL,**
- **rodzaj, seria i numer dokumentu tożsamości,**
- **nazwisko rodowe,**
- **obywatelstwo,**
- **adres zameldowania,**
- **adres zamieszkania,**
- **adres do korespondencji.**

Podobnie jest w przypadku szkoleń BHP. Treść zaświadczenia o ukończeniu szkolenia zawiera informacje dotyczące miejsca urodzenia pracownika. W obu wskazanych sytuacjach należy mieć na uwadze, że zgodnie z art. 22^{1} § 4 k.p. pracodawca żąda podania innych danych osobowych, gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa. Za prawidłową praktykę należy więc uznać zwrócenie się przez pracodawcę do pracownika z wnioskiem o uzyskanie ww. informacji, ze wskazaniem, że ich przetwarzanie jest niezbędne na potrzeby prawidłowego wypełnienia przez pracodawcę odpowiednich przepisów prawa.

W tym miejscu należy zaznaczyć, że UODO i Ministerstwo Rodziny, Pracy i Polityki Społecznej wydały stanowiska w sprawie przechowywania dokumentacji pracowniczej, a mianowicie omawianej kwestii pozyskiwania danych potrzebnych do zgłoszenia pracownika do ubezpieczeń społecznych z ZUS. Ministerstwo jako niewłaściwe oceniło postępowanie pracodawców polegające na żądaniu wpisania danych niezbędnych do zgłoszenia do ZUS (w tym np. adresów zameldowania i do korespondencji czy informacji o prawie do emerytury) w treści kwestionariusza osobowego pracownika. Ministerstwo wskazuje, że takie dane powinny znaleźć się tylko w druku ZUS ZUA, argumentując to krótszym okresem przechowywania takich danych (patrz część „Okresy przechowywania danych osobowych"). Ponadto UODO zwraca uwagę na różne etapy procesu zatrudnienia, na których poszczególne dane powinny być pozyskiwane. O ile żądanie adresu zamieszkania od kandydata wyłonionego w trakcie rekrutacji, z którym umowa o pracę nie została jeszcze zawarta, jest zdaniem UODO dopuszczalne (uzasadnieniem jego pozyskania jest przecież konieczność zawarcia umowy o pracę), o tyle inne dane niezbędne do zgłoszenia pracownika do ubezpieczenia powinny być zebrane dopiero po podpisaniu umowy o pracę z uwagi na fakt, że zgłoszenia do ubezpieczenia dokonuje się w ciągu 7 dni od zawarcia umowy o pracę.

Zgodnie z powyższym pracodawcy powinni zaniechać zbierania w kwestionariuszu osobowym innych danych pracownika niż wskazane w art. 22^1 k.p. oraz zwracać uwagę na to, aby dane niezbędne do zgłoszenia do ubezpieczenia były zbierane za pomocą przeznaczonego do tego druku ZUS ZUA.

JAK SKUTECZNIE SPEŁNIĆ OBOWIĄZEK INFORMACYJNY?

Pracodawca powinien przekazać pracownikowi wszystkie informacje wymagane przez art. 13 RODO w momencie pozyskania jego danych osobowych. Przyjętą w tym zakresie praktyką jest zamieszczanie treści obowiązku informacyjnego w umowie o pracę zawieranej z pracownikiem bądź w treści kwestionariusza osobowego. Zazwyczaj dokumenty te pracownik otrzymuje łącznie, dlatego wybór, w którym z nich zamieszczony zostanie obowiązek informacyjny, należy do pracodawcy.

Obowiązek informacyjny powinien być także spełniony względem pracowników, którzy zostali zatrudnieni przed rozpoczęciem obowiązywania RODO. W tym przypadku przyjętym w praktyce i rekomendowanym rozwiązaniem jest skierowanie mailingu z obowiązkiem informacyjnym do tych pracowników. Pracodawca unikanie w ten sposób konieczności aneksowania zawartych umów o pracę czy też zmiany kwestionariuszy osobowych. Nic nie stoi również na przeszkodzie, aby klauzulę informacyjną przedstawić w formie papierowej i uzyskać pod nią podpis pracownika, a następnie wpiąć do jego akt osobowych celem wypełnienia zasady rozliczalności.

WSPÓŁPRACOWNICY

Jeśli chodzi o osoby zatrudnione na podstawie umów cywilnoprawnych, rysują się pewne różnice co do podstaw przetwarzania danych osobowych. Kodeks pracy nie znajdzie bowiem zastosowania w przedmiotowej sytuacji.

Podstawa prawna

W pierwszej kolejności należy wskazać, że dane osobowe współpracowników będą przetwarzane na podstawie art. 6 ust. 1 lit. b RODO, tj. w celu zawarcia i realizacji umowy. Jednak w przypadku współpracowników mogą pojawić się również inne podstawy prawne przetwarzania, jak chociażby art. 6 ust. 1 lit. c RODO w zakresie, w jakim współpracownik jest zgłaszany do ubezpieczeń społecznych. Ponadto często charakter świadczonych usług na rzecz przedsiębiorcy (np. usługi remontowe, budowlane)

może uzasadniać przetwarzanie danych współpracownika na potrzeby przeprowadzenia szkolenia BHP, pomimo że z przepisów prawa pracy nie wynika wprost obowiązek szkolenia w tym zakresie. Wówczas za podstawę prawną przetwarzania należy przyjąć prawnie uzasadniony interes administratora – art. 6 ust. 1 lit. f RODO – w postaci zapewnienia współpracownikowi bezpiecznych warunków pracy podczas świadczenia usług na rzecz przedsiębiorcy.

Niezależnie od powyższego w stosunku do współpracowników znajdzie zastosowanie podstawa prawna przetwarzania w postaci zgody. Na podstawie zgody często będzie przetwarzany wizerunek współpracownika – na zasadach analogicznych do tych, które obowiązują w przypadku pracowników. Oczywiście w tym zakresie administrator zawsze musi kierować się zasadą adekwatności, zgodnie z którą przetwarzać powinien jedynie dane niezbędne do osiągniecia określonych przez siebie celów (w tym przypadku jest to realizacja umowy o współpracy).

Zakres danych osobowych

W stosunku do współpracowników nie ma przepisów regulujących zakres danych, które mogą być przetwarzane przez administratora. Należy więc kierować się zasadą minimalizacji danych, czyli przetwarzać jedynie takie dane, które są niezbędne dla realizacji określonych wcześniej celów przetwarzania. Dobrą praktyką jest również wspomaganie się przepisami k.p., które regulują, jakich danych pracodawca może żądać od pracownika.

OBOWIĄZEK INFORMACYJNY WZGLĘDEM OSÓB TRZECICH POJAWIAJĄCYCH SIĘ W PROCESIE ZATRUDNIENIA

Pracodawca oprócz danych osobowych swoich pracowników zazwyczaj jest również w posiadaniu danych osobowych członków ich rodzin i ich bliskich. Osobom tym również muszą zostać przekazane wszystkie informacje, o których mowa w przepisach RODO. Nie znajdujemy w przepisach prawa wyłączenia, które zwalniałoby pracodawcę z przedmiotowego obowiązku. Istotne jest, że pracodawca w opisywanej sytuacji nie pozyskuje danych osobowych bezpośrednio od osoby, której dane dotyczą. Dane osobowe są przekazywane pracodawcy przez jego pracowników. Stąd pracodawca zobligowany jest dotrzeć do osób trzecich z informacjami wynikającymi z art. 14 RODO.

Jak spełnić obowiązek informacyjny z art. 14 RODO?
Z praktyki wynika, że najczęstszym sposobem wypełnienia przez pracodawców omawianego obowiązku jest zobowiązanie pracownika do przekazania osobom trzecim podanych mu informacji. Sam pracodawca miałby bowiem trudności z dotarciem do osób, które pracownik wskazał do kontaktu w razie w wypadku czy też w związku ze zgłoszeniem do obowiązkowego ubezpieczenia lub ZFŚS.

Zatem pracodawca, pozyskując powyższe dane osobowe od pracownika, powinien jednocześnie zebrać oświadczenie pracownika, że wskazane przez niego osoby zostaną poinformowane zgodnie z informacjami z art. 14 RODO, które pracodawca udostępnił pracownikowi celem przekazania tym osobom.

POWIERZENIE DANYCH OSOBOWYCH PRACOWNIKÓW

W stosunku zatrudnienia niejednokrotnie spotykamy się z powierzeniem danych osobowych pracowników na zewnątrz. Najczęściej dzieje się to w związku ze zleceniem przez pracodawcę zewnętrznym firmom różnych usług. Typowymi sytuacjami, gdy spotykamy się z powierzeniem przetwarzania danych pracowników przez pracodawcę, jest outsourcing usług księgowych, kadrowych czy też niszczenie dokumentacji firmowej. We wskazanych przykładach nie mamy wątpliwości, że pracodawca pozostaje administratorem danych osobowych swoich pracowników, natomiast zewnętrzne firmy wykonujące usługi, np. księgowe, są podmiotem przetwarzającym dane osobowe powierzone przez pracodawcę celem wykonywania usługi.

Pracodawca zobowiązany jest zawrzeć umowę powierzenia przetwarzania danych osobowych z każdym podmiotem przetwarzającym wykonującym usługi na jego rzecz. Treść takiej umowy powinna zawierać wszystkie elementy wskazane w art. 28 ust. 3 RODO, tj. przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych (zakres powierzanych danych osobowych pracowników), kategorie osób, których dane dotyczą, obowiązki i prawa administratora oraz obowiązki samego podmiotu przetwarzającego.

Udostępnienie danych osobowych czy powierzenie ich przetwarzania?

Istnienie stosunku powierzenia nie zawsze jest jednak klarowne. Czasem pracodawcy stają przed dylematem, czy w konkretnej sytuacji powinni zawrzeć umowę powierzenia z kontrahentem, czy może właściwym rozwiązaniem byłoby udostępnienie danych pracowników na zasadzie administrator – administrator.

Takie kontrowersje pojawiają się często w relacji **pracodawca – biuro podróży**. Większość pracodawców korzysta z usług takich podmiotów celem chociażby organizacji podróży służbowej. Pracodawca przekazuje wówczas do biura podróży szereg danych osobowych swojego pracownika. W ramach usług świadczonych przez biuro podróży pracodawca z reguły powierza do przetwarzania dane osobowe swoich pracowników. Następuje to w określonym przez pracodawcę celu, jakim jest obsługa procesu organizacji podróży służ-

bowej. Biuro podróży działa w omawianej relacji w imieniu i na rzecz pracodawcy – decyduje, gdzie i jakim środkiem transportu odbywa się podróż służbowa pracownika. W związku z tym biuro podróży w procesie organizacji wyjazdów służbowych w stosunku do danych osobowych pracowników przekazywanych przez pracodawcę pełni funkcję podmiotu przetwarzającego.

OKRESY PRZECHOWYWANIA DANYCH OSOBOWYCH

Zatrudnienie

Wraz z 1 stycznia 2019 r. nastąpiła istotna zmiana w długości okresu przechowywania akt osobowych pracowników. Zgodnie z art. 94 pkt 9b k.p. pracodawca jest zobowiązany przechowywać dokumentację pracowniczą przez okres 10 lat od końca roku kalendarzowego, w którym stosunek pracy uległ rozwiązaniu lub wygasł. Okres przechowywania dokumentacji pracowniczej znacznie więc skrócono – z 50 do10 lat – po wejściu w życie RODO. Akta osobowe pracowników zatrudnianych po 1 stycznia 2019 r. będą przechowywane już tylko 10 lat.

Jak zatem postępować z danymi osobowymi pracowników, które nie są zgromadzone w aktach osobowych? Powyższy przepis reguluje w szczególności okres przechowywania dokumentacji gromadzonej przez pracodawcę w aktach osobowych pracownika. Pracodawca często przetwarza dane osobowe pracowników, które nie są gromadzone w aktach osobowych jako część dokumentacji pracowniczej. W stosunku do nich okres przechowywania będzie więc znacznie krótszy. Jako przykład może posłużyć zdjęcie pracownika zamieszczone na stronie internetowej pracodawcy. Oczywiste jest, że w przywołanym przypadku zdjęcie pracownika powinno zostać usunięte ze strony niezwłocznie po rozwiązaniu stosunku pracy i że nie powinno być przechowywane przez pracodawcę.

Ponadto zgodnie z opisanym powyżej stanowiskiem UODO i Ministerstwa Rodziny, Pracy i Polityki Społecznej, dane osobowe, które są gromadzone na potrzeby zgłoszenia pracownika do ubezpieczenia (druk ZUS ZUA), powinny być przechowywane przez 5 lat od dnia ich przekazania do ZUS.

[3] Zob. tamże, s. 40.

Zakładowy fundusz świadczeń socjalnych

Podobna sytuacja rysuje się w odniesieniu do ZFŚS, jeżeli funkcjonuje u konkretnego pracodawcy. Dane osobowe gromadzone w związku z przyznawanymi pracownikowi świadczeniami w ramach ZFŚS również nie będą przechowywane przez pracodawcę przez 10 lat. Zgodnie bowiem z art. 8 ust. 1c ustawy o zakładowym funduszu świadczeń socjalnych pracodawca przetwarza dane osobowe osoby uprawnionej do korzystania z ZFŚS przez okres niezbędny do przyznania ulgowej usługi i świadczenia, dopłaty z ZFŚS oraz ustalenia ich wysokości, a także przez okres niezbędny do dochodzenia praw lub roszczeń.

Pracodawca – ustalając, jak długo powinien przechowywać dane osobowe swoich pracowników – powinien kierować się więc nie tylko wymogami k.p., lecz także przepisami szczególnymi oraz zasadą ograniczenia przechowywania, wyrażoną w RODO. Zgodnie ze wskazaną zasadą należy mieć na uwadze, że dane osobowe powinny być przechowywane nie dłużej, niż jest to niezbędne do celów, w których przedmiotowe dane osobowe zostały zgromadzone.

Osoby zatrudnione na podstawie umów cywilnoprawnych

Zasada ograniczenia przechowywania odgrywa szczególnie istotną rolę w przypadku osób zatrudnionych na podstawie umów cywilnoprawnych. Jak wskazywano wyżej, do tej grupy osób nie znajdą bowiem zastosowania przepisy k.p. W związku z tym, określając czas przechowywania danych osobowych, pracodawca powinien wziąć w szczególności pod uwagę:

- **okres trwania umowy,**
- **okres ewentualnego dochodzenia roszczeń związanych z umową (okres przedawnienia roszczeń),**
- **obowiązki wynikające z przepisów prawa.**

Na powyższe przesłanki wskazuje również UODO w poradniku dla pracodawców[3].

W większości przypadków umów cywilnoprawnych podstawą prawną przetwarzania danych osobowych jest niezbędność ich przetwarzania do wykonania umowy cywilnoprawnej, której stroną jest osoba, której dane dotyczą,

lub niezbędność do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy. Takie dane osobowe będą więc przechowywane przez okres trwania umowy oraz po jej zakończeniu przez okres dochodzenia ewentualnych roszczeń związanych z umową.

Zdarza się jednak również, że część danych osobowych jest gromadzona w związku z obowiązkami prawnymi ciążącymi na administratorze, np. obowiązkiem zgłoszenia pracownika do ubezpieczenia zdrowotnego czy też – w niektórych przypadkach – obowiązkiem ukończenia przez niego szkolenia z zakresu BHP. Wówczas terminów przechowywania danych osobowych należy doszukiwać się w przepisach prawa.

Marketing

FORMY MARKETINGU A PODSTAWY PRAWNE PRZETWARZANIA DANYCH OSOBOWYCH

E-mail marketing (newsletter)

Informowanie klientów oraz subskrybentów, którzy udostępnili przedsiębiorcy swój adres e-mail, o oferowanych usługach, promocjach itp. jest jedną z najbardziej popularnych, a tym samym najczęściej wykorzystywanych przez przedsiębiorców form e-mail marketingu. Podstawą prawną przetwarzania danych osobowych w celu wysyłki newslettera jest prawnie uzasadniony interes administratora w postaci marketingu bezpośredniego jego usług i produktów. Powyższe potwierdza treść motywu 47 RODO, w którym czytamy: „Za działanie wykonywane w prawnie uzasadnionym interesie można uznać przetwarzanie danych osobowych do celów marketingu bezpośredniego". Warto więc pamiętać, że pozyskiwanie zgody na przetwarzanie danych osobowych dla celów wysyłki newslettera jest zbędne, gdyż przedsiębiorca, posiadając prawnie uzasadniony interes, przetwarza dane osobowe na podstawie art. 6 ust. 1 lit. f RODO.

Telemarketing

Popularną formą marketingu jest również telemarketing. Wydaje się, że jest on odbierany stosunkowo negatywnie przez ogół społeczeństwa, ponieważ często jest traktowany jako nękanie przez telemarketerów oferujących przeróżne usługi czy produkty. Dla przedsiębiorców podstawą prawną tego rodzaju marketingu jest prawnie uzasadniony interes administratora, czyli marketing bezpośredni produktów/usług. Wielu przedsiębiorców zapomina jednak, że oprzeć przetwarzanie danych osobowych w celach marketingowych na wskazanej podstawie można tylko wtedy, gdy osoba, której dane dotyczą, ma rozsądne przesłanki, by spodziewać się, że jej dane będą przetwarzane w konkretnym celu. W tym miejscu należy pamiętać również o przeprowadzeniu tzw. testu prawnie uzasadnionego interesu, o którym była mowa przy okazji analizy podstaw prawnych przetwarzania danych w procesie zatrudnienia.

Wobec tego o ile co do zasady nie ma wątpliwości, że dzwonienie pod numery znajdujące się w bazie naszych klientów nie narazi nas na zarzut wykorzystywania danych osobowych bez wiedzy konkretnej osoby, o tyle jeżeli korzystamy z publicznie dostępnych baz danych lub baz danych zakupionych z niesprawdzonych źródeł, z całą pewnością nie możemy przypuszczać, że osoba fizyczna spodziewa się kierowanej do niej oferty.

Powyższy problem nie aktualizuje się w tak dużym stopniu przy e-mail marketingu – głównie dlatego że ta forma jest znacznie mniej uciążliwa niż bezpośredni telefon do osoby fizycznej. Oprócz tego newsletter zazwyczaj kierowany jest do osób, które wcześniej same udostępniły swój adres e-mail celem jego otrzymywania. Niemniej wykorzystywanie adresów poczty elektronicznej do celów marketingowych bez wiedzy osób fizycznych, których dane dotyczą, pozostaje aktualnym zagadnieniem również przy e-mail marketingu, gdyż także w tym przypadku administratorzy niejednokrotnie wspomagają swoje działania marketingowe zakupionymi – nie zawsze ze sprawdzonych źródeł – bazami adresów e-mail.

E-mail marketing oraz telemarketing a zgody z ustaw szczególnych

Administrator, który prowadzi marketing przez e-mail oraz telemarketing, musi mieć na uwadze nie tylko przepisy RODO, lecz także przepisy ustawy o świadczeniu usług drogą elektroniczną (u.ś.u.d.e.) oraz ustawy – Prawo telekomunikacyjne (p.t.). Zgodnie z art. 10 u.ś.u.d.e. oraz art. 172 p.t. kontakt telefoniczny lub mailowy z osobą fizyczną w celach marketingowych dozwolony jest jedynie wówczas, gdy osoba ta wyrazi zgodę na konkretny sposób komunikacji. Administrator nie musi więc zbierać zgody na przetwarzanie danych, o której mowa w art. 6 ust. 1 lit. a RODO, gdyż dysponuje już podstawą prawną przetwarzania danych wyrażoną w art. 6 ust. 1 lit. f RODO. Jednak od zgód nie ucieknie, ponieważ musi je uzyskać stosownie do wskazanych wyżej przepisów szczególnych.

Mając powyższe na uwadze, istotne dla administratorów danych są zmiany, jakie do u.ś.u.d.e. oraz do p.t. wprowadziła ustawa o zmianie niektórych ustaw w związku z RODO, by dostosować treść ich przepisów do wymogów RODO. Zmiany te dotykają bowiem właśnie zgody, o której mowa w omawianych ustawach szczególnych.

Stosownie do RODO zgoda to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, zgodnie z któ-

rym osoba, której dane dotyczą, przyzwala na przetwarzanie jej danych osobowych, udzielając oświadczenia w formie pisemnej bądź poprzez wyraźne działanie. Po zmianach wprowadzonych do omawianych ustaw szczególnych zgoda wymagana na gruncie art. 10 u.ś.u.d.e. oraz art. 172 p.t. powinna spełniać następujące wymogi:

- **osoba fizyczna, wyrażając zgodę w pisemnym oświadczeniu, które obejmuje również inne kwestie, musi być w stanie odróżnić treść samej zgody. Zgoda ta powinna być więc sformułowana jasnym i prostym językiem, w zrozumiałej oraz łatwo dostępnej formie,**
- **administrator musi pozyskać zgodę w taki sposób, aby był w stanie udowodnić, że osoba, której dane dotyczą, wyraziła przedmiotową zgodę na konkretny cel,**
- **udzielona zgoda może zostać w każdym momencie wycofana, a wycofanie zgody nie może wpływać na zgodność z prawem przetwarzania danych osobowych dokonywanego na podstawie zgody przed jej wycofaniem,**
- **administrator zobligowany jest do poinformowania osoby fizycznej o możliwości wycofania zgody,**
- **wycofanie zgody powinno być tak samo łatwe jak jej udzielenie (tj. administrator nie powinien nakładać na osobę fizyczną obowiązku wysłania listu poleconego na adres siedziby administratora celem wycofania zgody, jeżeli do jej udzielenia wystarczyło zaznaczenie checkboxa),**
- **administrator, oceniając dobrowolność wyrażonej zgody, w szczególności powinien zwrócić uwagę, czy od udzielenia zgody nie jest uzależnione inne świadczenie, np. świadczenie usługi w związku z zawartą umową.**

WIĘCEJ

Biorąc pod uwagę powyższe, administrator, który kieruje marketing bezpośredni na podstawie prawnie uzasadnionego interesu do osoby fizycznej, musi pamiętać o pozyskaniu legalnej podstawy do komunikacji za pośrednictwem e-maila lub numeru telefonu, o której mowa w przepisach u.ś.u.d.e. oraz p.t.

Natomiast **jeśli osoba fizyczna nie jest klientem administratora i nie spodziewa się działań marketingowych ze strony konkretnego przedsiębiorcy**, to administrator powinien pamiętać, że nie może oprzeć przetwarzania danych osobowych takiej osoby na prawnie uzasadnionym interesie w postaci marketingu bezpośredniego. Konieczne będzie uzyskanie przez przedsiębiorcę zgody w rozumieniu art. 6 ust. 1 lit. a RODO na przetwarzanie danych osobowych w celach marketingowych.

Zważając na wspomniany już fakt, że zgoda może polegać na oświadczeniu bądź zachowaniu, które w określonej sytuacji wyraźnie wskazuje, że osoba, której dane dotyczą, wyraża zgodę na określone przetwarzanie jej danych osobowych, osoba fizyczna może wyrazić zgodę poprzez samo działanie potwierdzające określoną czynność. Wskazuje na to motyw 32 RODO. Zgoda nie musi więc być zgromadzona w formie klauzuli: „Wyrażam zgodę na….", która będzie opatrzona podpisem osoby fizycznej.

Mając na uwadze omawiane przepisy u.ś.u.d.e. oraz p.t., wskazane oświadczenie może zostać skonstruowane w taki sposób, aby spełniało wymogi zarówno RODO, jak i ustaw szczególnych. Dla zobrazowania poniżej przedstawiamy przykład łączonej zgody – oświadczenia informującego o przetwarzaniu danych osobowych dla celów marketingowych połączonego ze zgodą na wysyłanie informacji handlowych z wykorzystaniem adresu e-mail, tj. zgodą na kanał komunikacji.

Przykład: *Uzupełniając swój adres e-mail w niniejszym formularzu, zgadzasz się na regularne otrzymywanie na swój adres e-mail informacji handlowych zawierających treści o produktach i usługach* …… [nazwa przedsiębiorcy].

Jednocześnie informujemy, że na potrzeby wysyłki do Ciebie przedmiotowych informacji handlowych …… [nazwa przedsiębiorcy] *będzie przetwarzał Twoje dane osobowe. Udostępniając więc swój adres e-mail oraz zaznaczając powyższy przycisk (checkbox), godzisz się na przetwarzanie Twoich danych osobowych we wskazanym wyżej celu i zakresie. Twoje dane osobowe nie będą przetwarzane w żadnych innych celach.*

Pamiętaj, że udzieloną zgodę możesz wycofać w każdej chwili bez żadnych negatywnych konsekwencji. W celu wycofania zgody …… [administrator powinien w tym miejscu zaproponować najlepsze w konkretnej sytuacji rozwiązanie, które będzie równie proste jak udzielenie zgody, np. wysłanie wiadomości e-mail na adres administratora]. *Wycofanie zgody nie wpłynie jednak na zgodność z prawem przetwarzania dokonanego na jej podstawie przed wycofaniem zgody.*

POZOSTAŁE FORMY MARKETINGU – EVENTY ORAZ KONKURSY

Kolejną popularną formą promowania przez przedsiębiorcę firmy jest organizowanie różnych eventów oraz konkursów zarówno dla obecnych, jak i dla potencjalnych klientów. Jak przeprowadzać przedmiotowe wydarzenia zgodnie z przepisami RODO?

Event marketing, czyli pikniki, imprezy biznesowe, konferencje tematyczne itp.

Ta forma marketingu staje się coraz popularniejsza wśród przedsiębiorców. Służy nie tylko zwiększeniu lojalności pracowników oraz obecnych kontrahentów i klientów, lecz także pozyskaniu nowych. Niewątpliwie z organizacją przedmiotowych wydarzeń wiąże się przetwarzanie danych osobowych ich uczestników.

Podstawa prawna

Organizator wydarzenia, przetwarzając dane osobowe jego uczestników, musi pamiętać o posiadaniu ważnej podstawy prawnej przetwarzania. Uczestnicy, którzy zdecydują się wziąć udział w konkretnym evencie, zazwyczaj są zobligowani do zaakceptowania warunków uczestnictwa, określonych w regulaminie wydarzenia. W tym przypadku dane osobowe osób biorących udział w wydarzeniu administrator będzie więc przetwarzał na podstawie art. 6 ust. 1 lit. b ROOD, w celu zawarcia i realizacji umowy. Za umowę należy bowiem uznać wiążący przedsiębiorcę i uczestników wydarzenia regulamin. W razie braku omawianego regulaminu na administratorze ciąży pozyskanie od uczestników odpowiedniej zgody na przetwarzanie danych osobowych w związku z udziałem w wydarzeniu.

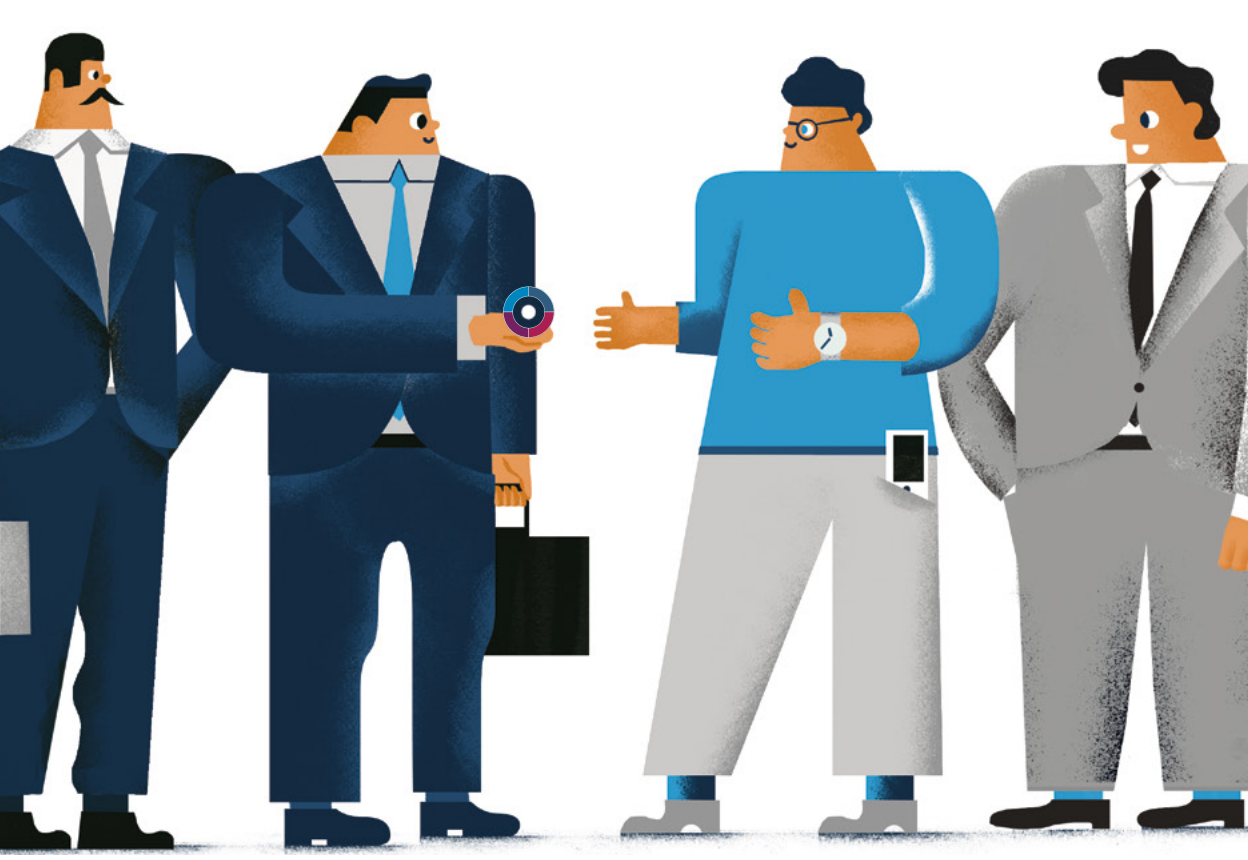
Utrwalanie i rozpowszechnianie wizerunku podczas eventów

Nieodłącznym elementem wydarzeń organizowanych przez przedsiębiorców jest fotorelacja. Zdjęcia często są zamieszczane w gazetkach firmowych, intranecie, mediach społecznościowych prowadzonych przez przedsiębiorcę czy też na firmowej stronie internetowej. Administrator danych powinien pamiętać, że jeśli zdecyduje się na fotorelacje podczas organizowanego wydarzenia, aby później używać zdjęć w celach marketingowych i tym samym rozpowszechniać utrwalony na nich wizerunek, potrzebuje zgody osoby fizycznej. Co istotne, przedmiotowa zgoda obwarowana jest przepisami u.p.a.p.p. (o zgodzie wynikającej z art. 81 u.p.a.p.p. była już mowa w części dotyczącej procesu zatrudnienia, przy okazji zamieszczania wizerunku pracownika na firmowej stronie internetowej). Należy mieć na uwadze, że z rozpowszechnianiem wizerunku mamy do czynienia niewątpliwie wtedy, gdy dociera on do nieokreślonego kręgu osób. Za rozpowszechnianie należy więc uznać publikowanie zdjęć w social mediach czy na firmowej stronie internetowej, ale również – co bywa kontrowersyjne – w firmowej gazetce.

O ile więc przetwarzamy dane osobowe w postaci wizerunku na podstawie art. 6 ust. 1 lit. b RODO – jeśli administrator w regulaminie zastrzegł, że na wydarzeniu będą robione zdjęcia – o tyle na rozpowszechnianie wizerunku musimy pozyskać zgodę wynikająca z ustawy szczególnej. Częstą praktyką wśród administratorów – w szczególności jeśli z regulaminu wydarzenia nie wynika wyraźnie możliwość fotografowania uczestników – jest zbieranie łączonych zgód na przetwarzanie danych osobowych w postaci wizerunku w związku z udziałem w konkretnym wydarzeniu oraz na późniejsze rozpowszechnianie wizerunku. Należy pamiętać, aby przy pozyskiwaniu zgody wynikającej z u.p.a.p.p. zawrzeć w treści zgody wszystkie elementy, których wymaga ustawa szczególna, tj. w szczególności miejsce i czas publikacji, pola eksploatacji, możliwość zestawienia z konkretną treścią oraz wizerunkami innych osób.

Warto również zaznaczyć, że celem organizowania różnych eventów jest dla administratora również rozbudowanie swoich baz marketingowych. W związku z tym administrator powinien pamiętać o pozyskaniu od uczestników, których dane osobowe nie znajdują się w jego bazach, stosownych zgód marketingowych, o których mowa była powyżej, w szczególności zaś zgody na odpowiedni kanał komunikacji, do której obligują przepisy u.ś.u.d.e. oraz p.t.

WIĘCEJ



Konkursy

Podstawa prawna

Podstawą prawną przetwarzania danych osobowych uczestników konkursu jest prawnie uzasadniony interes administratora danych, tj. art. 6 ust. 1 lit. f RODO, rozumiany jako organizacja konkursów, w tym obsługa zgłoszeń, informowanie o wynikach i wyłanianie zwycięzców oraz przyznawanie i wysyłanie nagród konkursowych. Oczywiście opierając przetwarzanie danych na prawnie uzasadnionym interesie administratora, nie możemy zapominać o teście równowagi, polegającym na porównaniu wagi interesu administratora, realizowanego w związku z konkretną czynnością przetwarzania danych, z interesami lub podstawowymi prawami i wolnościami podmiotu danych.

Dopuszczalne jest również uzyskiwanie zgody na przetwarzanie danych na potrzeby konkursu zgodnie z art. 6 ust. 1 lit. a RODO. Taka zgoda może zostać wyrażona poprzez aktywne działanie, tj. zgłoszenie chęci udziału w konkursie (motyw 32 RODO).

Konkurs jako przyrzeczenie publiczne

Za błędną należy uznać pojawiającą się praktykę wskazywania podstawy prawnej przetwarzania danych uczestników konkursu jako art. 6 ust. 1 lit. b RODO, tj. przetwarzanie jest niezbędne do wykonania umowy. Problem konstrukcji prawnej konkursu jako umowy lub przyrzeczenia publicznego był już kilkukrotnie rozstrzygany przez judykaturę. W związku z tym należałoby przychylić się do stwierdzenia, że konkurs jest co do zasady przyrzeczeniem publicznym, a w konsekwencji odstąpić od przyjmowania art. 6 ust. 1 lit. b RODO (przetwarzanie jest niezbędne do wykonania umowy) za podstawę prawną przetwarzania danych osobowych.

OBOWIĄZEK INFORMACYJNY – GDZIE I W JAKIEJ FORMIE NAJLEPIEJ GO SPEŁNIAĆ?

Administrator, który prowadzi marketing w dowolnej formie, nie może zapomnieć o spełnieniu obowiązku informacyjnego względem zainteresowanych osób. W zależności od formy marketingu rysują się różne możliwości spełnienia wymogu przekazania osobom fizycznym informacji wyszczególnionych w RODO.

Strona WWW

W tym miejscu warto wyszczególnić stronę internetową, którą ma znakomita większość przedsiębiorców, a z którą z reguły powiązane jest prowadzenie marketingu. Formularze zapisów na newsletter lub na organizowane przez firmę wydarzenia dostępne są często właśnie z poziomu strony internetowej, podobnie jak konkursy, które najczęściej są organizowane za pośrednictwem strony WWW lub przez social media. W związku z tym nie-

zwykle istotne jest dostosowanie firmowej strony internetowej do wymogów RODO. Obowiązek informacyjny powinien w szczególności znajdować się pod wspomnianymi formularzami dostępnymi na stronie administratora, tak aby osoba fizyczna przed wpisaniem swoich danych osobowych mogła uzyskać wymagane przez art. 13 RODO informacje dotyczące ich przetwarzania.

Częstym problemem spotykanym w praktyce jest zbyt mało miejsca na zamieszczenie klauzuli informacyjnej pod formularzem na stronie internetowej. Wówczas warto pamiętać o możliwości warstwowego spełnienia obowiązku informacyjnego. Pierwszą warstwę informacji należy zamieścić bezpośrednio pod formularzem, natomiast do reszty informacji powinien odsyłać bezpośredni link. Przyjmuje się, że w pierwszej warstwie informacji znajduje się informacja o administratorze, celach przetwarzania i prawach przysługujących osobie fizycznej na gruncie przepisów RODO. Reszta obowiązku informacyjnego, do którego zostanie przekierowana osoba fizyczna za pośrednictwem linku, może zostać zamieszczona np. w polityce prywatności czy w odrębnej zakładce na stronie internetowej, poświęconej ochronie danych osobowych.

Uwaga: Jeśli w ramach działań marketingowych pozyskujemy dane osobowe poprzez rozdawane podczas eventów formularze czy ankiety w formie papierowej, to musi znajdować się na nich treść klauzuli informacyjnej.

Obowiązek informacyjny wobec osób fizycznych, których dane osobowe znajdują się już w bazie marketingowej

Do takich osób również powinny zostać skierowane informacje wymagane przez RODO, jeżeli nie przekazano ich w momencie, gdy osoby te podawały swoje dane osobowe. Droga realizacji tego obowiązku jest różna w zależności od rodzaju danych osobowych, jakie administrator posiada. Jeżeli dysponuje adresami e-mail osób fizycznych, najlepszą praktyką jest rozesłanie klauzuli informacyjnej pocztą elektroniczną – co zresztą uczyniło wiele firm po wejściu w życie RODO (e-maile z informacjami wymaganymi przez RODO pojawiły się w skrzynkach większości z nas).

OKRESY PRZECHOWYWANIA DANYCH

W procesie marketingowym ustalenie i przestrzeganie konkretnych okresów przechowywania danych sprawia trudności wielu administratorom, decyzja o usunięciu bazy marketingowej nie jest bowiem łatwa. Często pojawia się też wątpliwość, jak długo przechowywać zgromadzone dane osobowe, czego efektem jest przechowywanie zbudowanych baz marketingowych bezterminowo. Rozważając okres przechowywania danych osobowych, musimy pamiętać w szczególności o dwóch zasadach wyrażonych w RODO. Zgodnie z pierwszą z nich dane osobowe przetwarzamy tak długo, jak długo istnieje cel przetwarzania, dla którego zostały one zgromadzone. Natomiast stosownie do zasady prawidłowości dane osobowe, które przetwarzamy, muszą być prawidłowe i w razie potrzeby uaktualniane.

Administrator danych po zakończeniu kampanii marketingowej, przeprowadzonej celem np. promocji swojej nowej usługi, powinien usunąć bądź zanonimizować dane osobowe odbiorców zainteresowanych tą konkretną kampanią. Jeżeli zaś działania marketingowe są prowadzone stale (taki sposób marketingu jest znacznie częstszy niż akcje jednorazowe), to administrator jest zobowiązany zaprzestać przetwarzania danych osobowych w celach marketingowych, gdy zdezaktualizuje się podstawa prawna, na której opiera przetwarzanie danych osobowych. Należy przez to rozumieć odpowiednio:

- **wniesienie sprzeciwu przez osobę, której dane dotyczą, jeżeli podstawą przetwarzania jest prawnie uzasadniony interes administratora,**
- **wycofanie zgody przez osobę, której dane dotyczą, jeżeli przetwarzanie jej danych odbywa się na podstawie udzielonej zgody.**

Administrator, który straci podstawę przetwarzania danych wykorzystywanych do promocji swojej marki oraz usług, powinien natychmiast zaprzestać przetwarzania danych osobowych w tym celu. Należy przy tym zwrócić uwagę, że zaprzestanie przetwarzania danych w celach marketingowych dla administratora nie zawsze będzie wiązało się z ich usunięciem, ponieważ często aktualne pozostają inne cele przetwarzania zgromadzonych danych, a najczęstszym z nich jest możliwość dochodzenia ewentualnych roszczeń i obrony przed nimi. Jednak w takiej sytuacji administrator musi liczyć się z tym, że

dane osobowe, które przechowuje np. ze względu na obronę przed roszczeniami, nie mogą już być wykorzystane do celów marketingowych.

Jak wspomniano, administrator powinien respektować zasadę prawidłowości danych przetwarzanych w swoich zbiorach, co jest istotne w szczególności, gdy działania marketingowe prowadzone są stale, a dane osobowe nie są usuwane po zakończeniu konkretnej kampanii. Wówczas administrator musi podejmować wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane. Może to być realizowane np. poprzez umieszczenie w wiadomości e-mail dodatkowej informacji o treści:

Przykład: *Pamiętaj, że zawsze możesz sprostować swoje dane osobowe, jeżeli utracą swoją aktualność. Administrator usunie wówczas niezwłocznie Twoje nieprawidłowe/nieaktualne dane osobowe.*

KWESTIE BUDZĄCE NAJWIĘCEJ WĄTPLIWOŚCI

Kupowanie baz danych

Kupowanie baz danych jest obecnie dość powszechną praktyką wśród administratorów. Wciąż aktualne pozostają jednak pytania: czy to na pewno legalne? jak zakupić bazę danych zgodnie z prawem?

Należy wskazać, że RODO nie wyłączyło możliwości kupowania baz danych, w związku z tym nie jest to działanie niezgodne z prawem. Problem jednak stanowi częste nabywanie przez administratorów niesprawdzonych baz danych, bez próby weryfikacji, w jaki sposób dane osobowe zostały zgromadzone przez zbywcę bazy. Ta weryfikacja jest niezwykle istotna, gdyż po nabyciu bazy danych stajemy się administratorem danych osobowych w niej zgromadzonych, a więc jesteśmy zobligowani do realizacji wszystkich wymogów RODO. Przede wszystkim administrator powinien być świadomy, czy dysponuje ważną podstawą prawną przetwarzania pozyskanych danych osobowych. Przed nabyciem konkretnej bazy danych powinniśmy więc zbadać, czy podmiot zbywający uzyskał dane osobowe w sposób legalny. Ponadto należy ustalić, czy zbywca pozyskał dane osobowe bezpośrednio od tej osoby, czy również od podmiotu trzeciego. Konieczne jest zatem ustalenie podstawy prawnej przetwarzania danych osobowych przez zbywcę. Z reguły w takiej sytuacji podstawę prawną przetwarzania będzie stanowiła zgoda udzielona przez osobę, której dane dotyczą, tj. art. 6 ust. 1 lit. a RODO. Kupując bazę danych, powinniśmy zadbać o pozyskanie od zbywcy zgód od wszystkich osób, których dane osobowe znajdują się w bazie. Bardzo ważne jest to, aby zgoda została uzyskana także na czynność sprzedaży/udostępnienia podmiotowi trzeciemu danych zgromadzonych w bazie. Zebranie zgody jedynie na cele marketingowe – wyłączając kwestię udostępnienia danych podmiotowi trzeciemu – należy uznać za niewystarczające.

Podsumowując, kupując bazę danych, nie możemy rezygnować z dokładnej weryfikacji zbywcy pod kątem zgromadzenia danych osobowych oraz istnienia ważnych podstaw prawnych przetwarzania danych osobowych zgromadzonych w bazie.

Wysyłanie zapytań z prośbą o wyrażenie zgody na marketing

Analizując wskazane zagadnienie, należy w pierwszej kolejności wziąć pod uwagę przepis art. 10 u.ś.u.d.e. Zgodnie z nim zakazane jest wysyłanie wiadomości e-mail zawierających informacje handlowe bez zgody odbiorcy będącego osobą fizyczną. Definicja informacji handlowej ma bardzo szeroki zakres przedmiotowy. W doktrynie pojawia się stanowisko, że samo zapytanie o możliwość przesyłania takich informacji należy uznać za mieszczące się w tej definicji. Wysyłanie takich zapytań niejednokrotnie jest więc komentowane jako próba obejścia art. 10 u.ś.u.d.e. Niemniej jest to kwestia sporna, w praktyce nie do końca rozstrzygnięta, gdyż pojawiają się również głosy przeciwne, wskazujące, że samo zapytanie o charakterze informacyjnym – zawierające jedynie informacje o przedsiębiorcy i jego produktach/usługach – nie powinno być odczytywane jako przesyłanie niezamówionej informacji handlowej. Korzystając jednak z takiej formy pozyskiwania klientów, należy być bardzo ostrożnym, aby nie narazić się na zarzut działania niezgodnego z art. 10 u.ś.u.d.e.

Jeżeli chodzi o połączenia telefoniczne, należy przywołać przepis art. 172 p.t., który zakazuje używania telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących do celów marketingu bezpośredniego. Stanowiska Urzędu Komunikacji Elektronicznej (UKE) oraz Urzędu Ochrony Konkurencji i Konsumentów (UOKiK) w tym zakresie nie są jednolite. Zatem również w tym przypadku trudno jednoznacznie stwierdzić, czy sam telefon z zapytaniem o zgodę byłby uznany za działanie sprzeczne z art. 172 p.t. Biorąc jednak pod uwagę wyczulenie społeczeństwa na „nękające" telefony z ofertami marketingowymi różnych firm oraz rozbieżne stanowiska UKE i UOKiK, ta forma pozyskiwania zgód powinna być wykorzystywana przez administratorów w szczególnych sytuacjach – na pewno nie należy jej nadużywać. Ryzykowbiem, że narazimy się na zarzut obejścia omawianych przepisów sektorowych, jest dość wysokie.

Działania marketingowe a zgoda na pliki cookies

W tym zakresie ustawa o zmianie niektórych ustaw w związku z RODO nie wprowadziła zmian do treści

art. 173 p.t., regulującego kwestię zgód na stosowanie cookies. Zgodnie z art. 173 ust. 2 p.t. abonent lub użytkownik końcowy może wyrazić zgodę, o której mowa w art. 173 ust. 1 pkt 2 p.t., za pomocą ustawień oprogramowania zainstalowanego w wykorzystywanym przez niego telekomunikacyjnym urządzeniu końcowym lub konfiguracji usługi.

W związku z powyższym zgoda na stosowanie cookies – również w celach marketingowych – może być udzielona za pomocą ustawień przeglądarki. Osoba fizyczna, która nie chce wyrażać zgody na pliki cookies, powinna więc zmienić ustawienia przeglądarki, z której korzysta. Nie ma obowiązku pozyskiwania odrębnej zgody w tym zakresie przez przedsiębiorcę. Warto jednak zwrócić uwagę, że zgoda na pliki cookies – stanowiąca dla przedsiębiorcy podstawę dostępu do takich danych – nie zastępuje konieczności posiadania podstawy prawnej przetwarzania danych osobowych przez administratora. W tym przypadku najczęściej będzie to prawnie uzasadniony interes administratora w postaci marketingu, tj. art. 6 ust. 1 lit. f RODO.

Sprzedaż i obsługa klienta

ZANIM DOJDZIE DO SPRZEDAŻY, CZYLI OFERTOWANIE

Aby sprzedać towar czy usługę, najpierw trzeba znaleźć nabywcę, a przynajmniej potencjalnego nabywcę. Kwestie związane z prowadzeniem działań marketingowych szczegółowo omówiliśmy w rozdziale dotyczącym marketingu, w tym miejscu natomiast skupimy się na samej czynności związanej z przedstawieniem oferty, czyli: komu ofertę możemy przedstawić, czy RODO wymaga od nas podjęcia dodatkowych działań w tym obszarze i jak długo powinniśmy przetwarzać dane pozyskiwane w ramach procesu ofertowania.

Jak pozyskiwać klientów zgodnie z RODO?

Istnieją dwa sposoby na pozyskanie klientów: klient zgłosi się z prośbą o ofertę sam albo to organizacja nawiąże z nim kontakt, czego wynikiem będzie przesłanie oferty.

Oferta na prośbę klienta

W przypadku gdy to potencjalny klient sam zgłosi się z prośbą o przedstawienie oferty lub wyrazi zainteresowanie produktem i poprosi o dodatkowe informacje (np. uzupełniając formularz ofertowy na stronie WWW czy prosząc o to telefonicznie/mailowo), podstawą prawną przetwarzania będzie art. 6 ust. 1 lit. b RODO. Wskazana podstawa mówi bowiem o przetwarzaniu niezbędnym do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy, z czym będziemy mieli niewątpliwie do czynienia w przypadku danych osoby, która docelowo ma być stroną umowy. W zakresie zaś, w jakim kontakt w celu przedstawienia oferty wymaga przetwarzania danych pracowników/przedstawicieli potencjalnego klienta, podstawą prawną przetwarzania ich danych będzie art. 6 ust. 1 lit. f RODO – prawnie uzasadnionym interesem będzie wymiana informacji/korespondencji w celu zawarcia umowy.

Oferta bez prośby klienta

Natomiast kontakt z klientem, który nie złożył samodzielnie zapytania ofertowego, należy zakwalifikować jako formę działań marketingowych. Jeszcze raz podkreślamy, że ważne jest to, aby **informację handlową czy treści marketingowe przesyłać wyłącznie do podmiotów, które się na to uprzednio zgodziły**.

Należy wyróżnić następujące źródła pozyskania danych klientów, którym wysyła się ofertę:

- **źródła powszechnie dostępne (np. publiczne rejestry typu CEiDG czy zakładki „kontakt" na stronach WWW),**
- **bazy byłych lub obecnych klientów,**
- **kupione bazy danych (patrz rozdział „Marketing").**

Jeśli zidentyfikujemy konkretne działania jako marketingowe, to zgodnie z motywem 47 RODO podstawą prawną przetwarzania danych osobowych powinien być art. 6 ust. 1 lit. f RODO, czyli prawnie uzasadniony interes, którym jest kierowanie ofert/marketingu bezpośredniego do potencjalnych nabywców. Nie oznacza to jednak, że prawnie uzasadniony interes pojawia się automatycznie w każdej sytuacji, w której decydujemy się reklamować nasze produkty. Aby stwierdzić jego istnienie, należy każdorazowo przeprowadzić ocenę, czy interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, nie są nadrzędne wobec interesu administratora (więcej na ten temat pisaliśmy w rozdziałach dotyczących procesów zatrudnienia i marketingu). RODO wprost statuuje, że taki prawnie uzasadniony interes może istnieć, gdy zachodzi „istotny i odpowiedni rodzaj powiązania między osobą, której dane dotyczą, a administratorem, na przykład gdy osoba, której dane dotyczą, jest klientem administratora lub działa na jego rzecz" (motyw 47 RODO).

Powyższe rozwiewa wątpliwości co do wykorzystywania danych obecnych klientów. Przy czym przypominamy, że posiadanie podstawy prawnej z RODO to jedno, a uzyskanie odpowiedniej zgody z przepisów szczególnych to drugie. Bez odpowiedniej zgody na przesyłanie informa-

cji konkretnym kanałem komunikacji (e-mail/telefon/SMS) administrator może prowadzić działania marketingowe wyłącznie tradycyjną drogą pocztową.

W przedmiocie pozyskiwania danych osobowych ze źródeł powszechnie dostępnych sytuacja jest analogiczna. Jeśli administrator dysponuje prawnie uzasadnionym interesem (ewentualnie zgodą na przetwarzanie z art. 6 ust. 1 lit. a RODO), dane te może przetwarzać, a nawet wykorzystywać do celów marketingu, jednak użycie takich kanałów komunikacji jak e-mail czy telefon rodzi potencjalne ryzyko ukarania przez UKE.

Jak realizować obowiązek informacyjny w ofertowaniu?

Aby przetwarzać dane osobowe zgodnie z RODO, nie wystarczy dysponować podstawą prawną przetwarzania z art. 6 ust. 1 RODO (ewentualnie art. 9 ust. 2 RODO) – każda osoba, której dane przetwarzamy, musi zostać o tym poinformowana. Standardowo katalog informacji z art. 13 RODO powinien zostać przedstawiony osobom, których dane osobowe pozyskaliśmy bezpośrednio od nich, czyli (bazując na podanych wyżej przykładach) byłym lub obecnym klientom, a także osobom, które zwróciły się o ofertę (np. za pośrednictwem przeznaczonego do tego celu formularza na stronie WWW).

Wskazówka: Klauzulę informacyjną – o ile nie została wcześniej zawarta w treści umowy z klientem – można przesłać np. w treści wiadomości e-mail czy w samej ofercie. Wykorzystując formularz, musimy natomiast pamiętać o przekazaniu niezbędnych informacji przy zbieraniu danych, w związku z tym obowiązek informacyjny najlepiej spełnić pod samym formularzem.

Z kolei art. 14 RODO znajdzie zastosowanie przy osobach, których dane zebraliśmy za pośrednictwem innego podmiotu (np. firmy sprzedającej bazy danych) lub ze źródeł powszechnie dostępnych. Wówczas przy pierwszym kontakcie, nie później jednak niż w ciągu 30 dni od pozyskania danych, musimy takiej osobie przekazać niezbędne informacje o przetwarzaniu jej danych, w tym informację o źródle pozyskanych danych i o tym, jakie dokładnie kategorie danych (np. imię, nazwisko, adres e-mail) będziemy przetwarzać.

Jak długo przechowywać dane?

Okres przechowywania danych zebranych w procesie ofertowania zależy od tego, czy dojdzie do zawarcia umowy. Oczywiście jeśli umowę zawrzemy, dane automatycznie „wpadną" do procesu sprzedaży/obsługi klienta (o tym poniżej). Natomiast w sytuacji gdy nie dojdzie do zawarcia umowy, okres przechowywania danych będzie zależał od tego, czy klient rokuje na przyszłość, czy dalsze kierowanie ofert/marketingu w jego stronę jest bezcelowe. Mając to na względzie, dane osobowe powinny zostać

odpowiednio: albo usunięte niezwłocznie po ustaniu celu przetwarzania w postaci zakończenia procesu negocjacji, albo przetwarzane w dalszym ciągu na podstawie prawnie uzasadnionego interesu administratora (jakim jest prowadzenie działań marketingowych) do czasu wniesienia przez osobę fizyczną sprzeciwu wobec przetwarzania.

DANE NIEZBĘDNE DO REALIZACJI UMOWY I PODSTAWA PRAWNA ICH PRZETWARZANIA

Aby wskazać prawidłową podstawę prawną przetwarzania danych osobowych niezbędnych do realizacji umowy, należy w pierwszej kolejności ustalić, jaki charakter ma podmiot, z którym zawieramy umowę. Stroną umowy może być albo osoba fizyczna, albo osoba prawna (lub ułomna osoba prawna, np. stowarzyszenie zwykłe czy wspólnota).

Osoba fizyczna jako strona umowy

Jeżeli stroną umowy jest osoba fizyczna, sytuacja jest jasna – stosownie do art. 6 ust. 1 lit. b RODO przetwarzanie jest zgodne z prawem, gdy jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą. Oznacza to, że wszelkie dane, które stanowią ścisłe minimum potrzebne do realizacji umowy, której stroną jest osoba fizyczna, przetwarzamy właśnie na tej przesłance i nie musimy zbierać żadnych odrębnych zgód na kontakt drogą telefoniczną czy na przetwarzanie danych w celu realizacji umowy. Mowa tu zarówno o danych, których potrzebujemy, aby umowę w ogóle zawrzeć (imię, nazwisko, adres zamieszkania, a w przypadku JDG: firma, NIP i REGON itp.), jak i o tych, które są niezbędne do jej realizacji (numer telefonu, adres e-mail, adres dostawy, numer rachunku bankowego), a także tych,

które mogą okazać się przydatne już po realizacji umowy (w uzasadnionych przypadkach np. numer PESEL w razie konieczności dochodzenia roszczeń na drodze sądowej).

Uwaga: Zgodnie z RODO nie ma znaczenia, czy umowę zawrzemy z Julianem Bezpiecznym, czy z Barbarą Osobową, prowadzącą działalność gospodarczą pod firmą „Usługi prawne Barbara Osobowa". W obu przypadkach mamy do czynienia z osobami fizycznymi, w związku z czym przepisy RODO znajdą tu zastosowanie.

Osoba prawna jako strona umowy

Powodem, dla którego w przypadku zawarcia umowy ze spółką (lub inną osobą prawną czy ułomną osobą prawną) zastosowania nie znajdzie art. 6 ust. 1 lit. b RODO, jest oczywiście to, że przywołana podstawa prawna przetwarzania dotyczy umów, których stroną jest osoba, której dane dotyczą, czyli osoba fizyczna. Zgodnie z motywem 14 RODO „rozporządzenie nie dotyczy przetwarzania danych osobowych dotyczących **osób prawnych**, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej".

Jednak umowa pomiędzy nami a spółką nie zrealizuje się sama – do tego potrzeba oczywiście personelu, czyli (współ)pracowników, przedstawicieli, osób wskazanych po stronie klienta do realizacji umowy. Przykładowo jeśli świadczymy usługi transportowe, niezbędne może być przetwarzanie przez nas danych kontaktowych pracowników klienta odpowiedzialnych za odbiór towaru w miejscu przeznaczenia. Jeśli zaś oferujemy usługi związane z obsługą księgową, najczęściej po stronie klienta nabywającego te usługi oddelegowane są osoby, które mają z nami stały kontakt i które faktycznie zlecają nam zadania do wykonania. Jako podstawę prawną przetwarzania danych osobowych w tym miejscu należy wskazać art. 6 ust. 1 lit. f RODO. Co bowiem pasuje do definicji prawnie uzasadnionego interesu administratora bardziej niż konieczność wykonania umowy sprzedaży towarów/usług, które stanowią główny przedmiot działalności organizacji?

KLAUZULA INFORMACYJNA W KONTAKTACH Z KLIENTAMI

Klauzulę informacyjną warto skonstruować w taki sposób, aby była uniwersalna i mogła być skierowana do klientów będących zarówno osobami fizycznymi, jak i osobami prawnymi, czyli żeby przy jej pomocy spełnić obowiązek informacyjny z art. 13 i 14 RODO (bo przecież nie wszystkie dane w procesie sprzedaży pozyskujemy bezpośrednio od osoby, której dane dotyczą, np. jeśli w treści umowy klient wskaże tzw. osoby do kontaktu). Pamiętajmy, że klauzule z obu wskazanych artykułów trochę się od siebie różnią, chociażby w zakresie dodatkowych informacji, jakie musimy przekazać na gruncie art. 14 RODO, w postaci źródła pozyskania danych i kategorii danych osobowych, którymi jako administrator dysponujemy (jak „fizycznie" spełnić obowiązek informacyjny z art. 14 RODO, patrz w rozdziale „Kontrahenci i dostawcy").

Przy konstruowaniu klauzuli w procesie sprzedaży zazwyczaj najwięcej problemów przysparza określenie celów i podstaw prawnych przetwarzania. Tworząc klauzulę, nie możemy być krótkowzroczni i zatrzymać się na celach związanych z samą realizacją umowy. Powinniśmy myśleć krok do przodu – poinformować osobę fizyczną również o tym, co później będzie działo się z jej danymi osobowymi – z uwagi np. na obowiązki prawne dotyczące przechowywania dokumentów księgowych, na ewentualne dochodzenie roszczeń lub obronę przed roszczeniami czy przeprowadzanie badań satysfakcji klienta. W klauzuli mogą zostać wskazane następujące cele (wraz z odpowiednimi podstawami przetwarzania danych osobowych w tym zakresie):

Przykład: *Twoje dane osobowe są przetwarzane w celu:*

- *zawarcia i realizacji umowy łączącej Ciebie jako klienta z Administratorem – na podstawie art. 6 ust. 1 lit. b RODO,*
- *realizacji umowy z Administratorem, której nie jesteś stroną, jednakże zostałeś wyznaczony przez klienta Administratora do jej wykonywania bądź jesteś przedstawicielem klienta Administratora wyznaczonym do zawarcia w jego imieniu wskazanej wyżej umowy – na podstawie art. 6 ust. 1 lit. f RODO, przy czym prawnie uzasadnionym interesem Administratora jest konieczność faktycznej realizacji umowy,*
- *spełnienia zobowiązań prawnych, w szczególności realizacji obowiązku prowadzenia sprawozdawczości finansowej i przechowywania dokumentów księgowych – na podstawie art. 6 ust. 1 lit. c RODO,*
- *realizacji obowiązków z zakresu rękojmi i reklamacji – na podstawie art. 6 ust. 1 lit. c RODO,*
- *realizacji prawnie uzasadnionego interesu Administratora, jakim jest prowadzenie działań marketingowych polegających na wysyłce informacji handlowych i działaniach promocyjnych, przeprowadzenie badania satysfakcji klienta, dochodzenie roszczeń lub obrona przed roszczeniami wynikającymi z umowy – na podstawie art. 6 ust. 1 lit. f RODO.*

OKRESY PRZECHOWYWANIA DANYCH W PROCESIE SPRZEDAŻY I OBSŁUGI KLIENTA

Terminy usunięcia danych są oczywiście zależne od celów, w jakich dane przetwarzamy. Najczęściej jednak w procesie sprzedaży i obsługi klienta dane osobowe będziemy przechowywać:

- **przez czas realizacji umowy, a po jego upływie – do czasu upływu terminu przedawnienia roszczeń**

wynikających z umowy lub wygaśnięcia obowiązków przechowywania danych wynikających z przepisów prawa, w szczególności przechowywania dokumentów księgowych i wypełniania zobowiązań podatkowych (tj. 5 lat od końca roku kalendarzowego, w którym zaktualizował się obowiązek podatkowy),

- **przez rok po terminie upływu rękojmi lub rozliczenia reklamacji,**
- **jeśli do przetwarzania dochodzi na podstawie prawnie uzasadnionego interesu administratora – najpóźniej do czasu wniesienia uzasadnionego sprzeciwu wobec takiego przetwarzania.**

KWESTIE BUDZĄCE NAJWIĘCEJ WĄTPLIWOŚCI

Zapłata danymi osobowymi

Przepis art. 7 RODO statuuje wprost, że jeśli od wyrażenia zgody na przetwarzanie danych jest uzależnione wykonanie umowy, w tym świadczenie usługi, a przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy, zgody takiej nie można uznać za dobrowolną.

Istnieją różne modele „wymuszania" płatności danymi osobowymi za towar/usługę, przy czym najczęstszy jest ten, w którym dana usługa może być świadczona w zamian za zgodę na przetwarzanie danych osobowych albo gdy umowa będzie zrealizowana wyłącznie w zamian za wykorzystanie danych w innych celach – oba sposoby postępowania co do zasady są sprzeczne z RODO. Zatem np. obligatoryjna zgoda na kierowanie działań marketingowych jako warunek złożenia zamówienia przez sklep internetowy z pewnością powinna zostać potraktowana jako naruszająca przepisy RODO.

Adekwatność – PESEL a numer dokumentu

Administratorzy, kierując się zasadą minimalizacji, każdorazowo powinni określić zakres danych osobowych, który stanowiłby niezbędne minimum umożliwiające wykonanie danej umowy. O ile w ramach relacji z podmiotami gospodarczymi (w tym osobami fizycznymi prowadzącymi JDG) zakres przetwarzanych danych osobowych jest określany wspólnie przez równe sobie strony zawieranej umowy, o tyle przy kontakcie z konsumentami należy przyłożyć szczególną wagę do tego, aby nie zbierać danych nadmiarowych.

Jeżeli administrator potrzebuje danych klienta do celów weryfikacji jego tożsamości, bezpieczniejszym rozwiązaniem jest zbieranie numeru dokumentu tożsamości. PESEL ujawnia więcej danych o osobie fizycznej (tj. również jej datę urodzenia i płeć), dlatego jest uważany za informację, która umożliwia kradzież tożsamości. Nie oznacza to jednak, że numeru PESEL bezwzględnie zbierać nie można (tę kwestię poruszono wyżej przy zagadnieniu „Osoba fizyczna jako strona umowy").

Profilowanie – e-commerce

Dotychczas większość sklepów stosowała tzw. profilowanie w celu lepszego dopasowania oferty do zainteresowań klientów. Polega ono na gromadzeniu wielu różnych danych na temat użytkownika (wiek, płeć, historia

zakupów itp.). Wcześniej proces ten mógł odbywać się bez wiedzy klienta, jednak obecnie – zgodnie z RODO – e-sklep powinien poinformować osobę, której dane dotyczą, o stosowaniu wobec niej profilowania, jeżeli jest ono w pełni zautomatyzowane oraz w wyniku zautomatyzowanego przetwarzania zapadają decyzje wywołujące skutki prawne dla osoby lub w inny sposób znacząco wpływają na osobę. Wówczas należy również zapewnić odpowiednią podstawę prawną takiego przetwarzania, zgodnie z art. 22 ust. 2 RODO.

Warto wskazać, że nie każde profilowanie kończy się zautomatyzowanym podejmowaniem decyzji. Samo sugerowanie spersonalizowanych treści czy dopasowanie odpowiedniej oferty nie jest jeszcze decyzją. Decyzją będzie już jednak uzależnianie ceny czy jakości oferowanego produktu od czynników dotyczących danej osoby (np. oferowanie kobietom różnej jakości kosmetyków w zależności od ich koloru skóry).

Kontrahenci i dostawcy

PODSTAWY PRAWNE PRZETWARZANIA DANYCH

W zależności od rodzaju podmiotu, z jakim podejmujemy współpracę, przetwarzamy dane osób fizycznych w różnych celach, a tym samym opierając się na różnych podstawach prawnych. Poniżej przedstawiany analizę podstaw prawnych przetwarzania danych w zależności od tego, kim jest kontrahent, przy czym – analogicznie do tego, co przedstawiliśmy w procesie sprzedaży i obsługi klienta – zasadniczą rolę odegra tu podział na kontrahentów będących osobami fizycznymi i osobami prawnymi.

Osoby prawne

Jeżeli kontrahentami są osoby prawne (w tym spółki prawa handlowego), RODO nie znajdzie do nich zastosowania – zgodnie z przywołanym już wcześniej motywem 43 RODO. Wobec tego administrator nie musi zastanawiać się, na jakiej podstawie może przetwarzać informacje dotyczące konkretnej spółki. Nie znaczy to jednak, że jeśli współpracuje z osobami prawnymi, to może zapomnieć o wymogach RODO. Oczywiste bowiem jest to, że spółka prawa handlowego – niezależnie od tego, czy działa w formie spółki z ograniczoną odpowiedzialnością, spółki akcyjnej, czy innej – działa przez swoich przedstawicieli oraz pracowników, czyli przez osoby fizyczne. Jaka więc jest podstawa prawna przetwarzania przez administratora danych tych osób?

Przedstawiciele kontrahentów będących osobami prawnymi, osoby do kontaktu wskazane w umowie oraz pracownicy tych kontrahentów wyznaczeni do realizacji łączącej strony umowy nie są stronami zawartej umowy, w związku z czym administrator nie może przetwarzać tych danych na podstawie art. 6 ust. 1 lit. b RODO. Niemniej przetwarzanie danych osobowych wymienionych osób jest dla przedsiębiorcy niezbędne do zawarcia, realizacji i wykonywania umowy, co stanowi prawnie uzasadniony interes administratora – art. 6 ust. 1 lit. f RODO. Nie ma więc wątpliwości, że administrator, zawierając umowę z kontrahentem, który działa w formie spółki prawa handlowego, bez obaw może przetwarzać dane osobowe jego pracowników i innych osób związanych z zawartą umową.

Istotną kwestią pozostaje adekwatność przetwarzanych danych osobowych, niezbędnych do realizacji umowy między stronami. Należy uwzględnić, że prawnie uzasadniony interes administratora stanowi podstawę przetwarzania jedynie dla zakresu danych, który jest niezbędny podczas zawierania i realizacji umowy. Z reguły zakres ten obejmuje: imię, nazwisko, numer telefonu służbowego, służbowy adres e-mail, stanowisko. Jeżeli więc kontrahent przekazuje nam zdecydowanie szerszy zakres danych niż ten, który jest niezbędny do realizacji umowy, musimy przeanalizować, czy potrzebujemy tych danych i w jakim celu, aby przetwarzać udostępniane dane osobowe zgodnie z przepisami prawa.

Jednoosobowe działalności gospodarcze

W przypadku osób fizycznych prowadzących JDG należy pamiętać, że ustawodawca nie wyłączył ich spod stosowania przepisów RODO. W związku z tym JDG należy traktować jak każdą osobę fizyczną. Jeżeli więc kontrahentem jest osoba fizyczna prowadząca JDG, dane oso-

bowe, które od niej pozyskano w związku z zawarciem i realizacją przedmiotowej umowy, np. imię, nazwisko, nazwa działalności, NIP, adres e-mail, numer telefonu itp., będą przetwarzane na podstawie art. 6 ust. 1 lit. b RODO. Oczywiście niejednokrotnie zdarza się tak, że w ramach JDG zatrudnia się również pracowników, których dane osobowe są przetwarzane w związku z wykonywaniem umowy łączącej strony. W takiej sytuacji, podobnie jak w przypadku osób prawnych, podstawę przetwarzania danych osobowych przywołanych osób stanowi prawnie uzasadniony interes administratora w postaci realizacji umowy.

OBOWIĄZEK INFORMACYJNY – JAK SPRAWNIE GO REALIZOWAĆ?

Sam fakt, że dane kontrahentów, ich przedstawicieli czy pracowników są przetwarzane z reguły w relacjach biznesowych w związku z łączącymi strony umowami, nie zwalnia administratora z obowiązku przekazania osobom fizycznym, których dane dotyczą, informacji wskazanych w RODO. Obowiązek ten na pierwszy rzut oka wydaje się problematyczny, bo pojawia się pytanie, jak dotrzeć do wszystkich pracowników kontrahenta, którzy mogą być wskazani do realizacji umowy zawartej z tym kontrahentem.

Krzyżowy obowiązek informacyjny

Praktyka poradziła sobie z tym problemem dzięki stosowaniu tzw. krzyżowego obowiązku informacyjnego – administratorzy zobowiązują się nawzajem do przekazania swoim pracownikom informacji wymaganych przez RODO. Należy jednak pamiętać, żeby dla zabezpieczenia zawrzeć odpowiednie postanowienie w tym zakresie w umowie z kontrahentem.

Jak łatwo zauważyć, dane osobowe w omawianej sytuacji nie będą udostępniane administratorowi bezpośrednio przez osoby fizyczne. Z reguły bowiem to kontrahent udostępni mu dane kontaktowe swojego pracownika. Zatem informacje, które administrator jest zobligowany przekazać osobie fizycznej, są wskazane w art. 14 RODO – są to informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą. Zapis do umowy, w której strony występują w rolach zleceniodawcy i zleceniobiorcy, może brzmieć następująco:

Przykład: *Zleceniobiorca zobowiązany jest do wykonania w imieniu Zleceniodawcy obowiązku informacyjnego, o którym mowa w art. 14 ust. 1 i 2 RODO, wobec reprezentantów/pracowników/współpracowników Zleceniobiorcy biorących udział w realizacji niniejszej Umowy, przy wsparciu Zleceniodawcy w niezbędnym zakresie, polegającym w szczególności na przedstawieniu Zleceniobiorcy informacji niezbędnych do wykonania obowiązku informacyjnego wynikającego z przepisów przywołanych na wstępie niniejszego zdania.*

Powyższy przykład można odpowiednio modyfikować w zależności od tego, w jakiej roli występuje administrator. Zgodnie z zaproponowanym zapisem administrator powinien również załączyć do umowy treść klauzuli informacyjnej z art. 14 RODO, tak aby ze swojej strony jak najbardziej usprawnić proces przekazania w jego imieniu informacji osobom fizycznym.

Stopki w wiadomościach e-mail

Niezależnie od obowiązku krzyżowego administrator może dodatkowo zabezpieczyć się przed zarzutem niedopełnienia obowiązku informacyjnego względem reprezentantów, pracowników lub współpracowników swojego kontrahenta. Sposobem na to jest zamieszczenie w stopce e-mail swoich pracowników odesłania do treści tego obowiązku, znajdującej się np. na firmowej stronie internetowej. Praktyka ta jest coraz częściej stosowana wśród przedsiębiorców, nie wymaga bowiem dużego nakładu pracy po stronie administratora, a skutecznie pomaga w spełnieniu wymogu poinformowania osób fizycznych o zasadach przetwarzania ich danych osobowych.

Ze względu na ograniczoną ilość przestrzeni w stopce mailowej za zasadne trzeba uznać odsyłanie do klauzuli informacyjnej, nie zaś umieszczanie całej jej treści w stopce. W takiej sytuacji – podobnie jak przy odesłaniu do treści obowiązku informacyjnego pod formularzami kontaktowymi czy też pod formularzem zapisu na newsletter, które znajdują się na stronie internetowej administratora – w pierwszej warstwie informacji przekazywanych w stopce należy zamieścić informację o tożsamości administratora, celach przetwarzania danych oraz prawach przysługujących osobie fizycznej.

Powyższe sposoby spełnienia obowiązku informacyjnego względem pracowników i przedstawicieli kontrahentów znajdą oczywiście zastosowanie także w przypadku pracowników i przedstawicieli klientów administratora, jak również – w zakresie informacji zamieszczonych w stopce mailowej – względem każdej osoby fizycznej, która będzie kontaktowała się z administratorem drogą mailową.

Obowiązek informacyjny w treści umowy

Powyżej opisano obowiązek poinformowania osób fizycznych wynikający z art. 14 RODO. Jednak w niniejszym procesie zdarza się również, że administrator pozyskuje dane osobowe bezpośrednio od osoby fizycznej. Najczęstszym przypadkiem pozyskiwania danych osobowych bezpośrednio od osoby fizycznej jest relacja

z kontrahentem prowadzącym JDG. Wówczas rekomendowanym rozwiązaniem jest zamieszczenie stosownych informacji – tym razem już z art. 13 RODO – w treści samej umowy z takim kontrahentem.

OKRES PRZECHOWYWANIA DANYCH OSOBOWYCH

Dane osobowe przedstawicieli oraz pracowników i współpracowników kontrahentów czy też klientów, a także dane osób fizycznych prowadzących JDG będą przechowywane przede wszystkim przez czas trwania umów łączących strony, natomiast po zakończeniu trwania umów – do czasu przedawnienia ewentualnych roszczeń, zgodnie z okresami przewidzianymi przepisami prawa. W tym zakresie należy w szczególności mieć na uwadze art. 118 Kodeksu cywilnego, zgodnie z którym termin przedawnienia wynosi sześć lat, a dla roszczeń o świadczenia okresowe oraz roszczeń związanych z prowadzeniem działalności gospodarczej – trzy lata.

POWIERZENIE PRZETWARZANIA DANYCH ZEWNĘTRZNYM PODMIOTOM – JAK DOBRAĆ ODPOWIEDNIEGO KONTRAHENTA?

WIĘCEJ

Zawarcie umowy powierzenia z podmiotem przetwarzającym

Umowa o współpracy zawarta z kontrahentem niejednokrotnie implikuje, ze względu na charakter świadczonych usług, konieczność powierzenia kontrahentowi danych osobowych do przetwarzania w imieniu administratora, którym jest organizacja (albo przedsiębiorca prowadzący JDG). Najczęściej dochodzi do powierzenia danych klientów, pracowników i współpracowników administratora, w związku z usługą świadczoną przez kontrahenta, w postaci np. hostingu lub zewnętrznej księgowości. Najistotniejszą kwestią pozostaje uregulowanie stosunku powierzenia zgodnie z RODO, co przeważnie odbywa się przez zawarcie umowy powierzenia przetwarzania danych. Przedmiotowa umowa powinna zawierać wszystkie elementy wskazane w art. 28 ust. 3 RODO (o niezbędnych postanowieniach umowy powierzenia patrz rozdział dotyczący procesu zatrudnienia).

Niezależnie od zawartej umowy powierzenia bardzo istotne jest to, czy podmiot przetwarzający, któremu powierzamy dane osobowe, faktycznie spełnia wymogi w zakresie posiadania odpowiednich zabezpieczeń technicznych i organizacyjnych.

Weryfikacja podmiotu przetwarzającego – audyt czy ankieta?

Możliwymi sposobami weryfikacji są audyt podmiotu przetwarzającego oraz ankieta. Przeprowadzenie audytu umożliwia dogłębne sprawdzenie konkretnego kontrahenta i skuteczne wychwycenie niezgodności, które mogą pojawić się w jego systemie ochrony danych osobowych. Jednak audyt wiąże się z dodatkowymi kosztami oraz nakłada wiele obowiązków pod względem organizacyjnym. Niemniej administrator w miarę możliwości powinien zadbać o przeprowadzenie audytu sprawdzającego u podmiotu przetwarzającego przed powierzeniem mu danych osobowych. Audyt pozwoli administratorowi utrzymać realną kontrolę nad powierzonymi danymi osobowymi i przysporzy wiedzy o rzeczywistym poziomie ochrony danych osobowych u procesora.

Nie zawsze istnieje jednak możliwość szybkiego i sprawnego przeprowadzenia audytu u podmiotu przetwarzającego. W takiej sytuacji dobrym rozwiązaniem jest przekazanie procesorowi do wypełnienia ankiety sprawdzającej. Powinna ona zawierać pytania dotyczące np. przyjętych i stosowanych przez procesora zabezpieczeń technicznych i organizacyjnych, przyjętej dokumentacji z zakresu ochrony danych osobowych, częstotliwości przeprowadzanych szkoleń dla pracowników z zakresu ochrony danych osobowych itp. Administrator powinien zadbać o to, żeby procesor rzetelne wypełnił ankietę, i zweryfikować odpowiedzi, zanim powierzy takiemu podmiotowi dane osobowe do przetwarzania.

Administrator odpowiada za zgodne z prawem przetwarzanie danych osobowych niezależnie od tego, czy dokonywane jest ono przy pomocy podmiotu zewnętrznego, czy też bezpośrednio w ramach jego struktur. Wynika to wprost z art. 28 RODO, zgodnie z którym administrator korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych. Niezwykle istotne jest więc rzetelne zweryfikowanie podmiotu przetwarzającego celem zminimalizowania ryzyka naruszenia ochrony danych osobowych. Zlecając na zewnątrz czynności przetwarzania danych osobowych, administrator powinien być pewny, że ochrona powierzonych danych osobowych zostanie zapewniona przynajmniej na takim samym poziomie, jaki zapewnia sam administrator.

III CZĘŚĆ. ZMIANY W OBSZARZE ZABEZPIECZEŃ DANYCH

Okazuje się, że przygotowanie do ewentualnej kontroli UODO to nie tylko szeroko omawiane kwestie formalno-prawne. Nowe obowiązki, mało precyzyjne przepisy i przede wszystkim milionowe kary spowodowały, że na rynku pojawiło się mnóstwo usług i narzędzi teleinformatycznych zapewniających „pełne bezpieczeństwo przetwarzania danych osobowych" i „zgodność z RODO". Czy takie rozwiązania w ogóle istnieją? Rzeczywiście większość oferowanych produktów umacnia system ochrony danych osobowych, ale na rynku nie ma pojedynczego rozwiązania, które zapewni pełne bezpieczeństwo ich przetwarzania. Jednocześnie nie oznacza to, że w takie produkty nie warto inwestować, bo **bezpieczeństwo to przecież zbiór zabezpieczeń**, natomiast niezależnie od ich wyboru ryzyka incydentu nie można wykluczyć, a jedynie możne je minimalizować.

Przepisy o ochronie danych osobowych przedstawiają zupełnie nowe podejście do stosowanych zabezpieczeń. Zrezygnowano bowiem ze wskazywania przedsiębiorcom konkretnych rozwiązań. Warto wspomnieć, że obowiązujące w poprzednim stanie prawnym podejście, polegające na zdefiniowaniu wymagań dotyczących bezpieczeństwa, wówczas nie sprawdziło się w pełnym, zapewne planowanym zakresie. Otóż stało się tak z powodu bardzo szybkiego postępu technologicznego oraz ciągłego ewoluowania lub pojawiania się nowych zagrożeń, które spowodowały, że zabezpieczenia wymienione wtedy w przepisach często okazywały się niewystarczające. Mówi się, że RODO to akt prawny neutralny technologicznie. Ale czy rzeczywiście w związku z tym nie musimy martwić się o ten obszar w razie kontroli? Czy nie wymaga on uwagi podczas wdrożenia systemu ochrony danych? Zarówno na te pytania, jak i na wiele innych odpowiemy w niniejszej części poradnika.

Wymóg analizy ryzyka

Dane osobowe stanowią obecnie zasób i czynnik produkcji – dzięki nowym rozwiązaniom i wciąż rozwijającej się technologii są one przetwarzane na niespotykaną dotąd skalę. Każda organizacja przetwarzająca dane osobowe jest narażona na wpływ czynników wewnętrznych oraz zewnętrznych, które mogą spowodować naruszenie bezpieczeństwa, prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieautoryzowanego dostępu do przetwarzanych danych osobowych. Stan ten nazywany jest ryzykiem, czyli wskaźnikiem prawdopodobieństwa wystąpienia takiego zdarzenia oraz wielkości strat, jakie może ono spowodować. To właśnie analiza ryzyka jest jednym z głównych założeń RODO.

OBSZARY ANALIZY RYZYKA NA GRUNCIE RODO

Analizę ryzyka na gruncie RODO można podzielić na dwa duże obszary analityczne. Pierwszym z nich jest analiza ryzyka dla praw i wolności osób fizycznych, tzw. DPIA, czy też ocena skutków przetwarzania (to pojęcie znajdziemy w RODO). Wynikiem takiej operacji powinny być procesy przetwarzania danych osobowych obarczonych niskim oraz wysokim ryzykiem dla ochrony praw i wolności osób fizycznych. Drugi obszar analityczny to szacowanie ryzyka dla zasobów, czyli wszelkich środków materialnych i niematerialnych służących do przetwarzania danych osobowych, takich jak komputer, telefon, system, ale również człowiek czy pomieszczenie. Wynikiem drugiego etapu jest zidentyfikowanie zasobów, z których wykorzystaniem wiąże się największe prawdopodobieństwo zmaterializowania się zagrożeń w zidentyfikowanych wcześniej procesach.

Innymi słowy: każda organizacja przetwarzająca dane osobowe w ramach przeprowadzonej analizy ryzyka dla zasobów powinna zidentyfikować obszary, które nie są zabezpieczone, w których zastosowane zabezpieczenia nie są wystarczająco efektywne, oraz aktywa, z których wykorzystaniem wiąże się największe prawdopodobieństwo wystąpienia danego zagrożenia, a następnie powinna działać właśnie na te zasoby. Działanie to powinno polegać na zminimalizowaniu zidentyfikowanego ryzyka do poziomu akceptowalnego przez organizację, a w razie braku takiej możliwości administrator powinien skonsultować się w tej sprawie z organem nadzorczym.

SPOSOBY REAKCJI NA ZIDENTYFIKOWANE RYZYKA

Tak jak w przypadku różnych metodyk wykonywania procesu szacowania ryzyka wiele jest sposobów reakcji na zidentyfikowane ryzyka. Najczęściej wykorzystywanym jest redukcja, która polega na wdrożeniu dodatkowych zabezpieczeń technicznych i/lub organizacyjnych. Innymi możliwymi sposobami są transfer ryzyka, czyli współdzielenie zidentyfikowanego ryzyka dla zasobów z podmiotem zewnętrznym, lub unikanie ryzyka, które polega na zrezygnowaniu z wykorzystania danego zasobu obarczonego wysokim ryzykiem.

WIĘCEJ
WIĘCEJ

Niestety zarówno w przepisach dotyczących ochrony danych osobowych, jak i w wytycznych Grupy Roboczej Art. 29 lub poradnikach UODO nie odnajdziemy informacji na temat tego, jaką metodykę zastosować celem prawidłowego wykonania omawianego procesu. Według wskazanych dokumentów każda organizacja taką metodykę powinna dobrać do własnych, indywidualnych potrzeb, uwzględniając przy tym branże, rozmiar lub sposób działania firmy. Dobrym pomysłem jest oparcie się w tym względzie na dobrych praktykach zawartych w normie PN-ISO/IEC 31000 – „Zasady i wytyczne zarządzania ryzykiem" oraz normie PN-ISO/IEC 27005 – „Zarządzanie ryzykiem w bezpieczeństwie informacji". Wskazuje na nie również Grupa Robocza Art. 29, przy czym należy wspomnieć, że są to standardy odpłatne. Można skorzystać również z darmowych rozwiązań – publikacji Narodowego Instytutu Standaryzacji i Technologii (NIST) lub Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA), lecz niestety nie są one dostępne w języku polskim.

DOKUMENTOWANIE PROCESU SZACOWANIA RYZYKA

Niezależnie od wyboru metodyki oprócz wykonania procesu szacowania ryzyka niezmiernie ważne jest odpowiednie jego udokumentowanie. RODO wprowadza pojęcie rozliczalności. Zgodnie z nim to administrator jest odpowiedzialny za przestrzeganie przepisów i to on musi być w stanie wykazać ich przestrzeganie. Dlatego też każda czynność w ramach prac związanych z zarządzaniem ryzykiem powinna być udokumentowana. Mowa tutaj nie tylko o wykonanych obliczeniach i planie postępowania z ryzykiem, który powinien być wynikiem przeprowadzonych prac, lecz także o dokumentacji w postaci procedury opisującej przyjęte kryteria oraz sposób wykonania całego procesu.

Uwaga: Bardzo ważne jest to, aby dokumenty, o których mowa powyżej, zostały formalnie przyjęte przez administratora. Zrealizowanie w pełni tego obowiązku zapewne będzie jednym z pierwszych elementów weryfikowanych przez UODO podczas kontroli.

CZĘSTOTLIWOŚĆ WYKONYWANIA ANALIZY RYZYKA

Warto wspomnieć o częstotliwości wykonywania analizy ryzyka. Okazuje się bowiem, że nie jest to czynność jednorazowa, a proces ciągły, który organizacja powinna systematycznie powtarzać, a przez to dążyć do ciągłego doskonalenia stosowanych przez nią zabezpieczeń. Dzięki takiemu podejściu mamy do czynienia z sytuacją, w której przepisy RODO w obszarze bezpieczeństwa danych nie przedawnią się wraz ze zmieniającym się światem – tak jak to było w poprzednim stanie prawnym.

Zabezpieczenia na gruncie RODO

RODO nie narzuca administratorom konkretnych rozwiązań umacniających system ochrony danych i minimalizujących ryzyko możliwego naruszenia ich przetwarzania. Na uwagę w zakresie stosowanych zabezpieczeń zasługuje jednak art. 32 ust. 1 lit. b RODO. W związku z tym przepisem administrator danych osobowych powinien zagwarantować organizacji zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania. Dobór zabezpieczeń na podstawie wyników analizy ryzyka może być dla wielu podmiotów bardzo skomplikowany, dlatego warto stosować się do dobrych praktyk w zakresie bezpieczeństwa. Nie sposób nie wspomnieć o zapisach zawartych w normach ISO, w tym PN-ISO/IEC 27001 – „Systemy zarządzania bezpieczeństwem informacji" lub PN-ISO/IEC 27002 – „Praktyczne zasady zabezpieczania informacji".

WIĘCEJ

KONTROLA DOSTĘPU DO OBSZARU PRZETWARZANIA DANYCH OSOBOWYCH

Badając obszar zabezpieczeń fizycznych, powinniśmy zwrócić uwagę na kontrolę dostępu do obszaru przetwarzania danych osobowych. W wielu organizacjach do tego celu wykorzystywany jest odpowiedni system, który odblokowuje zainstalowane elektrozamki po zbliżeniu karty RFID do czytnika lub po wpisaniu kodu PIN. Aby zachować pełną skuteczność systemu, należy pamiętać o tym, że każdy pracownik upoważniony do dostępu do organizacji powinien dysponować własną, indywidualną kartą, która w sposób jednoznaczny jest do niego przypisana (tak samo powinno być w przypadku kodu PIN). Dodatkowo zastosowany system powinien zbierać informacje na temat dokładnych dni oraz godzin wejścia pracownika do organizacji. Dzięki temu organizacja zapewni pełną rozliczalność wejść do obszaru przetwarzania danych osobowych, a ponadto być może będzie w stanie zidentyfikować przyczynę wystąpienia ewentualnego incydentu lub naruszenia ochrony danych osobowych.

Wskazówka: W tym obszarze można posunąć się o krok dalej. Mianowicie w zależności od zastosowanego systemu kontroli dostępu odpowiednie funkcjonalności mogą pozwalać na zdefiniowanie godzin lub dni, w których dostęp do organizacji jest możliwy. W celu podniesienia poziomu bezpieczeństwa można zablokować fizyczny dostęp do organizacji po godzinach pracy lub w dni od niej wolne. Przy stosowaniu tego typu zabezpieczeń trzeba jednak pamiętać, że wybrani pracownicy, np. działu IT, powinni mieć fizyczny dostęp do organizacji przez całą dobę i każdego dnia, choćby ze względu na nieoczekiwane awarie.

W przypadku gdy fizyczny dostęp do organizacji po godzinach pracy jest zabezpieczony tylko i wyłącznie z wykorzystaniem systemu kontroli, warto mieć na uwadze, że elektrozamki zwolnią się nie tylko po zbliżeniu karty magnetycznej lub wpisaniu kodu PIN, lecz także z powodu zaniku zasilania. W związku z tym można stosować dwuskładnikową kontrolę dostępu, łączącą stosowany system ze zwykłym kluczem mechanicznym, lub dodatkowo zapewnić alternatywne źródło energii dla zastosowanego systemu. Wykorzystywanie do zabezpieczenia organizacji wyłącznie omawianego systemu – bez dodatkowego klucza – niesie za sobą dodatkowe ryzyko. Mowa o niedomknięciu drzwi przez pracownika, przez co system zwyczajnie się nie uruchomi. Takie sytuacje często są wykorzystywane przez potencjalnych atakujących. W celu minimalizacji tego ryzyka warto stosować mocne samodomykacze w połączeniu z systemem informującym sygnałem dźwiękowym o niezamknięciu drzwi przez czas dłuższy niż np. 30 sekund. Informowani o takim zdarzeniu mogą być np. pracownicy ochrony obiektu.

Równie ważnym aspektem jest to, kto zarządza systemem, a tym samym kto ma wpływ na jego ostateczną konfigurację, oraz to, na jakiej podstawie takie zarządzanie jest realizowane. Każdorazowa zmiana w zakresie uprawnień powinna wymagać formalnego, udokumentowanego wniosku, który w zależności od zastosowanego podejścia w organizacji może być wysyłany do administratora systemu np. przez kierownika danej jednostki organizacyjnej, przedstawiciela działu kadr lub samego administratora danych osobowych. Jednocześnie niedopuszczalne są sytuacje, w których uprawnienia fizycznego dostępu do organizacji są odbierane po zakończeniu współpracy z danym pracownikiem czy współpracownikiem. Podobnie jak w przypadku każdego innego systemu takie uprawnienia powinny być wygaszane najpóźniej ostatniego dnia pracy takiej osoby.

Wskazówka: Analizując obszar bezpieczeństwa fizycznego, dodatkowo zwróćmy uwagę na to, jak długo przechowywane są logi zastosowanego systemu. Z reguły wystarczającym czasem ich przechowywania jest 30 dni.

MONITORING WIZYJNY

Monitoring wizyjny to powszechna forma zabezpieczenia – spotykamy się z nim na co dzień. Często niestety bywa tak, że nie wiemy, że jesteśmy obiektem takiego monitorowania, co w tym przypadku jest błędem. Z punktu widzenia ochrony danych osobowych każda osoba przebywająca w obszarze monitorowanym w organizacji powinna być o tym fakcie wyraźnie poinformowana. Do tego celu wykorzystuje się tablice informujące o stosowanym monitoringu.

Poza poinformowaniem osoby, której dane dotyczą, o fakcie, że administrator rozpoczyna zbieranie jej danych, nie zapominajmy również o konieczności spełnienia obowiązku informacyjnego z art. 13 RODO. W klauzuli informacyjnej powinniśmy wskazać m.in. czas przechowywania nagrań. W przypadku gdy dane nie stanowią materiału dowodowego, np. w prowadzonym postępowaniu, nie powinien on przekraczać trzech miesięcy. Najczęściej spotykanym terminem jest jednak 30 dni, po których upływie utrwalony materiał jest nadpisywany.

Ważne jest to, aby kamery zastosowanego systemu obejmowały wszystkie wejścia nie tylko do organizacji, lecz także do krytycznych pomieszczeń z punktu widzenia ochrony danych osobowych, np. serwerowni, archiwum dokumentów papierowych, działu kadr lub księgowości. Warto pamiętać, że nagrania nie powinny obejmować pomieszczeń sanitarnych, szatni, stołówek, palarni oraz pomieszczeń udostępnianych zakładowej organizacji związkowej (chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do zapewnienia bezpieczeństwa pracowników, ochrony mienia, kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę). W zależności od podstawy prawnej lub charakteru przedsiębiorcy uzasadnione może być również rejestrowanie fonii – jednak są to sytuacje bardzo rzadkie.

Pracodawca jest zobowiązany do formalnego poinformowania swoich pracowników o stosowanym monitoringu, a także do zamieszczenia, np. w regulaminie pracy, szczegółowych informacji dotyczących monitoringu (jego celu, zakresu oraz sposobu zastosowania).

Uwaga: Często występującym błędem instalacji systemu monitoringu wizyjnego jest nieodpowiednie zabezpieczenie fizyczne rejestratora – urządzenia do utrwalania materiału wideo, które jest przeważnie używane w organizacjach. Najlepiej tego typu sprzęt przechowywać w odpowiednio zabezpieczonym pomieszczeniu, np. w serwerowni.

KONTROLA DOSTĘPU DO POMIESZCZEŃ BIUROWYCH

Odpowiednie zabezpieczenia fizyczne obszaru przetwarzania danych osobowych dotyczą nie tylko fizycznego dostępu do organizacji oraz monitoringu wizyjnego. Na uwagę w tym zakresie zasługują również pomieszczenia wydzielone w obszarze przetwarzania, w szczególności wskazywane już serwerownie, archiwa dokumentów, pomieszczenia działu personalnego, księgowego lub prawnego. Oczywiście zakres zastosowanych zabezpieczeń zależy od charakteru lub sposobu działania organizacji, ponieważ część działań związanych z przetwarzaniem danych osobowych może być wyoutsourcowana lub zwyczajnie niepotrzebna.

Niezależnie od powyższego każde z pomieszczeń, w którym przetwarzane są dane osobowe, powinno być zabezpieczane na czas nieobecności osób upoważnionych. Najwygodniejszym i najskuteczniejszym rozwiązaniem jest stosowanie systemu kontroli dostępu. Warto jednak zaznaczyć, że uprawnienia dostępu do pomieszczeń biurowych powinny być nadawanie podobnie jak uprawnienia na poziomie wykorzystywanych systemów do przetwarzania danych. Ogólnie zakres przydzielania uprawnień powinien opierać się na tzw. **zasadzie wiedzy koniecznej**. Zgodnie z nią konkretna osoba powinna mieć dostęp tylko i wyłącznie do pomieszczeń, które są jej niezbędne do realizacji jej codziennych obowiązków. Jeżeli w organizacji nie ma zautomatyzowanego rozwiązania umożliwiającego fizyczny dostęp do pomieszczeń biurowych, powinniśmy posiłkować się zwykłym kluczem mechanicznym.

Mówiąc o zabezpieczeniach samych pomieszczeń, należy też wspomnieć o zobowiązaniu pracowników do zamykania okien na czas nieobecności osób upoważnionych. Jest to szczególnie ważne w przypadku pomieszczeń znajdujących się na poziomie gruntu.

POLITYKA CZYSTEGO BIURKA

WIĘCEJ

Zabezpieczenie dostępu do organizacji, monitoring wizyjny i zabezpieczenie pomieszczeń biurowych to nie wszystkie środki, jakie powinniśmy podjąć, na bezpieczeństwo bowiem składa się zbiór zabezpieczeń. Należy pamiętać o tzw. polityce czystego biurka. W imię tej powszechnej zasady – choć niestety rzadko sumiennie stosowanej – każdy z pracowników powinien być zobowiązany do przechowywania dokumentów, które zawierają dane osobowe, w meblach biurowych zamykanych na klucz. Organizacja musi więc zapewnić swoim pracownikom wystarczającą liczbę takich mebli. Zasada, o której mowa, powinna obowiązywać przede wszystkim po godzinach pracy, ale również na czas każdej dłuższej nieobecności w pomieszczeniu osoby upoważnionej. Meble powinny być zamykane, a klucze – przechowywane w miejscu znanym jedynie osobom odpowiedzialnym za dokumenty tam składowane. Jeżeli organizacja dysponuje archiwum, które wykorzystuje do przechowywania dokumentów, dostęp do niego powinien być maksymalnie ograniczony.

Mówiąc o odpowiednim zabezpieczaniu dokumentów w formie papierowej, warto również wspomnieć o ich utylizacji. Do tego celu powinny być wykorzystywane tylko i wyłącznie niszczarki dokumentów lub specjalne pojemniki. W przypadku wyboru drugiego rozwiązania trzeba pamiętać, aby możliwość otworzenia pojemników miały tylko osoby do tego uprawnione. Stosowanie polityki czystego biurka będzie szczególnie ważne w sytuacji, gdy pracownicy UODO zdecydują się na kontrolę po godzinach pracy organizacji lub gdy przeprowadzana kontrola się wydłuży.

ZABEZPIECZENIA PRZECIWPOŻAROWE

Zabezpieczenie organizacji przed ewentualnym pożarem również może zainteresować kontrolujących z ramienia UODO. Wydawać się może, że związek tego obszaru z ochroną danych osobowych jest nikły, ale on również jest kontrolowany, więc warto przygotować się na to możliwie najdokładniej. Optymalna będzie tutaj sytuacja, w której o zabezpieczenia przeciwpożarowe dba administrator budynku, u którego organizacja – jako administrator w rozumieniu RODO – wynajmuje lokal. Z reguły w takim przypadku stosuje się m.in. hydranty, czujniki zadymienia, klapy oddymiające, gaśnice oraz zraszacze wodne. Jednak to, że administrator budynku powinien dbać o stosowany system, przeprowadzać jego przeglądy i testy, nie oznacza, że ostatecznie administrator danych osobowych nie jest odpowiedzialny za ochronę danych osobowych przed ich utraceniem w razie katastrofy.

W omawianym obszarze można popełnić wiele błędów, które z pewnością zauważą kontrolujący z UODO. Szczególnie należy wskazać na zraszacze, których działanie z pewnością jest efektywne, lecz mogą one skutecznie uszkodzić elementy infrastruktury IT lub dokumenty papierowe, dlatego nie można ich wykorzystywać w każdym pomieszczeniu. Niedopuszczalne jest instalowanie tych urządzeń w takich miejscach jak serwerownie lub archiwa. Serwerownia, w której najprawdopodobniej administrator przetwarza większość danych osobowych, powinna być wyposażona w odpowiednie systemy gaszenia. Najprostszym i jednocześnie najpopularniejszym rozwiązaniem jest wykorzystanie do tego celu gaśnicy. Powinna być ona przeznaczona do gaszenia urządzeń pod napięciem, co zagwarantuje, że nie uszkodzimy elementów infrastruktury w razie konieczności jej użycia. Gaśnica nie powinna znajdować się bezpośrednio w takim pomieszczeniu, a w oznaczonym miejscu tuż przed wejściem do niego. Co ważne, kontrolerzy mogą zweryfikować waż-

ność przeglądów zastosowanych gaśnic – ich brak jest jednym z najczęstszym błędów. Oczywiście administrator może też zastosować system gaszenia gazowego, którego instalacja i serwis niestety nie należą do najtańszych.

WIĘCEJ

ZABEZPIECZENIE POMIESZCZENIA SERWEROWNI

Do najtańszych nie należy też przygotowanie odpowiednio przystosowanego pomieszczenia serwerowni (na ten temat można by napisać osobny poradnik). W tym obszarze bardzo istotne jest zapewnienie odpowiedniej lokalizacji serwerowni w budynku. Nie powinna być ona zlokalizowana w miejscu, gdzie istnieje duże ryzyko zalania, np. piwnica, poddasze, pokój w bezpośrednim sąsiedztwie pomieszczeń sanitarnych i kuchni. Zaleca się, aby ściany serwerowni były murowane, najlepiej o podwyższonej odporności ogniowej. Zastosowanie ścian z karton-gipsu, które można przeciąć scyzorykiem, nie znajdzie uzasadnienia podczas kontroli. Podobnie drzwi do serwerowni powinny charakteryzować się wytrzymałością ogniową i najlepiej być antywłamaniowe. Zamontowanie drzwi przeszklonych lub z płyty wiórowej nie jest najlepszym rozwiązaniem. W pomieszczeniu serwerowni nie powinno być grzejników, instalacji wodno-kanalizacyjnych oraz okien, które podwyższają ryzyko włamania oraz powodują niepotrzebne nagrzewanie się pomieszczenia przez wpadające promienie słoneczne.

Uwaga: Ogólną zasadą zabezpieczeń fizycznego dostępu jest to, że powinny być one na tyle wytrzymałe, aby czas ich przełamania był dłuższy niż czas wykrycia próby ich przełamania, a także wystarczający do odpowiedniej reakcji pracowników ochrony.

Weryfikując omawiany obszar, należy też zwrócić uwagę na zapewnienie kontroli dostępu do pomieszczenia. Do tego celu możemy wykorzystać dwuskładnikową kontrolę dostępu w postaci np. kodu PIN oraz klucza mechanicznego (szerzej patrz rozdział „Kontrola dostępu do obszaru przetwarzania danych osobowych"). Coraz popularniejszym rozwiązaniem zapewniającym rozliczalność wejść do takich miejsc jest stosowanie systemów, które po wykryciu ruchu w pomieszczeniu wykonują zdjęcie osoby uzyskującej dostęp do strzeżonego obszaru, a stosowne o tym powiadomienie przesyłają natychmiastowo do wskazanych osób – z reguły do personelu działu IT. W celu usprawnienia tego rozwiązania należy skonfigurować powiadomienia tak, aby były one przesyłane do co najmniej dwóch osób oraz co najmniej dwoma różnymi kanałami kontaktu, np. wiadomość mailowa oraz SMS. Bardzo ważne jest też to, aby dostęp do pomieszczenia był ograniczony do minimalnej i tylko niezbędnej liczby osób upoważnionych.

Wskazówka: Jeżeli nie mamy zaawansowanego systemu kontroli dostępu i wykorzystujemy tylko klucz mechaniczny, warto zwrócić uwagę na miejsce jego przechowywania. Powinno ono gwarantować brak możliwości nieuprawnionego dostępu. Przechowywanie kluczy w niezamykanej szufladzie w recepcji nie jest najlepszym pomysłem, szczególnie gdy pracownik recepcji nie wie, komu taki klucz może udostępnić.

Przygotowując pomieszczenie serwerowni, nie powinniśmy zapominać o zachowaniu optymalnych warunków środowiskowych do bezpiecznej pracy urządzeń. W tym celu zaleca się wyposażenie pomieszczenia w czujniki temperatury (najlepiej umieszczone w górnej części szafy rack, w której zlokalizowano najwięcej sprzętu), wilgotności oraz zalania, które oczywiście powinny znaleźć się w najniższym punkcie pomieszczenia. Warto przy tym wspomnieć o systemie BMS (ang. *building management system*), który ma na celu kontrolę pracy wszystkich urządzeń pomiarowych. System integruje wiele sygnałów z różnych urządzeń i na bieżąco kontroluje ich stan. Każde odstępstwo od normy jest zgłaszane odpowiednim osobom np. w krótkiej wiadomości SMS oraz e-mail. Ponadto takie rozwiązanie zapewnia możliwość stałego podglądu stanu pracy instalacji oraz warunków środowiskowych przez Internet. Znacznie podnosi to poziom bezpieczeństwa przetwarzanych informacji i z pewnością spotka się z pozytywnym odbiorem podczas ewentualnej kontroli UODO.

Istotne jest utrzymanie odpowiedniej temperatury w pomieszczeniu. Duże nagromadzenie urządzeń teleinformatycznych w centrum danych powoduje emitowanie znacznych ilości ciepła. Przyjmuje się, że optymalna temperatura w serwerowni (w zależności od producentów urządzeń) to około 18–21°C. Parametr ten musi być automatycznie kontrolowany, dlatego niezbędny będzie system klimatyzacji dostosowany do kształtu i rozmiaru pomieszczenia. Rekomenduje się, aby serwerownia była wyposażona w przynajmniej dwa klimatyzatory, aby w razie awarii jednego z nich za odpowiednią temperaturę odpowiadał drugi. Dodatkowo instalacja klimatyzatorów powinna być wykonana tak, aby przełączały się one między sobą automatycznie i nie były umieszczone nad szafami rack, w których pracują urządzenia, ponieważ groziłoby to zalaniem.

Zanik zasilania stanowi jedno z podstawowych zagrożeń dla centrów przetwarzania danych, dlatego zastosowane zabezpieczenia zasilania energetycznego powinny gwarantować nieprzerwaną pracę serwerowni, nawet w razie nieprzewidzianych zakłóceń w dostawach energii. Najczęściej stosowanym zapasowych źródłem energii są UPS-y (ang. *uninterruptible power supply* – nieprzerywalne zasilanie energią), które dzięki wbudowanym stabilizatorom pozwalają zabezpieczyć urządzenia przed niespodziewanymi skokami napięcia oraz umożliwiają pracę serwerowni w trakcie krótkotrwałego zaniku zasilania. Czas podtrzymania awaryjnego zasilania może być kwestią sporną – zależy on od wielu czynników.

Warto jednak uwzględnić, że w przypadku automatycznej aktualizacji systemów operacyjnych stosowanych na serwerach obliczeniowych prawidłowe i bezpieczne ich automatyczne zamknięcie może potrwać nawet 45 minut. W przypadku przełączenia na zasilanie awaryjne ważne jest również to, żeby personel IT został o tym poinformowany. Konfiguracja systemu powinna zagwarantować automatyczne przesyłanie stosownej wiadomości do administratorów systemów. Przedsiębiorstwa, które nie mogą sobie pozwolić na przerwę w działaniu ich kluczowych systemów, powinny zadbać o to, aby w razie zaniku zasilania nastąpiło automatyczne przełączenie zasilania na agregat prądotwórczy lub alternatywną, niezależną linię zasilającą. Dodatkowo rekomenduje się okresowe testowanie poprawności działania takiego systemu oraz rzeczywistej sprawności UPS-ów.

ZABEZPIECZENIE POMIESZCZENIA ARCHIWUM

Podobnie jak do serwerowni administrator danych powinien ograniczyć dostęp fizyczny do archiwum dokumentów do minimalnej i niezbędnej liczby osób oraz zapewnić rozliczalność ich wejść i wyjść. W pomieszczeniu nie powinny znajdować się żadne źródła wody, w tym instalacje wodno-kanalizacyjne, często ukryte nad podwieszanym sufitem. Pomieszczenie archiwum powinno być pozbawione również okien.

Nie tylko na wypadek kontroli, lecz także przez cały okres użytkowania pomieszczenia dokumenty znajdujące się w archiwum powinny być przechowywane na podwyższeniu – nawet w zwykłych regałach. Ważne jest to, żeby dokumentacja nie była przechowywana bezpośrednio na podłodze (co niestety dzieje się dość często), ponieważ powoduje to ryzyko jej zalania. Zainstalowanie czujników zalania w pomieszczeniu archiwum będzie z pewnością pozytywnie ocenione przez organ nadzorczy.

ZABEZPIECZENIE STACJI ROBOCZYCH I LAPTOPÓW

Zabezpieczenie stacji roboczych i laptopów również może zostać poddane ewentualnej kontroli organu nadzorczego. W pierwszej kolejności warto zweryfikować, jakie systemy operacyjne obsługują urządzenia i czy wśród nich nie funkcjonuje jeszcze system, który nie ma już wsparcia producenta (najczęściej jest to stary system operacyjny z rodziny Microsoft w wersji Windows XP). Bardzo ważny jest nadzór nad ich prawidłową aktualizacją, co może być szczególnie trudne w przypadku rozbudowanej infrastruktury. Z pomocą administratorom systemów przychodzą zautomatyzowane rozwiązania, których wdrożenie zdecydowanie warto rozważyć. Mowa o usługach służących do centralnej dystrybucji wszelkich łatek i poprawek systemowych opublikowanych przez producenta danego systemu. Dodatkowo należy zaznaczyć, że poprawne zarządzanie siecią komputerów jest bardzo utrudnione lub prawie niemożliwe bez tzw. usługi katalogowej w postaci Active Directory.

Wskazówka: Zweryfikujmy oprogramowanie zainstalowane na komputerach pod kątem jego legalności i przydatności.

Kolejny element, którzy trzeba uwzględnić przy konfiguracji sprzętu, to zakres uprawnień użytkowników. Powinien on być ograniczony, w przeciwnym razie pracownik organizacji, który niekoniecznie posiada wiedzę w zakresie bezpieczeństwa, będzie mógł nie tylko dokonywać zmian konfiguracyjnych używanego systemu, lecz także instalować dodatkowe oprogramowanie, którego warunki licencyjne tego zabraniają. Ponadto przy okazji pobrania dodatkowego oprogramowania z nieoficjalnego źródła użytkownik może uruchomić złośliwy kod – zaszyfruje on dostęp do przetwarzanych danych, a w zamian za klucz odszyfrowujący przestępca, który stoi za atakiem, zażąda np. opłaty. Uprawnienia administracyjne powinny mieć zatem tylko i wyłącznie te osoby, których zakres zadań i obowiązków to uzasadnia, a ponadto które mają odpowiednią wiedzę.

Podobnie jak w przypadku pomieszczeń biurowych tutaj również należy zadbać o kontrolę dostępu do systemu. W tym celu każdemu użytkownikowi powinien zostać nadany indywidualny identyfikator systemowy (tzw. login). Następnie należy zadbać o odpowiednią politykę haseł dostępowych. RODO – w przeciwieństwie do poprzedniego stanu prawnego – nie narzuca administratorom w tym obszarze żadnych wytycznych. Nie oznacza to jednak, że haseł w ogóle nie powinno być i że nie powinny one zmieniać się okresowo. Nie możemy przecież zrezygnować z bezpieczeństwa na rzecz wygody użytkownika. Najczęściej stosowaną w tym zakresie praktyką jest wymuszanie haseł składających się z minimum 8 znaków, w tym małych i dużych liter, cyfr lub znaków specjalnych, których zmiana następuje nie rzadziej niż raz na kwartał. Dobrze skonfigurowana polityka haseł przewiduje również inne reguły. Jedną z nich jest zapamiętywanie przez system ostatnio użytych haseł, np. 10 wstecz. Dzięki temu zapobiegniemy sytuacji, w której użytkownik podczas wymuszonej przez system zmiany hasła ustawi taki sam klucz, jaki stosował poprzednio. Pamiętajmy też o konfiguracji minimalnego czasu życia hasła. Z pewnością trzeba wykazać się dużym sprytem, żeby obejść zabezpieczenia dotyczące konfiguracji zapamiętywania ostatnio użytych haseł, jednak nieco bardziej zaawansowani użytkownicy mogą wpaść na pomysł, aby zmieniać swoje hasło dopóty, dopóki nie powrócą do klucza, którego używali poprzednio. Reguła minimalnego czasu życia hasła z pewnością skutecznie im w tym przeszkodzi.

WIĘCEJ

Nie zapominajmy także o konfiguracji wymuszania zmiany haseł tymczasowych. Często popełnianym przez pracowników błędem jest niezmienianie haseł przekazanych przez dział IT na potrzeby pierwszego logowania. Jeśli system nie wymusi takiej zmiany lub użytkownik nie wykona tej czynności manualnie, to przez okres, w którym hasło tymczasowe jest używane, mamy do czynienia z brakiem rozliczalności działań pracowników. Często nie są oni świadomi tego, że skoro używają danych logowania przekazanych przez inną osobę (nieważne, że jest to dział IT), to znaczy, że oprócz nich ktoś jeszcze ma do nich dostęp. Warto pamiętać, że logi systemowe przypiszą wszelkie czynności wykonane na koncie dostępowym użytkownika do jego właściciela, a nie do osoby, która faktycznie działała w systemie.

Pamiętajmy też o wdrożeniu tymczasowej lub całkowitej blokady konta systemowego w przypadku kilkukrotnej próby wprowadzenia niepoprawnych danych logowania. Najlepiej jeśli system automatycznie powiadomi administratora o blokadzie. Dzięki takiemu rozwiązaniu zminimalizujemy ryzyko przełamania poświadczeń uwierzytelniających przy użyciu ataków typu *brute force* oraz zachowamy większą kontrolę nad nieautoryzowanymi próbami dostępu do danych. Szczególnej ostrożności w tym względzie wymagają systemy, do których dostęp jest realizowany przez przeglądarkę internetową korzystającą z publicznej sieci.

Wszyscy wiemy, że procedury organizacyjne mają jedną wspólną właściwość – nie zawsze działają tak, jak zamierzono. Świetnym tego przykładem jest powszechny w takich procedurach obowiązek pracowników dotyczący blokowania stacji roboczych na czas nieobecności osoby upoważnionej. Żeby zminimalizować ryzyko nieuprawnionego dostępu do danych lub ryzyko stwierdzenia naruszenia w trakcie kontroli, warto wdrożyć zwykłe wygaszacze ekranów. Zablokują one konto automatycznie – za użytkownika – po upływie np. 5 minut od braku jego aktywności. Zastosowanie takiego rozwiązania nie powinno w żadnym wypadku zwalniać pracowników z wykonywania tej czynności manualnie. Należy bowiem pamiętać o wspominanej już zasadzie, że bezpieczeństwo to zbiór zabezpieczeń. Samo skonfigurowanie wygaszacza to nie wszystko. Z pewnością trafimy w organizacji na osoby, którym automatyczna blokada się nie spodoba, więc wpadną na pomysł, żeby zmienić tę konfigurację. Administratorzy systemów powinni zablokować taką możliwość.

Czynności użytkownika nie mogą wpływać również na konfigurację systemu antywirusowego, który powinien pracować na każdym komputerze wykorzystywanym w organizacji. Pod żadnym pozorem pracownik nie może mieć możliwości wyłączenia systemu antywirusowego, np. w sytuacji gdy jego prewencyjne działanie uniemożliwia mu odwiedzenie ulubionej strony internetowej lub

otwarcie pliku z pendrive'a znalezionego przed wejściem do organizacji. Podobnie jak w przypadku systemów operacyjnych należy zadbać o systematyczną aktualizację systemu antywirusowego oraz wykorzystywanych przez niego sygnatur wirusów. Przy większej infrastrukturze i bez odpowiednich narzędzi to zadanie może okazać się trudne i czasochłonne. Jego realizację może ułatwić skonfigurowanie konsoli do zdalnego zarządzania całą siecią systemu. Dzięki takiemu rozwiązaniu administrator systemów zdalnie, z jednego miejsca, będzie mógł szybciej reagować na zagrożenia zidentyfikowane przez system i odpowiednio nadzorować przebieg aktualizacji systemu na każdej stacji roboczej.

Niestety system antywirusowy nie jest lekiem na całe zło. Oprócz wysyłania cyklicznych wiadomości przypominających pracownikom o podstawowych zasadach postępowania z powierzonym sprzętem oraz informujących ich o nowych zagrożeniach warto zadbać o coś jeszcze – żadne z powyższych zabezpieczeń nie uchroni bowiem danych przed dostępem do nich w razie kradzieży lub zgubienia sprzętu (szczególnie dotyczy to urządzeń przenośnych, np. smartfonów, tabletów, nośników wymiennych oraz laptopów). Najskuteczniejszym w tym zakresie zabezpieczeniem jest szyfrowanie pamięci. Podczas jego wdrażania należy zwrócić uwagę na konieczność wprowadzenia zabezpieczenia na całej przestrzeni dyskowej, a nie tylko dla wybranych partycji, ponieważ nigdy nie możemy mieć pewności, w którym dokładnie miejscu użytkownik zdecyduje się zapisać ważne informacje. Dodatkowo uwierzytelnianie powinno następować dwuskładnikowo – z wykorzystaniem hasła do dysku oraz hasła na poziomie systemu operacyjnego. Szyfrowanie jest na tyle silnym zabezpieczeniem, że w szczególnych sytuacjach może doprowadzić do utraty dostępu do danych, np. gdy firma z jakiegoś powodu rozstanie się z pracownikiem w mało pozytywnych relacjach, a ten w odwecie nie przekaże swojego hasła do dysku. Dlatego też administratorzy systemów powinni przechowywać tzw. klucze odzyskiwania. Chociaż korzystanie z nich jest ostatecznością, przydadzą się również na wypadek, gdy użytkownik sprzętu zapomni swojego hasła.

Podczas przeglądu konfiguracji komputerów użytkowników istotne są też takie szczegóły jak prawidłowe ustawienie ekranów monitorów w sposób uniemożliwiający wgląd osobom postronnym w wyświetlane treści. Jeżeli układ pomieszczenia na to nie pozwala lub jeśli pracownicy wykonują swoje czynności służbowe w dużej mierze zdalnie, warto rozważyć wyposażenie ekranów w filtry ograniczające kąt ich widzenia.

WIĘCEJ

Wskazówka: Na każdym komputerze administrator systemu powinien zapewnić oprogramowanie do zabezpieczania załączników wiadomości elektronicznych. Warto również poinstruować pracowników, w jaki sposób wykorzystywać tego typu oprogramowanie w codziennej pracy.

ZABEZPIECZENIE URZĄDZEŃ MOBILNYCH

Smartfony i tablety to urządzenia wciąż niedostrzegane pod kątem bezpieczeństwa. Najczęściej w organizacjach sprzęt tego typu kupuje dział administracji/zakupów, a użytkownik sam dokonuje jego konfiguracji we własnym zakresie. Należy pamiętać, że urządzenia mobilne dorównują wydajnością komputerom – a w wielu przypadkach zastępują ich funkcjonalności – i przetwarzają całą masę danych, w tym zarówno danych osobowych, jak i informacji stanowiących tajemnice przedsiębiorstwa. Jednym z największych zagrożeń jest konfiguracja na takim sprzęcie dostępu do poczty elektronicznej, na której mogą znajdować się nie tylko cenne wiadomości, lecz także niezabezpieczone załączniki. Warto mieć też świadomość, że poczta elektroniczna daje szeroki wachlarz możliwości, np. umożliwia zmianę hasła, z wykorzystaniem opcji „Przypomnij hasło", do kluczowego systemu organizacji. W jaki sposób zabezpieczyć więc urządzenia mobilne?

Konfiguracje na poziomie samego urządzenia, dokonywane przez personel działu IT, mogą okazać się nieskuteczne, ponieważ wpływ na nie ma również użytkownik końcowy tego sprzętu (jeżeli stosowana kontrola dostępu w postaci kodu PIN będzie dla pracownika niewygodna, to zwyczajnie ją wyłączy). Z pomocą administratorom systemów informatycznych przychodzi w tym zakresie oprogramowanie typu MDM (ang. *mobile device management*), służące do zdalnego zarządzania urządzeniami mobilnymi. Dzięki niemu personel działu IT za pomocą kilku kliknięć jest w stanie wymusić, a co za tym idzie – ustandaryzować konfigurację floty smartfonów lub tabletów, niezależnie od wykorzystywanej przez nie platformy (iOS, Android, Windows).

Jednym z najważniejszych elementów bezpieczeństwa, które należy skonfigurować w urządzeniach mobilnych, jest kontrola dostępu. Niezależnie od tego, czy metodą uwierzytelniania jest wpisanie kodu PIN, hasła, czy znaku graficznego, jest to pierwsza linia obrony danych osobowych przetwarzanych przez administratora przed nieautoryzowanym dostępem powodującym naruszenie bezpieczeństwa. Sama autoryzacja użytkownika nie jest w tym przypadku wystarczająca. Warto zadbać o to, żeby zabezpieczenia smartfonów i tabletów wykorzystywanych przez organizację były zbliżone do zabezpieczeń stosowanych w komputerach. Jaki sens miałoby bowiem zabezpieczanie komputerów, skoro wyciek danych może nastąpić przez niezabezpieczone smartfony? Należy mieć tu na uwadze ogólną zasadę – zabezpieczenia są tak silne, jak ich najsłabsze ogniwo. Warto więc, podobnie jak w przypadku innych urządzeń, stosować szyfrowanie pamięci wbudowanej oraz dołączanych kart pamięci. Nie zaszkodzi, a na pewno pozytywnie wpłynie na bezpieczeństwo zapewnienie na tego typu urządzeniach oprogramowania antywiru-

sowego i wygaszacza ekranu, automatycznie blokującego dostęp do sprzętu po upływie wskazanego czasu bezczynności użytkownika, a także wdrożenie wytycznych dotyczących stosowanych haseł oraz ograniczeń w zakresie instalacji oprogramowania bez odpowiednich do tego uprawnień.

Jedną z bardzo istotnych funkcjonalności rozwiązań typu MDM jest możliwość zdalnego wymazania pamięci urządzenia lub jego zlokalizowania w razie zgubienia lub kradzieży. Warto jednak pamiętać, że uruchomienie funkcjonalności związanej ze śledzeniem urządzenia jest tożsame ze śledzeniem pracownika, a to może wpłynąć na jego prywatność, szczególnie jeśli użytkownik nie rozstaje się z urządzeniem również po godzinach pracy. Takie działanie (podobnie jak używanie lokalizatora zainstalowanego w pojazdach służbowych) jest dozwolone pod pewnym warunkiem. Otóż w celu jego zalegalizowania należy formalnie i w przejrzysty sposób poinformować pracownika o stosowaniu takich systemów.

ZABEZPIECZENIE URZĄDZEŃ DRUKUJĄCYCH

Ze względu na bezpieczeństwo należy szczególnie zwrócić uwagę na te urządzenia drukujące, które znajdują się w ciągach komunikacyjnych i są przeznaczone dla wielu użytkowników, często dla pracowników całego piętra lub całej organizacji. Głównym zagrożeniem jest nieprawidłowe wykorzystywanie takiego sprzętu. Chodzi przede wszystkim o pozostawianie wydruków zawierających dane osobowe lub poufne informacje na urządzeniach, bez nadzoru osoby upoważnionej. Żaden z administratorów danych nie chciałby dowiedzieć się, że kurier, dostawca wody, listonosz lub pracownik UODO natknął się na wydrukowaną listę płac lub listę potencjalnych klientów, pozostawioną na korytarzu bez nadzoru osoby upoważnionej. W celu minimalizacji ryzyka związanego z zasygnalizowaną sytuacją można wykorzystać dość popularną i skuteczną funkcjonalność, którą zapewnia zdecydowana większości tego typu urządzeń, polegającą na wdrożeniu autoryzacji wydruku. Konfiguracja takiego zabezpieczenia powoduje, że użytkownik przed zrealizowaniem wydruku jest zmuszony „zameldować się" przy drukarce, co może polegać np. na odbiciu karty RFID, nawet tej samej, którą pracownik wykorzystuje do uzyskania dostępu do organizacji i pomieszczenia, w którym realizuje swoje czynności służbowe. Takie rozwiązanie jest zarówno wygodne, jak i bezpieczne – pod warunkiem odpowiedniego postępowania z przydzieloną kartą. Innym sposobem może być wprowadzenie kodu PIN zdefiniowanego przez pracownika. Niestety w tym przypadku – jeżeli administrator systemów nie zdecyduje się na zdefiniowanie sposobu budowania PIN-ów – pracownicy organizacji mogą pójść na skróty i tworzyć zbyt oczywiste, a przez to łatwe do odgadnięcia kody, np. 1234, 0000, 5555 itp.

Przy okazji wdrożenia autoryzacji wydruku warto zweryfikować, czy administrator systemów nie zapomniał ograniczyć uprawnień administracyjnych do urządzenia oraz czy zmienił domyślne dane uwierzytelniające na poziomie administracyjnym. W przeciwnym razie nieoczekiwanie ktoś może wpłynąć na konfigurację sprzętu. Dodatkowo zalecane jest ograniczenie możliwości skanowania dokumentów, co dotyczy miejsc, gdzie ich wysyłanie jest dozwolone. W tym celu stosuje się różne konfiguracje, np. zdefiniowanie stałej listy odbiorców, ograniczenie ich wyłącznie do domeny organizacji lub do zasobów sieciowych. W tym ostatnim przypadku należy pamiętać, aby w myśl zasady wiedzy koniecznej skanowanie było realizowane zawsze na indywidualny katalog pracownika, a nie katalog wymiany danych pomiędzy pracownikami danego działu lub całej organizacji.

Co ważne, urządzenia drukujące mają wbudowaną pamięć, nazywaną buforem wydruku. W zależności od jego przewidzianej przestrzeni przez pewien czas przechowywane są tam wszystkie wydrukowane dokumenty. Urządzenie udostępnione osobie postronnej – bez jego wcześniejszego odpowiedniego przygotowania – może stanowić cenne źródło informacji na temat organizacji. Zabezpieczeniem minimalizującym ilość przechowywanych danych jest konfiguracja okresowego czyszczenia bufora pamięci wydruku, np. w cyklach 2-godzinnych.

ZARZĄDZANIE KOPIAMI ZAPASOWYMI

Kopie zapasowe (tzw. backup) to obszerny temat, dlatego w niniejszym poradniku ograniczamy się jedynie do błędów najczęściej popełnianych w procesie zarządzania nimi. Niezależnie od rozmiaru organizacji lub wykorzystywanych zaawansowanych technologii bardzo często można zaobserwować, że wykonany backup

WIĘCEJ

jest przechowywany w niewłaściwym miejscu. Jak się okazuje, najczęściej wybieranym miejscem są nośniki, na których pracują systemy produkcyjne, których kopia została wykonana. Wówczas mamy do czynienia z sytuacją, w której w razie pożaru, zalania, zainfekowania serwera lub awarii administrator traci zarówno dane produkcyjne, na bieżąco wykorzystywane, jak i wykonane kopie bezpieczeństwa. W wyniku takiego zdarzenia organizacja nie tylko zostanie pozbawiona parametru dostępności do danych, lecz także najprawdopodobniej poniesie ogromne straty finansowe spowodowane utrudnieniami lub niemożnością kontynuowania biznesu. Na zapewnienie bezpieczeństwa przechowywania kopii zapasowych naciskały już przepisy w poprzednim stanie prawnym. Nie liczmy więc na to, że pracownicy UODO ominą ten obszar w razie kontroli przeprowadzanej na gruncie RODO.

Gdzie w takim razie przechowywać wykonane kopie zapasowe? Najlepiej w innej lokalizacji lub przynajmniej w innej strefie pożarowej niż pracujące środowiska produkcyjne.

Przykład: Kopie mogą być przechowywane w sejfach/szafach ogniotrwałych czy skrytkach bankowych. Dobrym sposobem na zapewnienie bezpieczeństwa przechowywania kopii zapasowych jest ich replikacja na serwer w innej lokalizacji lub wykorzystanie do tego celu tzw. chmury.

Warto pamiętać, że dane w chmurze to dane na serwerach jakiegoś dostawcy tej usługi, a administrator nigdy nie może mieć pewności, kto ostatecznie ma dostęp do wszystkich jego danych oraz w jaki sposób są one zabezpieczone. Ponadto należy zaznaczyć, że sama czynność przechowywania jest, w myśl definicji tego pojęcia, przetwarzaniem danych osobowych, a zatem wiąże się z zawarciem odpowiedniej umowy z podmiotem zewnętrznym dostarczającym rozwiązanie chmurowe. Co ważne, utrwalane tam kopie powinny zostać zabezpieczone już po stronie administratora, z wykorzystaniem skutecznego szyfrowania. **Zalecamy stosowanie szyfrowania wszędzie tam, gdzie to możliwe**. Dotyczy to również kopii zapasowych utrwalonych na nośnikach, a następnie umieszczonych w sejfie organizacji, do którego mają dostęp np. pracownicy kadrowi lub księgowi. Na podstawie nieodpowiednio zabezpieczonych kopii zapasowych osoba nieuprawniona może bowiem odtworzyć wszystkie dane osobowe przetwarzane przez administratora. Dlatego też bardzo ważne jest ich odpowiednie zabezpieczenie przed zagrożeniami nie tylko zewnętrznymi, lecz także wewnętrznymi.

Kolejnym elementem, dość często pomijanym przez administratorów systemów informatycznych, jest weryfikacja integralności wykonanych kopii bezpieczeństwa. Nie sposób testować ich wszystkich, ale warto robić to wybiórczo i nie dopiero w razie zaistnienia potrzeby ich odtworzenia. Najczęściej stosowaną praktyką jest testowanie kopii zapasowych w odstępach kwartalnych. Dzięki temu zminimalizujemy ryzyko braku możliwości odtworzenia backupu w sytuacji kryzysowej. Dużo uwagi nie wymaga również konfiguracja powiadomień systemu służącego do wykonywania kopii z informacją o prawidłowo lub nieprawidłowo wykonanym procesie.

Omawiając kopie bezpieczeństwa, należy wspomnieć o lokalnych dyskach komputerów pracowników, którzy zawsze powinni posiadać skonfigurowany dostęp do zasobów sieciowych, np. usługi serwera plików. Dzięki temu użytkownicy będą mieć możliwość utrwalania dokumentów elektronicznych w miejscu, z którego wykonywane są kopie bezpieczeństwa, umożliwiające odzyskanie dostępu do danych w razie infekcji komputera, jego zgubienia, kradzieży lub uszkodzenia systemu. Niestety nie wszyscy użytkownicy są świadomi, jakie korzyści niesie za sobą wykorzystywanie zasobów sieciowych udostępnionych przez organizację, dopóki nie utracą danych. Dlatego też szkolenia to bardzo ważny element bezpieczeństwa każdej organizacji, bo nie bez powodu twierdzi się, że człowiek to najsłabsze ogniowo każdego systemu zabezpieczeń. Nie musimy jednak ograniczać się w tym zakresie tylko i wyłącznie do edukacji. Dość często spotykanym i zdecydowanie wartym rozważenia zabezpieczeniem jest synchronizacja wybranych, najczęściej używanych przez pracowników katalogów lokalnych z zasobem sieciowym. Rzadszym, ale również możliwym do zastosowania zabezpieczeniem jest blokowanie możliwości zapisu danych lokalnie.

ZEWNĘTRZNE PODMIOTY DZIAŁAJĄCE W OBSZARZE TELEINFORMATYCZNYM

Gdzie w obszarze teleinformatycznym zidentyfikujemy podmioty, z którymi należy aneksować umowę na zgodność z RODO, czyli uregulować stosunek powierzenia przetwarzania danych osobowych pomiędzy administratorem a tzw. procesorem? Obszar IT jest niestety często pomijany, jeśli chodzi o odpowiednie uregulowanie umów z podmiotami przetwarzającymi, a jak się okazuje – jest to skrupulatnie weryfikowane przez kontrole UODO. Może być wiele miejsc, w których zewnętrzne podmioty działające w obszarze teleinformatycznym mogą mieć dostęp do danych osobowych przetwarzanych przez administratorów. Warto jednak w pierwszej kolejności skupić się na podmiotach:

- **świadczących usługi wsparcia dla systemów wykorzystywanych przez organizację, służących do przetwarzania danych osobowych – w tym nie tylko zewnętrzne działy IT, lecz także okazjonalny support systemów,**
- **dostarczających organizacji systemy w modelu SaaS, w którym systemy przetwarzają dane osobowe na serwerach dostawcy usługi,**
- **świadczących serwis sprzętu teleinformatycznego, w tym np. serwis komputerów, smartfonów i tabletów, serwerów, urządzeń sieciowych, urządzeń drukujących,**
- **świadczących usługę utylizacji sprzętu teleinformatycznego,**
- **świadczących dzierżawę urządzeń służących do przetwarzania danych osobowych (pod warunkiem braku ich odpowiedniego przygotowania przez organizację przed zwrotem/wymianą),**
- **świadczących usługi audytowe lub dotyczące testów stosowanych zabezpieczeń.**

WIĘCEJ

Zakończenie

W niniejszym poradniku krok po kroku omówiliśmy podstawowe zagadnienia związane z kontrolą przeprowadzaną przez pracowników UODO, najważniejsze i najczęściej występujące w organizacji procesy przetwarzania danych, wskazując w każdym z nich kluczowe działania, jakie powinieneś podjąć w celu zapewnienia zgodności z RODO, oraz wytłumaczyliśmy, jak na kontrolę UODO przygotować się od strony IT.

Poradnik z pewnością będzie dla Ciebie pomocny, jeżeli zechcesz podjąć się niełatwego zadania, jakim jest wdrażanie RODO w organizacji, lub gdy zostaniesz wyznaczony do przeprowadzenia audytu kontrolnego systemu ochrony danych osobowych jako osoba pełniąca funkcję inspektora ochrony danych w organizacji czy będąca nieformalnym koordynatorem ds. ochrony danych osobowych.

Wierzymy, że dzięki poruszeniu problematycznych zagadnień rozwialiśmy Twoje wątpliwości, z którymi borykasz się na co dzień. Staraliśmy się przekazać wszystkie nasze przemyślenia oraz wskazówki, jak również opisać obowiązki nałożone na administratorów przepisami prawa w najbardziej przystępny sposób. Celem, który nam przyświecał, było bowiem stworzenie praktycznej instrukcji. Liczymy na to, że będziesz kierować się nią na co dzień, angażując się w procesy przetwarzania danych osobowych.

Mamy również nadzieję, że nasze praktyczne porady i uwagi w zakresie kontroli przeprowadzanych przez UODO sprawią, że myśl o nich nie będzie przysparzać Ci tyle stresu. Teraz już wiesz, czego kontrolerzy mogą od Ciebie oczekiwać, jak wygląda kontrola i jak się do niej przygotować, tak aby nic Cię nie zaskoczyło.

Chcesz wiedzieć więcej?

Strefa RODO
Najważniejsze zmiany i nowości
ODO24.pl/RODO

RODO nawigator
Tekst i praktyczne odesłania
ODO24.pl/RODO-Nawigator

Pomoc ODO 24
Bezpłatne porady
ODO24.pl/Pomoc

Biuletyn informacyjny
Tylko to, co najważniejsze
ODO24./Biuletyn

Publikacje naszych ekspertów

ODO24.pl/publikacje

Notatki

Ochrona Danych Osobowych

BEZPIECZEŃSTWO INFORMACJI

Audyt zgodności

Wykonujemy pełny audyt zgodności z RODO. Badamy zarówno bezpieczeństwo urządzeń, systemów, sieci i aplikacji, jak i poprawność klauzul, regulaminów oraz rejestrów. Doradzamy, jak praktycznie wdrożyć nasze zalecenia.

DPIA i analiza ryzyka

Analizę ryzyka i DPIA rozumiemy jako fundament RODO – sposób na racjonalizację kosztów ochrony danych oraz troskę o prywatność osób, których dane Państwo przetwarzają.

Wdrożenie RODO

Wypełniamy „neutralne" technologicznie RODO. Pomagamy dostosować: procesy biznesowe (np. marketing, rekrutacja), środowisko teleinformatyczne, dokumentację ochrony danych.

Przejęcie funkcji IOD

Pełniąc funkcję IOD, wspomagamy i nadzorujemy organizację w utrzymaniu zgodności z RODO. Działamy szybko i efektywnie dzięki doświadczonym ekspertom z obszaru prawa, IT oraz zarządzania ryzykiem.

Bieżące wsparcie

Dzięki dostarczanym przez nas narzędziom oraz wiedzy jesteśmy w stanie przyczynić się do monitorowania i rozwoju funkcjonującego u Państwa systemu ochrony danych osobowych.

Szkolenia otwarte

Dzielimy się wiedzą, pomagamy w zdobyciu umiejętności i wyposażamy w narzędzia, które umożliwią Państwu skuteczne wykonywanie obowiązków związanych z ochroną danych osobowych.

Szkolenia zamknięte

Dostosowujemy je do potrzeb organizacji oraz specyfiki branży, w której działa. Stawiamy na praktykę – Państwa pracownicy nauczą się wykorzystywać wiedzę o RODO w swojej codziennej pracy.

E-learning

Nasza platforma pozwala w krótkim czasie (nawet w największej organizacji) przeszkolić personel oraz zweryfikować nabytą wiedzę. Minimalizujemy w ten sposób najczęstszą przyczynę incydentów – nieświadomość pracowników.

Narzędzia

Dostarczamy rozwiązania pozwalające kontrolować przepływ danych w organizacji, w tym prowadzić niezbędne rejestry oraz zarządzać szkoleniami, incydentami, upoważnieniami etc.

Usługi powiązane

Pomoc w razie kontroli UODO, wsparcie we wdrożeniu systemu ISO 27001, ISO 20000, ISO 22301, a także dyrektywy NIS (tzw. cyberustawy).

Jedna specjalizacja

SZEROKA PERSPEKTYWA

- Przepisy prawa
- Bezpieczeństwo sieci i systemów IT
- Zarządzanie ryzykiem
- Bezpieczeństwo fizyczne
- Wiedza i świadomość personelu

ODO24.pl
tel. 22 740 99 00