NAJCZĘSTSZE PROBLEMY DOTYCZĄCE WDROŻENIA RODO

1. Stosowanie RODO w praktyce str. 1
2. Obowiązek powołania inspektora ochrony danych str. 2
3. Zasady prowadzenia analizy ryzyka str. 2
4. Prowadzenie rejestru czynności przetwarzania str. 3
5. Ewidencja i zgłaszanie naruszeń ochrony danych str. 4
6. Zawarcie umowy powierzenia z biurem rachunkowym str. 4
7. Administrator systemów informatycznych str. 4
8. Udokumentowanie braku powołania IOD str. 4

1. Stosowanie RODO w praktyce

Już przeszło rok we wszystkich krajach Unii Europejskiej obowiązuje rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych – zwane RODO). W tym czasie w naszym kraju weszła w życie nowa ustawa o ochronie danych osobowych, która zastąpiła dotychczas obowiązującą ustawę o tym samym tytule, a z dniem 4 maja 2019 r. tzw. ustawa wdrażająca RODO, która znowelizowała m.in. przepisy Kodeksu pracy, ustawy o zakładowym funduszu świadczeń socjalnych, Prawa bankowego czy Prawa zamówień publicznych.

Wszystkie zmiany w przepisach, z którymi mieliśmy do czynienia przez ostatni rok (tj. od 25 maja 2018 r.), mimo iż niewątpliwie potrzebne, powodują wiele wątpliwości u administratorów danych, do których należą zarówno podmioty publiczne, jak i prywatne firmy. Polski organ nadzoru, tj. Prezes Urzędu Ochrony Danych Osobowych przeprowadził bilans stosowania RODO w jednostkach samorządu terytorialnego, który wypadł pozytywnie. Zwrócił jednak uwagę na aspekty wdrażania RODO, które przysporzyły tym jednostkom najwięcej problemów. Były to rejestry mieszkańców, monitoring wizyjny, zasoby Biuletynów Informacji Publicznej (BIP). UODO stwierdził, że z niewłaściwym zarządzaniem danymi osobowymi i ich ochroną, co wykazały kontrole, mamy do czynienia w Biuletynie Informacji Publicznej. Szczególnie kłopotliwy okazał się brak wytycznych wobec okresu przechowywania danych w BIP. W związku z tym przez wiele lat uznawano, że informacja raz tam przekazana ma prawo w niej funkcjonować wieczyście, a nie jest to zgodne z przepisami o ochronie danych osobowych. Inne problemy związane z BIP, to m.in. przekazywanie danych osobowych w nadmiernym zakresie, bez niewłaściwego procesu anonimizacji danych, brak procedur usuwania informacji oraz stron internetowych urzędów. W tych obszarach samorządowcy mieli problemy ze stosowaniem ogólnego rozporządzenia o ochronie danych osobowych.

Prezes UODO zwrócił uwagę, iż administratorzy w jednostkach samorządu terytorialnego powinni inwestować w edukację personelu (w tym kierownictwa) z zakresu ochrony danych osobowych, a także rozważyć tworzenie kodeksów postępowań.

Również Europejska Rada Ochrony Danych (EROD) zebrała wyniki ankiet, wypełnionych przez organy nadzorcze krajów Europejskiego Obszaru Gospodarczego (EOG) i sporządziła bilans dotychczasowych osiągnięć. Na szczeblu krajowym większość organów nadzorczych zgłasza wzrost liczby zapytań i skarg w porównaniu z rokiem 2017. Odnotowano duży wzrost świadomości obowiązywania przepisów dotyczących ochrony danych osobowych wśród społeczeństwa europejskiego. Przykładem jest większa niż przed wejściem w życie RODO liczba skarg i zgłoszonych naruszeń. UODO stwierdza, iż wpływa do niego średnio 25 skarg dziennie (na dzień 15 maja 2019 r. Urząd zarejestrował 9.246 skarg).

Polski organ nadzorczy nałożył dopiero dwie kary z tytułu naruszenia przepisów dotyczących ochrony danych osobowych (stan na dzień oddania dodatku do druku). Pierwsza dotyczyła niedopełnienia obowiązku informacyjnego wynikającego z art. 13 RODO i wyniosła ponad 943 tys. zł. Druga kara została nałożona za upublicznienie zbyt szerokiego zakresu danych osobowych w sieci. Jej wysokość wyniosła 55.750,50 zł.

Obecnie administratorzy danych muszą wobec osób, których dane przetwarzają, spełniać obowiązki informacyjne wynikające z RODO. Rozporządzenie stanowi, że informacje zawarte w art. 13 i 14 muszą być przekazywane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy kierowane są do dziecka. Informacje mogą być udzielane na piśmie lub w inny sposób, w tym, w stosownych przypadkach – elektronicznie. Motyw 60 preambuły do RODO stanowi, że osoba, której dane dotyczą, musi być poinformowana o prowadzeniu operacji przetwarzania i o jej celach. Administrator danych osobowych powinien podać takiej osobie wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych. Ponadto musi poinformować osobę, której dane dotyczą, o fakcie profilowania oraz o konsekwencjach takiego profilowania. Jeżeli dane osobowe są gromadzone, należy ją też poinformować, czy ma ona obowiązek je podać, oraz o konsekwencjach ich niepodania.

Do najczęstszych problemów, z jakimi zmagają się administratorzy danych należą:

– prawidłowe wypełnianie obowiązków informacyjnych,
– prowadzenie rejestru czynności przetwarzania,
– prowadzenie analizy ryzyka,
– konieczność lub brak powołania inspektora ochrony danych,
– prowadzenie ewidencji naruszeń ochrony danych,
– zawieranie umów powierzenia.

Przykład klauzuli informacyjnej w placówce medycznej

Zgodnie z art. 13 RODO informuję, iż:

1. Administratorem Pani/Pana danych osobowych jest: Publiczny Zakład Opieki Zdrowotnej Przychodnia Kolejowa. Kontakt do administratora: ul. Krakowska 116, 34-120 Andrychów, tel. 601 415 845.
2. Dane osobowe są zbierane w celu udzielania świadczeń opieki zdrowotnej, prowadzenia, przechowywania i udostępniania dokumentacji medycznej.
3. Podstawę do przetwarzania danych osobowych stanowi:
   – art. 6 ust. 1 lit. c) RODO,
   – art. 9 ust. 2 lit. h) RODO,
   – ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2019 r. poz. 1127 ze zm.),
   – ustawa o zawodach lekarza i lekarza dentysty (Dz. U. z 2019 r. poz. 537 ze zm.),
   – rozporządzenie Ministra Zdrowia w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz. U. z 2015 r. poz. 2069).
4. Odbiorcami Pani/Pana danych osobowych są podmioty, o których mowa w art. 26 ust. 3 pkt 1–12 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz podmioty przetwarzające (podmioty, którym powierzono przetwarzanie danych osobowych w zakresie: przeglądów, napraw i serwisu aparatury medycznej i sprzętu medycznego, serwisu i utrzymania systemów informatycznych, konsultacji medycznych, zlecania badań i usług medycznych).
5. Pani/Pana dane przechowywane są przez okres 20 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu, z wyjątkiem sytuacji przewidzianych w art. 29 ust. 1 pkt 1–4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.
6. Przysługuje Pani/Panu prawo do żądania od administratora: dostępu do treści swoich danych, ich sprostowania, usunięcia, ograniczenia przetwarzania, a także prawo do przenoszenia danych lub do wniesienia sprzeciwu wobec ich przetwarzania oraz wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie Pani/Pana danych osobowych przez Administratora narusza przepisy RODO.
7. Podanie danych osobowych jest wymogiem ustawowym. Brak podania niniejszych danych uniemożliwi realizację celu związanego z udzielaniem świadczeń opieki zdrowotnej.
8. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany, w tym w oparciu o profilowanie.

2. Obowiązek powołania inspektora ochrony danych

Po wejściu w życie przepisów RODO wielu administratorów danych miało problem ze stwierdzeniem czy w ich jednostce istnieje obowiązek powołania inspektora ochrony danych (IOD), czy też nie.

RODO przewiduje obowiązek wyznaczenia inspektora dla administratorów i podmiotów przetwarzających, gdy:
- przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości, przy czym przez organy i podmioty publiczne zobowiązane do wyznaczenia IOD rozumie się w Polsce jednostki sektora finansów publicznych (np. jednostki samorządu terytorialnego, uczelnie publiczne), instytuty badawcze oraz Narodowy Bank Polski,
- główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą na dużą skalę,
- główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO oraz danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o których mowa w art. 10 RODO.

Zasady powoływania inspektorów ochrony danych uszczegóławia polska ustawa o ochronie danych osobowych, która stanowi, że przez organy i podmioty publiczne należy rozumieć:
- jednostki sektora finansów publicznych, o których mowa w art. 9 ustawy o finansach publicznych (patrz ramka),
- instytuty badawcze, o których mowa w ustawie o instytutach badawczych,
- Narodowy Bank Polski.

Pozostałe podmioty przetwarzające dane osobowe, niespełniające tych kryteriów, nie mają obowiązku ustanawiania inspektora, choć mogą oczywiście powołać taką osobę fakultatywnie.

Kto może zostać inspektorem?

RODO jest dość lakoniczne w zakresie wymagań, jakie ma spełniać inspektor ochrony danych. Stwierdza jedynie, że IOD powinien być wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, które nakłada na niego RODO.

Prezes UODO na stronie internetowej www.uodo.gov.pl podaje, że inspektor powinien posiadać:
- fachową wiedzę z zakresu krajowych i europejskich przepisów o ochronie danych osobowych,
- fachową wiedzę z zakresu praktyk w dziedzinie ochrony danych osobowych,
- dogłębną znajomość przepisów RODO,
- wiedzę biznesową i sektorową dotyczącą działalności administratora,
- odpowiednią wiedzę na temat procesów przetwarzania danych, systemów informatycznych oraz zabezpieczeń stosowanych u administratora i jego potrzeb w zakresie ochrony danych,
- w przypadku organów i podmiotów publicznych IOD powinien również wykazywać się znajomością procedur administracyjnych i funkcjonowania jednostki.

Priorytetem inspektora powinno być zapewnienie przestrzegania RODO. Inspektor ma zatem odgrywać kluczową rolę w zakresie wspierania „kultury ochrony danych" oraz pomagać w implementacji niezbędnych elementów RODO, tj.:
- zasad przetwarzania danych osobowych,
- praw osób, których dane dotyczą,
- ochrony danych w fazie projektowania oraz domyślnej ochrony danych,
- prowadzenia rejestru czynności przetwarzania,
- wymogów bezpieczeństwa przetwarzania,
- zgłaszania naruszeń do organów nadzorczych.

Jeśli chodzi o osobiste cechy inspektora kwalifikujące go do wykonywania tej funkcji, to są to: rzetelne podejście do wykonywania swoich obowiązków i wysoki poziom etyki zawodowej.

Uprawnienia inspektora

RODO stanowi, że to administrator danych musi zapewnić, aby inspektor był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Ponadto musi wspierać IOD w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do ich wykonania oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej. Inspektor nie może otrzymywać instrukcji dotyczących wykonywania tych zadań, nie może też zostać odwołany bądź ukarany przez administratora za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora. Może też wykonywać inne zadania i obowiązki, jednakże administrator lub podmiot przetwarzający muszą zapewnić, aby takie zadania i obowiązki nie powodowały konfliktu interesów. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem krajowym. Inspektor może być pracownikiem administratora lub podmiotu przetwarzającego bądź wykonywać zadania na podstawie umowy o świadczenie usług.

Inspektor ochrony danych jest pierwszą osobą, z którą mogą kontaktować się osoby, których dane przetwarza administrator danych lub podmiot przetwarzający we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

Zgłoszenie w organie nadzorczym

Zasadniczo administrator lub podmiot przetwarzający zawiadamia Prezesa UODO o wyznaczeniu inspektora w ciągu 14 dni od dnia jego wyznaczenia. Jedynym prawidłowym i skutecznym sposobem zawiadomienia o wyznaczeniu jest zawiadomienie w postaci elektronicznej, opatrzone kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.

Sektor finansów publicznych to:
- organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały,
- jednostki samorządu terytorialnego oraz ich związki,
- związki metropolitalne,
- jednostki budżetowe,
- samorządowe zakłady budżetowe,
- agencje wykonawcze,
- instytucje gospodarki budżetowej,
- państwowe fundusze celowe,
- ZUS i zarządzane przez niego fundusze oraz KRUS i fundusze zarządzane przez Prezesa KRUS,
- NFZ,
- samodzielne publiczne zakłady opieki zdrowotnej,
- uczelnie publiczne,
- PAN i tworzone przez nią jednostki organizacyjne,
- państwowe i samorządowe instytucje kultury,
- inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych, banków i spółek prawa handlowego.

3. Zasady prowadzenia analizy ryzyka

Unijne rozporządzenie o ochronie danych osobowych wymaga od administratorów danych dokonywania samodzielnej oceny ryzyka, jakie przetwarzanie danych osobowych może spowodować dla praw i wolności osób, których te dane dotyczą. Przy czym przepisy RODO nie wskazują w tym zakresie żadnych wytycznych, jak taką analizę prowadzić.

Podejście oparte na ryzyku

Nie można wskazać jednej, uniwersalnej metody szacowania ryzyka. Prowadząc analizę ryzyka w zakresie ochrony danych osobowych administrator danych może opierać się na wdrożonych wcześniej normach, np. ISO. Pewne wskazówki w zakresie prowadzenia tej analizy daje również publikacja UODO pt. „Jak stosować podejście oparte na ryzyku?", dostępna na stronie www.uodo.gov.pl.

W pierwszej kolejności należy zidentyfikować i sklasyfikować wszystkie aktywa organizacji, które wiążą się z przetwarzaniem danych osobowych. Przez aktywa rozumie się przede wszystkim informacje zawierające dane osobowe, ale również inne zasoby jednostki jak np. jej pracownicy, sprzęt, oprogramowanie oraz inne środki techniczne i organizacyjne związane z przetwarzaniem danych osobowych. Następnie należy przeanalizować stosowane w jednostce zabezpieczenia. Głównym celem stosowania zabezpieczeń jest zmniejszenie występującego ryzyka. Zabezpieczenia można podzielić na:
- organizacyjne (wdrożone polityki bezpieczeństwa, regulaminy ochrony danych osobowych),
- personalne (upoważnienie do przetwarzania danych osobowych, oświadczenia o poufności),
- techniczne (system antywirusowy, firewall),
- fizyczne (strefy bezpieczeństwa, alarmy, monitoring).

Krok 1 – identyfikacja zagrożeń

Szacowanie ryzyka polega na określeniu, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i jakie będą tego konsekwencje.

Uwzględniając sklasyfikowane wcześniej aktywa występujące u danego administratora danych oraz opisane procesy przetwarzania danych osobowych należy przeanalizować i oszacować:
- występujące zagrożenia dla bezpieczeństwa przetwarzanych danych,
- zastosowane środki bezpieczeństwa,
- podatność przyjętych rozwiązań z uwzględnieniem zastosowanych środków bezpieczeństwa,
- potencjalne następstwa w przypadku zaistnienia określonych zagrożeń.

Mając opisane aktywa danej jednostki, wykaz zidentyfikowanych zagrożeń oraz stosowanych zabezpieczeń należy określić, jaka jest podatność na poszczególne zagrożenia.

Krok 2 – analiza i ocena następstw

Zdefiniowanie występujących zagrożeń i podatności pozwala na ustalenie, jakie mogą być ich następstwa, np. straty finansowe, kary finansowe nakładane przez Prezesa UODO, utrata reputacji przez firmę. Po wykonaniu wszystkich tych kroków, tj.:
- rozpoznaniu aktywów,
- zidentyfikowaniu zagrożeń,
- uwzględnieniu podatności,
- oceny potencjalnych następstw,

należy dokonać całościowej oceny poziomu ryzyka, na jakie narażone są przetwarzane dane.

Krok 3 – szacowanie poziomu ryzyka

Urząd w opracowaniu wskazał, że: „Mając wyznaczone prawdopodobieństwo wystąpienia określonego zdarzenia oraz straty, jakie mogą być nim spowodowane (tj. wielkość skutku), wyznacza się wartość ryzyka jako iloczyn prawdopodobieństwa wystąpienia danego zdarzenia i jego skutku".

Wartość tę można wyliczyć m.in. za pomocą metody ilościowej, przy zastosowaniu wzoru:

R = S × P

gdzie:
- **R** – ryzyko,
- **P** – prawdopodobieństwo wystąpienia zdarzenia,
- **S** – skutki wystąpienia incydentu.

Do wyliczenia ryzyka wykorzystuje się ustaloną wcześniej skalę. Dla P – prawdopodobieństwa wystąpienia zdarzenia są to:
- zagrożenie niskie – 1,
- zagrożenie średnie – 2,
- zagrożenie wysokie – 3.

Natomiast dla skutków (S) ustala się skalę:
- małe (do 10.000 zł) – 1,
- średnie (powyżej 10.000 zł – 100.000 zł) – 2,
- duże (powyżej 100.000 zł) – 3.

W kolejnym kroku administrator danych porównuje wyliczone ryzyka ze skalą. Ustala skalę właściwą dla ryzyka:
- 1–2 – ryzyko pomijalne i akceptowalne (należy zaakceptować),
- 3–6 – ryzyko jest opcjonalne (trzeba zaakceptować albo obniżyć),
- 9 – ryzyko jest nieakceptowalne (należy wdrożyć szybkie działania).

Krok 4 – podjęcie działań

Kolejną czynnością, jaką należy wykonać po oszacowaniu ryzyka dla poszczególnych operacji przetwarzania, jest podjęcie decyzji dotyczącej poszczególnych ryzyk. Przykładowo można wymienić następujące działania:
- modyfikowanie (redukcja) ryzyka – polega na obniżeniu poziomu ryzyka; np. zmniejszenie prawdopodobieństwa wystąpienia zdarzenia spowodowanego przerwą w dostawie energii można osiągnąć włączając w układ zasilania odpowiednią automatykę i niezależne źródła energii (UPS, generatory),
- akceptowanie ryzyka – to świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w działaniu organizacji,
- unikanie ryzyka – polega na unikaniu przez organizację działań, które powodują powstanie określonych typów ryzyka,
- dzielenie (przeniesienie) ryzyka – polega np. na scedowaniu skutków ryzyka na kontrahenta (m.in. na podwykonawcę).

Przykład

Administrator ustala wartość ryzyka dla sprzętu komputerowego, zagrożonego kradzieżą. W związku z tym, że w firmie nie jest zainstalowany system alarmowy, określa, że prawdopodobieństwo wystąpienia incydentu jest wysokie – 3. Sprzęt komputerowy wykorzystywany jest w bieżącej pracy z danymi osobowymi klientów. Skutki kradzieży sprzętu i wycieku danych osobowych ocenia na średnie.

Ryzyko wyliczone według przyjętej formuły wynosi 6 (3 × 2 = 6). Administrator danych postanawia je obniżyć, wdrażając odpowiednie zabezpieczenia w postaci instalacji alarmu.

4. Prowadzenie rejestru czynności przetwarzania

Prowadzenie rejestru czynności przetwarzania to jeden z tych obowiązków wynikających z RODO, który również sprawia administratorom danych dużo problemów. Jednakże właściwe opisanie i pogrupowanie czynności przetwarzania może ułatwić administratorowi zarządzanie procesami przetwarzania i ochrony danych. Jest też konieczne na wypadek kontroli Prezesa UODO.

Rodzaje i zawartość rejestrów

Obowiązek prowadzenia rejestru czynności przetwarzania wynika z art. 30 ust. 1 ogólnego rozporządzenia o ochronie danych, który stanowi, że każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora, prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. Motyw 82 RODO określa dwa podstawowe cele prowadzenia rejestru:

– zachowanie przez administratora i podmiot przetwarzający zgodności z RODO,
– umożliwienie organowi nadzorczemu monitorowania prowadzonego przetwarzania.

Rejestr prowadzony przez administratora danych powinien zawierać:

a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych,
b) cele przetwarzania,
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwę tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentację odpowiednich zabezpieczeń,
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
g) jeśli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

Podmioty przetwarzające, tj. osoby fizyczne lub prawne, organy publiczne, jednostki lub inne podmioty, które przetwarzają dane osobowe w imieniu administratora, prowadzą rejestry wszystkich kategorii czynności przetwarzania wykonywanych w imieniu zlecających im je administratorów danych. Ich rejestry powinny zawierać:

a) imię i nazwisko lub nazwę oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych,
b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,
c) gdy ma to zastosowanie – przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentację odpowiednich zabezpieczeń,
d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

Kto powinien prowadzić rejestr?

Art. 30 ust. 5 RODO stwierdza, że obowiązek rejestrowania czynności przetwarzania (zarówno przez administratorów, jak i podmioty przetwarzające) nie ma zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób. Jednocześnie jednak wskazuje przesłanki, których zaistnienie aktualizuje obowiązek prowadzenia takiego rejestru. Wskazane w tym przepisie wyłączenia powodują, że również przedsiębiorcy i pracodawcy zatrudniający mniej niż 250 osób zobowiązani są prowadzić taki rejestr, jeżeli przetwarzanie:

– którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą,
– nie ma charakteru sporadycznego lub
– obejmuje szczególne kategorie danych osobowych, lub
– obejmuje dane osobowe dotyczące wyroków skazujących i czynów zabronionych.

Najwięcej wątpliwości budzi sformułowanie „sporadyczność przetwarzania danych osobowych". Sporadyczny oznacza występujący rzadko. W przypadku prowadzenia działalności gospodarczej czy też wykonywania innej funkcji przez podmiot np. zatrudniający pracowników, trudno mówić o sporadycznym przetwarzaniu danych osobowych. Większość procesów przetwarzania danych osobowych, np. pracowników czy klientów, odbywa się bowiem w sposób ciągły.

Czym są czynności przetwarzania?

Rejestr dotyczy czynności przetwarzania, konieczne jest więc zdefiniowanie tego pojęcia. Niestety RODO takiej definicji nie zawiera. Nasz krajowy organ nadzoru, czyli Prezes Urzędu Ochrony Danych Osobowych, w publikacji „Wskazówki i wyjaśnienia dotyczące obowiązku rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO" zawartej na stronie www.uodo.gov.pl stwierdza, iż: „W kontekście obowiązku określonego w art. 30 ust. 1 RODO przyjąć należy, że czynności przetwarzania to zespół powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane. Tytułem przykładu: w przypadku rekrutacji pracowników, jeden cel będzie obejmował wiele cząstkowych operacji niewymagających szczegółowego ich opisywania w rejestrze, takich jak: pozyskiwanie informacji o kandydatach z ofert nadesłanych w wyniku ogłoszenia, dokonywanie ich selekcji, uzyskiwanie dodatkowych informacji w ramach przeprowadzania wywiadów z wybranymi osobami, usunięcie danych osób, które nie zostały wskazane do zatrudnienia itp. Nie ma konieczności opisywania każdej poszczególnej operacji wykonywanej na danych w procesie określonym zbiorczo »rekrutacja pracowników«, bo nie jest to konieczne dla scharakteryzowania przetwarzania w świetle wskazanych w art. 30 ust. 1 RODO kryteriów".

Nazwa i dane kontaktowe administratora danych:

UNI-TECH SP. Z O.O., UL. GRABSKIEGO 15, ŁÓDŹ, TEL. 682-543-781, unitech@net.pl

Dane kontaktowe Inspektora Ochrony Danych:

AGNIESZKA KOWALIK, TEL. 654-987-654, iod.unitech@net.pl

REJESTR CZYNNOŚCI PRZETWARZANIA

Lp.	Nazwa czynności przetwarzania	Dział	Cel przetwarzania	Kategorie osób, których dane dotyczą	Kategorie danych	Planowany termin usunięcia danych	Nazwa systemu/ oprogramowania	Ogólny opis zastosowanych środków	Kategorie odbiorców
1.	Rekrutacja pracowników	Dyrektor	Rekrutacja pracowników	Kandydaci do pracy	Dane identyfikacyjne, dane adresowe, o wykształceniu, stażu pracy, uprawnieniach zawodowych.	Po zakończeniu procesu rekrutacyjnego.	System kadry. Dokumentacja papierowa.	Dostęp tylko dla osób upoważnionych, kontrola dostępu do systemu informatycznego, zamykane szafy i pomieszczenia.	Dane nie są przekazywane innym podmiotom.
2.	Prowadzenie akt pracowniczych i ewidencji czasu ich pracy	Stanowisko ds. kadr	Prowadzenie dokumentacji pracowniczej zgodnie z Kodeksem pracy	Pracownicy	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, przebiegu pracy, absencji, dane o zakresie obowiązków, stawce wynagrodzenia, karach i nagrodach oraz inne dane wymagane przepisami prawa pracy.	Zgodnie z: – art. 94^5 Kodeksu pracy, – art. 125a ustawy o emeryturach i rentach z Funduszu Ubezpieczeń.	System kadry. Płatnik. Dokumentacja papierowa.	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań.	ZUS, inne firmy ubezpieczeniowe – dotyczy tylko osób posiadających polisy ubezpieczeniowe.
3.	Umowy cywilnoprawne	Stanowisko ds. kadr	Realizacja obowiązków wynikających z zawartych umów cywilnoprawnych	Osoby realizujące zadania na podstawie umów zlecenia i o dzieło	Zbiór danych osobowych zwykłych: imię, nazwisko, dane kontaktowe.	10 lat	System kadry. Dokumentacja papierowa.	Dostęp tylko dla osób upoważnionych, kontrola dostępu do systemu informatycznego, zamykane szafy i pomieszczenia.	Odbiorcy upoważnieni z mocy przepisów prawa i podmioty przetwarzające, z którymi administrator danych zawarł umowy powierzenia.
4.	Kontrahenci będący osobami fizycznymi	Obsługa zamówień	Realizacja i rozliczanie umów	Osoby świadczące usługi, realizujące zawarte umowy	Dane osobowe zwykłe: imię nazwisko, nazwa firmy, NIP, dane kontaktowe.	6 lat	Programy komputerowe. Dokumentacja papierowa.	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań.	Odbiorcy upoważnieni z mocy przepisów prawa i podmioty przetwarzające, z którymi administrator danych zawarł umowy powierzenia.

5. Ewidencja i zgłaszanie naruszeń ochrony danych

Jednym z nowych obowiązków, jakie nałożyło na administratorów danych RODO, jest zgłaszanie do organów nadzorczych incydentów naruszeń ochrony danych osobowych. W Polsce takim organem jest Prezes Urzędu Ochrony Danych Osobowych.

Czym jest naruszenie ochrony danych?

Administrator danych ma obowiązek zgłoszenia przypadku naruszenia ochrony danych osobowych, jeżeli naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W przypadku wykrycia naruszenia ochrony danych osobowych w pierwszej kolejności należy przeanalizować czy takie ryzyko wystąpiło. Jeśli administrator danych uzna, że takie ryzyko nie zaistniało, wówczas nie ma obowiązku dokonywania zgłoszenia.

Organ nadzorczy może zwrócić się do administratora o uzasadnienie decyzji o niezgłaszaniu naruszenia, w związku z tym wnioski z przeprowadzonej analizy trzeba udokumentować w wewnętrznej ewidencji naruszeń.

Prezes UODO na swojej stronie internetowej www.uodo.gov.pl informuje, że: „Ryzyko naruszenia praw i wolności osób fizycznych jest obecne, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono".

Szkodami takimi są np. dyskryminacja, kradzież tożsamości lub oszustwo dotyczące tożsamości, nadużycia finansowe, straty finansowe, nieuprawnione cofnięcie pseudonimizacji, utrata poufności danych osobowych chronionych tajemnicą zawodową, naruszenie dobrego imienia lub inne znaczące skutki gospodarcze lub społeczne dla danej osoby fizycznej. Jeżeli naruszenie dotyczy danych osobowych ujawniających pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych lub danych genetycznych, dotyczących zdrowia lub życia seksualnego, należy uznać, że występuje duże prawdopodobieństwo takiej szkody.

Jak je dokumentować?

RODO w art. 33 ust. 5 nakłada na administratorów danych obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Użyte w tym artykule sformułowanie „wszelkich naruszeń" oznacza, że ewidencja powinna obejmować wszystkie naruszenia spełniające kryteria określone w definicji zawartej w art. 4 pkt 12 RODO (patrz ramka). Są to zarówno naruszenia, które nie wymagały dokonania zgłoszenia, jak i te podlegające temu obowiązkowi.

Jeżeli chodzi o sposób prowadzenia ewidencji, to Grupa Robocza Art. 29 stoi na stanowisku, że administrator może zdecydować o dokumentowaniu naruszeń w rejestrze czynności przetwarzania prowadzonym zgodnie z art. 30 RODO. Nie ma wymogu prowadzenia osobnego rejestru naruszeń, gdy informacje dotyczące naruszenia można łatwo zidentyfikować i przedłożyć na żądanie.

Kiedy trzeba zgłosić?

W przypadku gdy ryzyko naruszenia praw i wolności osób fizycznych zaistniało, to zgłoszenia należy dokonać niezwłocznie, najpóźniej w ciągu 72 godzin. Gdy administrator nie jest w stanie dokonać zgłoszenia w tym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

Zgłoszenia naruszenia dokonuje się elektronicznie za pomocą formularza dostępnego na stronie Urzędu Ochrony Danych Osobowych, który należy dołączyć do pisma ogólnego dostępnego na platformie biznes.gov.pl bądź wysłać przez ePUAP na adres elektronicznej skrzynki podawczej:/GIODO/SkrytkaESP. Możliwe jest również wysłanie formularza w postaci załącznika na adres elektronicznej skrzynki podawczej:/GIODO/SkrytkaESP.

Administrator powinien ustalić, czy zaistniałe naruszenie było wynikiem błędu ludzkiego, czy problemu systemowego. Następnie powinien ocenić, w jaki sposób można zapobiec takiemu incydentowi w przyszłości, np. poprzez szkolenia pracowników, jeżeli to czynnik ludzki zawinił.

Kiedy powiadomić poszkodowanych?

Jeśli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator danych bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Przy czym nie jest konieczne, by faktycznie doszło do naruszenia praw lub wolności osoby, której dane są przetwarzane. Wystarczający jest fakt samego pojawienia się wysokiego ryzyka naruszenia praw lub wolności.

Zawiadomienia należy dokonać niezwłocznie, jasnym i prostym językiem, opisując charakter naruszenia ochrony danych osobowych. Powinno ono również opisywać m.in. środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych w przyszłości.

Jak podaje Prezes Urzędu Ochrony Danych Osobowych: „Poinformowanie na czas osób fizycznych o zaistniałym naruszeniu ma na celu umożliwienie podmiotom danych podjęcie niezbędnych działań zapobiegawczych dla ochrony przed negatywnymi skutkami naruszenia. Jako przykład można wskazać wyciek haseł bankowych, w przypadku którego reakcja banku powinna być natychmiastowa".

Definicja naruszenia ochrony danych osobowych (art. 4 pkt 12 RODO)

Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

6. Zawarcie umowy powierzenia z biurem rachunkowym

Prowadzę działalność gospodarczą w zakresie rozliczania podatkowego małych firm. Moi klienci nie zatrudniają pracowników, zdarza się jednak, że zawierają umowy o dzieło. Czy w związku z tym ze wszystkimi klientami powinnam podpisać umowę o przetwarzanie danych osobowych?

TAK. Czytelniczka prowadząc opisaną działalność spełnia definicję podmiotu przetwarzającego. Takim podmiotem jest w rozumieniu RODO osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Z taką sytuacją mamy do czynienia w przypadku biur rachunkowych, które świadczą swoje usługi na rzecz pracodawców lub przedsiębiorców. To, że klienci Czytelniczki nie zatrudniają pracowników powoduje, że przetwarzanych danych osobowych jest na pewno mniej. Nie zmienia to jednak faktu, że Czytelniczka przetwarza inne dane osobowe w imieniu swoich klientów. Chodzi tu m.in. o dane osobowe zawarte np. w rejestrach VAT (faktury zawierające dane osobowe przedsiębiorców będących osobami fizycznymi), w dowodach zakupów wykorzystywanych np. przy prowadzeniu ewidencji ryczałtu itp. Czytelniczka przetwarza też dane osobowe przy rozliczeniach rocznych np. gdy jej klienci rozliczają się wspólnie ze swoimi małżonkami. RODO ma zastosowanie do danych osobowych wszystkich osób fizycznych.

Przetwarzanie przez podmiot przetwarzający musi odbywać się na podstawie umowy, która określa: przedmiot i czas trwania przetwarzania, jego charakter i cel, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

Umowa powinna stanowić w szczególności, że podmiot przetwarzający:

– przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora,

– zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,

– podejmuje wszelkie środki wymagane na mocy art. 32 RODO (tj. wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić właściwy stopień bezpieczeństwa przetwarzanym danym),

– przestrzega warunków korzystania z usług innego podmiotu przetwarzającego,

– pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w RODO,

– uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO (m.in. zgłasza do PUODO naruszenia ochrony danych osobowych),

– po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych,

– udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia nałożonych na niego obowiązków oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

W związku z powyższym Czytelniczka powinna zawrzeć stosowne umowy z klientami.

7. Administrator systemów informatycznych

Zgodnie z przepisami powołaliśmy inspektora ochrony danych. Czy oprócz niego należy powołać również administratora systemów informatycznych? Czy ewentualnie jedna osoba może pełnić obie te funkcje?

Żaden z przepisów unijnego rozporządzenia o ochronie danych osobowych ani też polska ustawa o ochronie danych osobowych nie wymagają powołania administratora systemów informatycznych. Nie posługują się też takim pojęciem. W wielu jednak firmach i instytucjach takie stanowisko istnieje. Było też popularne pod rządami poprzednio obowiązujących przepisów. W związku z tym, w dokumentach wielu podmiotów, jak np. polityka bezpieczeństwa czy instrukcja zarządzania systemami informatycznymi, takie stanowiska się pojawiają. Administrator danych ma możliwość dowolnego tworzenia wewnętrznej struktury organizacyjnej, a powoływanie ASI lub np. pełnomocników do spraw niejawnych jest w polskich firmach bardzo popularne.

O ile przepisy nie wymagają obecnie powołania ASI, to jego powołanie powinni rozważyć administratorzy danych, którzy przetwarzają w większości dane osobowe z wykorzystaniem systemów informatycznych. W strukturze takiego podmiotu powinien pojawić się wówczas ASI, ale oczywiście decyzja o jego ustanowieniu należy do administratora danych.

Ewentualna możliwość łączenia funkcji administratora systemów informatycznych (ASI) czy też pełnomocników do spraw niejawnych z wykonywaniem funkcji inspektora ochrony danych wciąż budzi spore kontrowersje. Z obecnie obowiązujących przepisów nie wynika zakaz łączenia takich funkcji. Zdarza się więc, że na funkcję inspektorów ochrony danych powoływane są właśnie takie osoby. Przyjęcie takiego rozwiązania może prowadzić do sytuacji, w której IOD będzie nadzorował w ramach przyznanych mu kompetencji swoje własne czynności wykonywane jako administrator systemów informatycznych. Z tego względu lepszym rozwiązaniem jest wyznaczanie IOD spośród pracowników, którzy nie są zatrudnieni przy przetwarzaniu danych osobowych. Postuluje się, aby IOD miał funkcję zupełnie niezależną od pionu informatycznego.

8. Udokumentowanie braku powołania IOD

Jednostka przeprowadziła analizę i wydaje się nam, że nie musimy powoływać inspektora ochrony danych. Czy fakt ten należy jakoś udokumentować na potrzeby ewentualnej kontroli?

TAK. Administrator i podmiot przetwarzający mają obowiązek wyznaczać IOD, zawsze gdy:

– przetwarzania dokonuje organ lub podmiot publiczny,

– główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę,

– główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO.

Pozostałe podmioty o powołaniu IOD decydują same. Grupa Robocza Art. 29 zaleca administratorom i podmiotom przetwarzającym udokumentowanie wewnętrznej procedury przeprowadzonej w celu ustalenia obowiązku bądź braku obowiązku wyznaczenia inspektora. Celem stworzenia takiego dokumentu jest wykazanie, iż stosowne czynniki odnośnie obowiązku powołania IOD zostały przez administratora danych lub podmiot przetwarzający uwzględnione.