Fragment

Bezpieczeństwo danych osobowych. Podejście oparte na ryzyku

Rozdział I. Przepisy i normy dotyczące ochrony danych osobowych

1. Wymagania nałożone przez RODO

Przepisy RODO stanowią jedną z wielu odpowiedzi na szybki rozwój technologiczny i gwałtowną globalizację. W art. 2 RODO wskazano, że akt ten ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych. Zautomatyzowane przetwarzanie należy rozumieć jako przetwarzanie maszynowe, komputerowe. Nie ma znaczenia, w jakim momencie cyklu życia danych osobowych przetwarzanie zostanie wykorzystane. To oznacza, że **RODO znajduje zastosowanie do każdego przetwarzania danych osobowych za pomocą systemów komputerowych**.

Ważne

Rozporządzenie europejskie jest podobne do polskich ustaw, ma charakter wiążący i obowiązuje bezpośrednio w każdym kraju członkowskim Unii Europejskiej. Oznacza to, że do RODO należy stosować się tak, jakby to była polska ustawa.

1.1. Ochrona praw i wolności osób fizycznych

Osoby fizyczne są w samym centrum konstrukcji RODO. Wybitnie podkreślono to w art. 1 ust. 1 i 2 RODO, wskazującym, że są to przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych, chroniące podstawowe prawa i wolności osób fizycznych, a w szczególności ich prawo do ochrony danych osobowych. Już z tych zapisów można wyciągnąć wniosek, że **bezpieczeństwo, jakie należy zapewnić przetwarzanym danym osobowym, ma chronić osoby fizyczne, ich podstawowe prawa i wolności**.

W RODO nie zdefiniowano, czym są prawa i wolności osób fizycznych. W takiej sytuacji należy przyjąć, że są to te wartości, które wymieniono w KPP, mianowicie:

1) godność, w tym: **poszanowanie godności ludzkiej**, prawo do życia oraz do integralności fizycznej i psychicznej, zakaz tortur i poniżającego traktowania lub karania, zakaz niewolnictwa i pracy przymusowej;
2) wolność, w tym m.in.: **prawo do ochrony danych osobowych**, prawo do wolności i bezpieczeństwa osobistego, do poszanowania prywatności i życia rodzinnego, prawo zawarcia małżeństwa i założenia rodziny, wolność myśli, sumienia i religii, wolność zgromadzania się i stowarzyszania się, prawo do nauki, wolność wyboru zawodu i prawo podejmowania pracy w każdym państwie członkowskim;
3) równość, w tym m.in.: równość wobec prawa, **zakaz wszelkiej dyskryminacji**, prawa dziecka, prawa osób starszych, prawa osób niepełnosprawnych;
4) solidarność, w tym m.in.: prawo pracowników do informacji i konsultacji, do rokowań i działań zbiorowych, dostępu do pośrednictwa pracy, **prawo do ochrony przed nieuzasadnionym zwolnieniem z pracy**, prawo do godziwych warunków pracy, zakaz pracy dzieci i ochrona młodocianych w pracy, prawna, ekonomiczna i społeczna ochrona rodziny, prawo do zabezpieczenia społecznego i pomocy społecznej, do ochrony zdrowia;
5) prawa obywatelskie, w tym m.in.: prawo głosowania i kandydowania w wyborach do Parlamentu Europejskiego i w wyborach lokalnych, prawo do dobrej administracji, swoboda przemieszczania się i pobytu, wymiaru sprawiedliwości, w tym prawo dostępu do bezstronnego sądu i do skutecznego środka odwoławczego.

W motywie 75 RODO wskazano, jak przetwarzanie może negatywnie wpływać na prawa lub wolności osób fizycznych: ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego, szkody majątkowej lub niemajątkowej. W szczególności ma to następujące skutki:

1) dyskryminacja,
2) kradzież tożsamości,
3) oszustwo dotyczące tożsamości,
4) strata finansowa,
5) naruszenie dobrego imienia,
6) naruszenie poufności danych osobowych chronionych tajemnicą zawodową,
7) nieuprawnione odwrócenie pseudonimizacji,
8) znaczna szkoda gospodarcza lub społeczna.

1.2. Zabezpieczenie danych

Wymagania dotyczące zabezpieczenia danych osobowych są nakreślone w RODO bardzo ogólnie. Może to sprawiać wrażenie, że w tym akcie prawnym kwestie bezpieczeństwa są potraktowane jako poboczne. Nic bardziej mylnego – śmiało można powiedzieć, że **zabezpieczenie danych to co najmniej połowa całego wysiłku, który należy włożyć w zapewnienie zgodności z wymaganiami RODO**.

Najbardziej interesująca część RODO ze względu na tematykę niniejszej publikacji, dotycząca zabezpieczania danych, to sekcja 2 „Bezpieczeństwo danych osobowych" w roz-

dziale IV (art. 32, 33 i 34 RODO). W art. 32 ust. 1 RODO wskazano, że uwzględniając stan wiedzy technicznej, koszt wdrażania zabezpieczeń i charakter, zakres, kontekst i cele przetwarzania danych osobowych oraz ryzyko naruszenia praw i wolności osób fizycznych (które może mieć różne prawdopodobieństwo zdarzenia i poziom negatywnych skutków), każdy przetwarzający dane (administrator i podmiot przetwarzający) wdraża takie środki bezpieczeństwa, aby zapewniły stopień bezpieczeństwa odpowiedni do tego ryzyka.

Jak ustalono w art. 32 ust. 2 RODO, oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Ważne

Oceniając stopień bezpieczeństwa, trzeba jednocześnie ocenić ryzyko dla praw i wolności danych osób fizycznych, które może wynikać z niechcianych zdarzeń, takich jak:

1) przypadkowe lub niezgodne z prawem zniszczenie, utrata, modyfikacja danych,
2) nieuprawione ujawnienie danych,
3) nieuprawiony dostęp do danych (niezależnie od tego, czy są one przesyłane, przechowywane, czy w inny sposób przetwarzane).

Motyw 83 RODO dostarcza dodatkowych wyjaśnień. Zgodnie z nim w celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z RODO administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki – takie jak szyfrowanie – minimalizujące to ryzyko. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność, oraz uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie. Oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.

W tym świetle warto zauważyć, że art. 25 ust. 1 RODO nakazuje, aby niezbędne zabezpieczenia były włączane już na etapie projektowania przetwarzania danych osobowych, zgodnie z zasadą, że lepiej zapobiegać niż leczyć. Stosownie do tego przepisu, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

W powyższych regulacjach zwraca uwagę użycie określenia „odpowiednie" (odpowiednie środki bezpieczeństwa, środki techniczne i organizacyjne, odpowiedni stopień/poziom bezpieczeństwa). Jeżeli coś jest odpowiednie, to jest dopasowane do sytuacji (mówimy przecież o ubiorze odpowiednim do okazji, tzw. dress codzie, czy o odpowiedniej dawce leku, uwzględniającej np. wiek pacjenta, jego wagę lub stan zdrowia). Obowiązek wyboru odpowiednich zabezpieczeń spoczywa zatem na firmie (administratorze danych lub podmiocie przetwarzającym) – **to przedsiębiorca musi ocenić, czy one są adekwatne i pasujące do procesów przetwarzania danych oraz oszacowanego ryzyka**. Przepisy RODO nie narzucają żadnych rozwiązań technicznych i organizacyjnych – są pod tym względem całkowicie neutralne. Z jednej strony, to bardzo dobrze, bo dają one organizacjom większą swobodę w doborze rozwiązań, ale z drugiej strony, mniej doświadczone podmioty mogą nie wiedzieć, jak podejść do zabezpieczenia systemów, jeśli nie zostaną w pewnym sensie poprowadzone za rękę.

Przy doborze środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa danym osobowym przepisy nakazują uwzględniać „stan wiedzy", który powinno się oceniać z uwzględnieniem warunków rynkowych, w szczególności dostępności i akceptowalności rynkowej danego rozwiązania technicznego. Wskazówek w tym przedmiocie dostarczają obowiązujące standardy i normy, w szczególności normy ISO, które ulegają również ciągłym przeglądom i zmianom warunkowanym postępem technologicznym[1]. W dużym uproszczeniu można powiedzieć, że stosowane zabezpieczenia muszą być w miarę aktualne, nowoczesne (współczesne) i nie mogą być przestarzałe.

Trzeba pamiętać, że w art. 23 RODO wprowadzono zasadę uwzględniania ochrony danych w fazie projektowania (ang. *data protection by design*)[2]. Usługi społeczeństwa informacyjnego (i nie tylko) powinny być tak budowane, aby w przypadku możliwości wielu ich konfiguracji podstawowym stanem było takie ustawienie, które najpełniej gwarantuje użytkownikom poszanowanie ich prywatności. System przetwarzania danych osobowych powinien być zatem tak projektowany – i to jeszcze przed rozpoczęciem zbierania danych – aby administrator mógł realizować swoje interesy, a jednocześnie prawa jednostek były jak najbardziej chronione.

Ważne

Podczas planowania, a później stosowania zabezpieczeń danych osobowych należy, z jednej strony, uwzględniać to, jakie rozwiązania są obecnie dostępne, jaki jest ich koszt i jakie wykształciły się dobre praktyki ich stosowania, a z drugiej – brać pod uwagę ryzyko dla praw i wolności osób w związku z przetwarzaniem ich danych.

1 Zob. https://uodo.gov.pl/decyzje/ZSPR.421.2.2019 (dostęp: 4.10.2019 r.).

2 Koncepcja „prywatności przez projektowanie" została sformułowana w 2009 r. przez *A. Cavoukian* (kanadyjską IOD) – RODO zaadaptowało ten racjonalny model. Zob. tejże, Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices Information & Privacy Commissioner Ontario, Toronto 2011, https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf (dostęp: 21.6.2019 r.). Więcej o wbudowanej ochronie danych zob. *L. Kępa*, Ochrona danych osobowych..., s. 30.

1.3. Monitorowanie i wykrywanie naruszeń

W RODO wskazano, że należy stosować rozwiązania pozwalające na jak najszybsze wykrywanie wszystkich nieprawidłowych sytuacji, określanych jako „naruszenia ochrony danych osobowych". Zgodnie z art. 4 pkt 12 RODO przez naruszenie ochrony danych osobowych rozumie się naruszenie bezpieczeństwa, prowadzące do:

1) przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania,
2) nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Motyw 87 RODO nakazuje upewnić się, czy wdrożono wszelkie odpowiednie techniczne środki ochrony i wszelkie odpowiednie środki organizacyjne, by od razu stwierdzić naruszenie ochrony danych osobowych i szybko poinformować organ nadzorczy i osobę, której dane dotyczą. Trzeba odnotować, że motywy nie stanowią wymagań, a raczej wskazówki pozwalające interpretować akt prawa. W swoim zamierzeniu mają zawierać uzasadnienie przepisów części normatywnej (artykułów)[3]. Przypomnę jeszcze raz, że w RODO nie proponuje się i nie nakazuje żadnych konkretnych rozwiązań, bo akt ten z założenia ma mieć charakter ponadczasowy i być odporny na zmiany w technologii. Zatem RODO bezpośrednio nie obliguje do wdrażania rozwiązań umożliwiających wykrywanie naruszeń. Jest to raczej nakaz domniemywany z art. 32 w zw. z motywem 87 RODO, który jest uzasadnieniem przepisu.

Zastosowane rozwiązania w zakresie bezpieczeństwa mają chronić dane, a jednocześnie umożliwiać sprawne wykrywanie sytuacji, gdy ta ochrona zostanie naruszona. Szybkie stwierdzanie naruszeń jest niezbędne, aby można było o nich zawiadomić, w zależności od okoliczności, organ nadzorczy lub organ oraz osoby, których dane dotyczą. Zgodnie z art. 33 ust. 1 RODO w przypadku naruszenia ochrony danych osobowych administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Zgłoszenie musi opisywać m.in. charakter naruszenia, jego konsekwencje i proponowane albo podjęte środki w celu zaradzenia naruszeniom w przyszłości. Należy prowadzić dokumentację wszelkich naruszeń ochrony danych osobowych. Stosownie do art. 33 ust. 5 RODO administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania tego obowiązku.

W niektórych przypadkach należy zawiadomić również osoby, których dane osobowe się przetwarza. Należy to zrobić, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (art. 34 ust. 1 RODO), tj. wtedy gdy zdarzenie może mieć przykre, negatywne konsekwencje dla osób, których dane dotyczą. Celem zawiadamiania jest to, aby osoby dotknięte zdarzeniem

[3] Zob. Unia Europejska, Międzyinstytucjonalny przewodnik redakcyjny, http://publications.europa.eu/code/pl/pl-120200.htm (dostęp: 21.6.2019 r.).

miały wiedzę o tym, co się stało i jakie kroki poczyniła firma, aby zminimalizować skutki naruszenia, i dzięki temu mogły na nie odpowiednio zareagować.

1.4. Stosowanie zabezpieczeń przez podmiot przetwarzający

1.4.1. Powierzenie przetwarzania danych

Powierzenie przetwarzania danych osobowych jest bardzo ważnym zagadnieniem dla przedsiębiorcy. Podmiot, któremu powierza się przetwarzanie danych osobowych (np. w celu wysłania wyciągów bankowych), określany jest w RODO jako podmiot przetwarzający. Podmiot ten nie może decydować o celu przetwarzania danych – jego „władza" nad danymi osobowymi ograniczona jest do tego, na co zleceniodawca zezwoli mu w umowie. Można by powiedzieć, że powierzenie jest odpowiednikiem udzielania pełnomocnictwa – nie udziela się go przypadkowym osobom.

Przepisy wskazują, że zleceniobiorca przetwarzający dane osobowe (podmiot przetwarzający) musi stosować odpowiednie zabezpieczenia. Wynika to bezpośrednio z art. 32 ust. 1 RODO, zgodnie z którym administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Widać wyraźnie, że zleceniobiorca (podmiot przetwarzający) jest zobowiązany chronić dane osobowe dokładnie na takich samych zasadach jak administrator. Obowiązek zabezpieczania danych powinien być zapisany w umowie zawieranej z takim podmiotem. Przepis art. 28 ust. 3 RODO jasno ustala, że przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora.

1.4.2. Zaufani dostawcy i zleceniobiorcy

Przetwarzania nie można zlecić jakiemukolwiek podmiotowi. W myśl art. 28 ust. 1 RODO można korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Te gwarancje oznaczają, że:

1) podmiot będzie miał wolę podpisać umowę w formie pisemnej (co nakazuje art. 28 ust. 9 RODO), która zawiera wszystkie elementy wymagane prawem, opisane w art. 28 RODO;
2) podmiot dostarczy administratorowi dodatkowe informacje, które pozwolą mu się upewnić, że przetwarzanie przez niego będzie spełniało wymagania RODO, a tym samym chroniło prawa osób, a co najmniej ich nie naruszało;
3) umowa będzie określała:
   a) przedmiot, charakter i cel przetwarzania (w jakim celu zawarta jest umowa, o jakie zlecenie chodzi),
   b) czas przetwarzania (na jak długo umowa została zawarta),
   c) rodzaj danych osobowych i kategorie osób, których dane dotyczą,
   d) obowiązki i prawa administratora.

W szczególności w umowie powinny znaleźć się zapisy z art. 28 ust. 3 RODO. Stosownie do nich zleceniobiorca:

1) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy (wydaje się, że wystarczy, aby podobnie jak administrator podmiot przetwarzający zapoznał pracujące u niego osoby z przepisami o ochronie danych osobowych i zobowiązał do ich stosowania – wówczas zachowanie tajemnicy będzie częścią tych zobowiązań);
2) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w art. 28 ust. 2 i 4 RODO (powierza dalej przetwarzanie, tj. korzysta z podwykonawców, tylko na podstawie zgody administratora, a umowy powierzenia spełniają wszystkie wymagania RODO);
3) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO (zabezpieczenie danych, wykrywanie i informowanie o naruszeniach, zawiadomienia osób, pomoc przy wykonywaniu oceny skutków dla ochrony danych);
4) 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;
5) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich (z tego wynika obowiązek audytów i inspekcji podmiotów przetwarzających);
6) podejmuje wszelkie środki wymagane na mocy art. 32 RODO (zabezpiecza dane odpowiednio do poziomu ryzyka dla praw i wolności osób; oznacza to, że identyfikacja i ocena ryzyka w związku z przyjęciem zlecenia jest obowiązkiem zleceniobiorcy, chyba że zleceniodawca, tj. administrator danych, zdecyduje się podzielić wykonaną analizą).

1.4.3. Podpowierzenie przetwarzania danych

Obowiązek odpowiedniego zabezpieczania danych osobowych to nie jedyne wymaganie, jakie przepisy RODO stawiają przed zleceniobiorcami czy dostawcami przetwarzającymi dane osobowe w imieniu organizacji (administratora danych). Przed wyborem zleceniobiorcy należy ustalić, czy korzysta on z usług podwykonawców, i zobowiązać go co najmniej do informowania o tym, komu dalej powierza przetwarzanie danych osobowych. Zgodnie z art. 28 ust. 2 RODO podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian. Jeśli więc podmiot przetwarzający korzysta z podwykonawców, to oni także muszą stosować odpowiednie zabezpieczenia.

Przykład

W obszarze cyberbezpieczeństwa, a nawet ogólnie – w obszarze IT, bardzo często pojawiają się wątpliwości, czy określona usługa stanowi „przetwarzanie w imieniu". Dobrym przykładem są testy penetracyjne. Jest to badanie systemów informatycznych przez zespół ludzi, co polega na penetrowaniu rozmaitych zakamarków aplikacji i rozwiązań IT w poszukiwaniu słabości i podatności, które mógłby wykorzystać potencjalny atakujący. Najczęściej testuje się środowiska testowe, czyli takie, w których nie ma żadnych danych osobowych, rzadziej – także środowiska produkcyjne lub takie, które zawierają dane osobowe. Celem umowy ze zleceniobiorcą jest wykonanie testów, a nie przetwarzanie danych osobowych, dlatego rzadko zawiera się umowy powierzenia przetwarzania, wymagane przez RODO. Przeważnie zawierana jest zwykła umowa na wykonanie usługi. Dodatkowo – gdy w związku ze zleceniem istnieje ryzyko, że osoba może uzyskać dostęp do danych osobowych (chociaż nie jest to przedmiotem zlecenia) – powinno zawrzeć się umowę o zachowaniu informacji w poufności.

1.5. Środki minimalizujące ryzyko: szyfrowanie, pseudonimizacja i anonimizacja

Szyfrowanie to w dużym uproszczeniu metoda zapisu jawnej treści, by stała się ona nieczytelna dla osób trzecich, a możliwa do odczytania tylko przez tych, którzy mają odpowiedni klucz i wiedzą, jak to zrobić. Szyfrowanie pojawia się w motywie 83 RODO – jest wymienione jako przykład środka minimalizującego ryzyko. W art. 32 ust. 1 lit. a RODO szyfrowanie wskazano jako środek techniczny do zapewnienia odpowiedniego stopnia bezpieczeństwa. Pojawia się ono także w art. 34 ust. 3 lit. a RODO, nakazującym zawiadamiać osoby, których dane dotyczą, o naruszeniu bezpieczeństwa, chyba że zastosowano np. szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.

W art. 32 ust. 1 lit. a RODO jako przykładowy środek techniczny do zapewnienia odpowiedniego stopnia bezpieczeństwa wskazano również pseudonimizację. Zgodnie z art. 4 pkt 5 RODO jest to przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Definicję tę można uprościć: jest to zmiana danych, które identyfikują osobę, na tzw. alias (nick, identyfikator, token) – takie wyjaśnienie pojęcia pseudonimizacji zaprezentowano w normie ISO/IEC 29100 (zob. pkt 5.1.2. niniejszego rozdziału). Dane, które poddano pseudonimizacji, określa się jako dane spseudonimizowane (lub dane pseudonimowe). Zabieg pseudonimizacji stosuje się od dość dawna w szkolnictwie wyższym: przy publikowaniu ocen z egzaminów zamiast imienia i nazwiska podaje się numer indeksu.

Ważne

Warto zauważyć, że RODO nie nakazuje w żadnym konkretnym przypadku stosować szyfrowania ani pseudonimizacji. Podaje je raczej jako przykład możliwego do zastosowania środka zabezpie-

czającego dane. Uważam jednak, że skoro są one wyszczególnione w przepisach, to należy je brać pod uwagę i traktować jako środki specjalne.

Natomiast anonimizacja, chociaż wydaje się podobna do pseudonimizacji, różni się od niej znacząco tym, że jest nieodwracalna. Dane identyfikujące osobę mogą zostać całkowicie usunięte lub zmodyfikowane tak, że nie da się zidentyfikować osoby, której dotyczą (np. zamienione na pseudonim lub wybrany identyfikator). Do anonimizacji odnosi się motyw 26 RODO. Wskazuje on, że zasady ochrony danych nie powinny mieć zastosowania do informacji anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować. W świetle tego anonimizacja jest uznawana za odpowiednik usuwania danych – skutek w obu przypadkach jest ten sam. Warto zatem pamiętać o tym zabiegu, gdyż RODO nakazuje usuwać dane osobowe, gdy skończą się wszystkie cele przetwarzania.

1.6. Środki i polityki bezpieczeństwa

W art. 24 ust. 1 i 2 RODO określono obowiązki administratora związane z zapewnieniem zgodności z przepisami o ochronie danych osobowych. Stosownie do art. 24 ust. 1 RODO, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

Ważne

Środki techniczne i organizacyjne trzeba wdrażać w taki sposób, aby zapewnić zgodność z przepisami i aby można było tę zgodność wykazać. Dokumentacja zabezpieczeń będzie stanowić jeden ze sposobów pozwalających wykazać zapewnienie zgodności z przepisami. W razie potrzeby należy poddawać te środki przeglądom i uaktualnieniom – bez dokumentacji to zadanie może okazać się dość trudne.

Przepis art. 24 ust. 2 RODO wskazuje, że w pewnych sytuacjach – jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania – administrator może wdrożyć odpowiednie polityki ochrony danych. Pojęcie polityki ochrony danych nie zostało zdefiniowane w RODO, dlatego może być różnie interpretowane: „Przez to pojęcie rozumieć można strategię ochrony danych, a więc przemyślany plan działań w dziedzinie ochrony danych, mający umożliwić osiągnięcie celu, jakim jest skuteczna ochrona danych. W tym rozumieniu polityka ochrony danych oznacza ogólny dokument wskazujący podstawowe założenia i cele, natomiast nie jest to akt normujący szczegółowe zagadnienia związane z technicznymi i organizacyjnymi środkami zabezpieczenia danych”[4].

[4] *P. Fajgielski*, Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018, s. 320.

Wyraz „polityka" (tłumaczenie ang. *policy*) oznacza zasady, sposób działania (przykładowo ang. *company policy* – zasady firmowe). Organizacja – o ile jest to proporcjonalne w stosunku do czynności przetwarzania – może wdrożyć polityki ochrony danych, a zatem nie jest to bezwzględny obowiązek. Decyzję o ich wdrożeniu należy podjąć po dokonaniu oceny, czy jest to odpowiednie z uwagi na czynności przetwarzania, przykładowo na dużą skalę przetwarzania danych. Im większa organizacja i im bardziej skomplikowane są procesy przetwarzania, tym większa potrzeba wdrożenia polityk ochrony danych, które nie tylko dokumentują zasady postępowania, zapewniające zgodność z przepisami, lecz także pełnią funkcję edukacyjną. Warto odnotować, że jeśli organizacja jest zobowiązana stosować przepisy RachunkU, to zgodnie z art. 10 ust. 1 RachunkU powinna posiadać dokumentację opisującą w języku polskim przyjęte przez nią zasady (politykę) rachunkowości, a w szczególności dotyczące systemu służącego ochronie danych i ich zbiorów, w tym dowodów księgowych.

Polityki bezpieczeństwa danych osobowych skupiają się na zapewnieniu bezpieczeństwa informacji. Stanowią one podzbiór polityki ochrony danych osobowych, której celem jest zapewnienie i zarządzanie całościową zgodnością z RODO.

1.7. Rejestr czynności przetwarzania

Rejestr czynności przetwarzania powinny przygotowywać w zasadzie prawie wszystkie organizacje – zarówno administratorzy, jak i podmioty przetwarzające. Przepis art. 30 RODO ustala, że:

1) każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych,
2) każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania.

Powyższe rozróżnienie rejestrów może wprowadzać małe zamieszanie, chodzi jednak, co do zasady, o takie same rejestry, pozwalające każdemu, kto przetwarza dane osobowe, zorientować się, czym rozporządza (a organowi nadzorczemu – czy przetwarzanie odbywa się zgodnie z przepisami). Rejestr czynności (lub kategorii) przetwarzania to uproszczony opis tego:

1) kto dane przetwarza i w jakiej roli (czy jest administratorem, czy procesorem),
2) kto jest administratorem danych,
3) jakie dane są przetwarzane i w jakim celu,
4) komu dane są udostępniane,
5) czy dane są przekazywane do państw trzecich, a jeśli tak, to do jakich,
6) kiedy przewiduje się usuwać dane,
7) jak ogólnie zabezpiecza się dane (np. wybrany poziom zabezpieczeń).

Przedsiębiorca przede wszystkim powinien wiedzieć, jakie dane przetwarza i w jakim celu. Niemniej aby móc sprawnie zarządzać bezpieczeństwem danych osobowych,

warto w rejestrze podać kilka dodatkowych informacji (niewymaganych przez przepisy RODO), np.:

1) przepływ informacji – gdzie dane znajdują się w określonym czasie ich życia (rodzaje nośników, miejsca, osoby),
2) orientacyjna ilość danych,
3) klasyfikacja danych ze względu na ryzyko dla praw i wolności osób,
4) wynik oceny ryzyka (obecny poziom ryzyka), ewentualnie wynik wykonanej oceny skutków dla ochrony danych.

Administrator powinien wskazać ponadto:

1) kto w jego imieniu przetwarza dane, których jest on administratorem (komu zlecono przetwarzanie), oraz informacje o dalszych powierzeniach (podwykonawcach),
2) podstawy prawne przetwarzania (tzw. przesłanki legalności),
3) sposób realizacji praw osób.

Z perspektywy cyberbezpieczeństwa istotne będzie dostarczenie osobie, która prowadzi rejestry (najczęściej jest to IOD), informacji o tym, jak dane osobowe są zabezpieczone w systemach informatycznych. Jeśli w organizacji jest przygotowana polityka bezpieczeństwa informacji uwzględniająca ten obszar, to w takich rejestrach można tylko się do niej odnieść. Nieracjonalne byłoby ponowne opisywanie tego samego, chociażby dlatego że przy zmianie zasad (polityk) trzeba będzie zmienić rejestry.

W mojej ocenie rejestr czynności przetwarzania powinien prowadzić każdy – niezależnie od tego, czy prawo nakłada na niego taki obowiązek. Nakład pracy jest nieduży: najczęściej jest to mniej więcej jedna strona dokumentacji na jeden proces (w przeciętnej organizacji procesów będzie raczej kilka, w większej pewnie kilkanaście). Warto z rejestrów uczynić swojego rodzaju **karty procesów przetwarzania, dzięki którym organizacja będzie mogła zebrać wszystkie niezbędne informacje o przetwarzaniu danych osobowych w jednym miejscu**.

Ważne

Prowadzenie rejestrów czynności przetwarzania stanowi zapewnienie stosowania zasady rozliczalności wskazanej w art. 5 ust. 2 RODO. Chociaż RODO nie wskazuje tego wprost, z decyzji polskiego organu nadzorczego wynika, że rejestr czynności przetwarzania powinno się przechowywać także po zakończeniu przetwarzania, aby można było wykazać, że dane osobowe były przetwarzane zgodnie z prawem, a także dlatego, że wymóg dotyczący stosowania zasady rozliczalności dotyczy wszystkich etapów przetwarzania, w konsekwencji także etapu usuwania danych[5].

1.8. Ocena skutków dla ochrony danych

Przepis art. 35 RODO jest poświęcony ocenie skutków dla ochrony danych. Proces ten można wytłumaczyć na przykładzie usługi przewozu osób autobusem. Odpowiednikiem oceny skutków byłaby tu ocena stanu autobusu, kwalifikacji i stanu zdrowia kierowcy,

[5] W decyzji ZSPR.421.2.2019 z 10.9.2019 r. Prezes Urzędu Ochrony Danych Osobowych podkreśla, że pomimo zamknięcia procesu przetwarzania administrator musi zawsze być w stanie wykazać, że dane osobowe są przetwarzane zgodnie z prawem – https://uodo.gov.pl/decyzje/ZSPR.421.2.2019 (dostęp: 1.10.2019 r.).

tras przejazdu, liczby pasażerów, rodzaju ubezpieczenia itp. Jeśli ocena wykaże, że jest spore ryzyko dla życia i zdrowia pasażerów (autobus jest stary, jego stan techniczny jest przeciętny, kierowca ma problemy ze zdrowiem, zbyt długo pracuje), to trzeba to ryzyko zmniejszyć przed rozpoczęciem świadczenia usługi (naprawić lub wymienić pojazd, zatrudnić dodatkowego kierowcę).

Ocena skutków dla ochrony danych stanowi źródło informacji o zagrożeniach oraz ich potencjalnych konsekwencjach, co jest kluczowe dla procesu zarządzania ryzykiem, a przede wszystkim – identyfikacji ryzyka, ponieważ pozwala dobrać odpowiednie zabezpieczenia. Według mnie **ocena skutków dla ochrony danych stanowi kluczowy element projektowania systemu przetwarzania danych osobowych**[6]. Również UODO wielokrotnie podkreślał, że administrator dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych przed rozpoczęciem przetwarzania[7]. Zgodnie z opinią Grupy Roboczej Art. 29 ocena skutków w zakresie ochrony danych „oznacza uporządkowany proces oceny ewentualnych skutków zagrożeń, w przypadku gdy operacje przetwarzania mogą powodować określone zagrożenia dla praw i wolności osób, których dotyczą dane, ze względu na ich charakter, zakres lub cel”[8].

Podczas planowania nowego procesu przetwarzania danych należy sprawdzić:

1) czy znajduje się on w wykazie rodzajów operacji przetwarzania wymagających oceny skutków – taki wykaz został opublikowany w komunikacie Prezesa Urzędu Ochrony Danych Osobowych z 17.6.2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M.P. poz. 666);
2) czy jest to zautomatyzowana ocena czynników osobowych, w tym profilowanie (art. 35 ust. 3 lit. a RODO);
3) czy jest to przetwarzanie na dużą skalę danych wrażliwych lub danych dotyczących wyroków skazujących lub czynów zabronionych (art. 35 ust. 3 lit. b RODO);
4) czy chodzi o systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie (art. 35 ust. 3 lit. c RODO).

Środkiem pomocniczym pozwalającym podjąć decyzję, czy należy wykonywać ocenę skutków dla ochrony danych, może być też decyzja Europejskiego Inspektora Ochrony Danych z 16.7.2019 r. w sprawie wykazu ocen skutków dla ochrony danych wydana na podstawie art. 39 ust. 4 i 5 rozporządzenia 2018/1725[9]. W załączniku do decyzji znajduje się tabela z wymienionymi kryteriami oceny, czy dane przetwarzanie może powodować wysokie ryzyko dla praw i wolności osób fizycznych. Podawane przykłady dzielą się na te, które mogą powodować to ryzyko i te, które tego ryzyka nie powodują, np. użycie

6 Szerzej o ocenie skutków zob. *L. Kępa*, Ochrona danych osobowych..., s. 287–307.

7 Przykładowo zob. Urząd Ochrony Danych Osobowych, Jak rozumieć podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku. Część 1, maj 2018, https://uodo.gov.pl/pl/383/208 (dostęp: 22.7.2019 r.), s. 15.

8 Grupa Robocza Art. 29, Opinia 04/2013 w sprawie szablonu oceny skutków w zakresie ochrony danych na potrzeby inteligentnych sieci i inteligentnych systemów pomiarowych, opracowanego przez grupę ekspertów nr 2 w ramach grupy zadaniowej Komisji ds. inteligentnych sieci (00678/13/PL, WP205), przyjęta 22.4.2013 r., https://archiwum.giodo.gov.pl/pl/1520167/6567 (dostęp: 22.7.2019 r.), s. 7.

9 Zob. https://edps.europa.eu/sites/edp/files/publication/19-07-16_edps_dpia_list_en.pdf (dostęp: 4.10.2019 r.).

nowych technologii takich jak uczenie maszynowe, samochody komunikujące się ze sobą (ang. *connected cars*), zautomatyzowane prześwietlanie kandydatów do pracy mogą powodować ryzyko, ale biometria odcisku palca w celu kontroli dostępu już nie.

Ważne

Najlepiej i najbezpieczniej jest dokonać oceny skutków dla każdego planowanego procesu, a nie tylko wówczas, gdy spełnione są warunki określone przepisami. Da to przedsiębiorcy pewność, że niczego nie przeoczył oraz wziął pod uwagę wszystko, co potrzebne, i ma na to dowody. Pamiętajmy, że sercem całego systemu ochrony danych osobowych jest zarządzanie ryzykiem dla praw i wolności osób fizycznych, w tym głównie tych, których dane dotyczą – jest to naturalna konsekwencja celu RODO, opisanego w art. 1 ust. 2 RODO.

W myśl art. 35 ust. 7 RODO ocena skutków powinna zawierać:

1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym – gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora,
2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,
3) ocenę ryzyka naruszenia praw i wolności osób fizycznych (dowolnych osób – także tych, których dane nie są, a nawet nie będą przetwarzane),
4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

Ocena skutków dla ochrony danych z punktu widzenia zabezpieczeń danych osobowych ma szczególne znaczenie. Powiedziałbym nawet, że stanowi ona początek całego systemu ochrony danych. Nawet jeśli przepisy RODO nie nakazują wykonania oceny skutków, zalecam jej przeprowadzenie, gdyż **potencjalne skutki przetwarzania dla praw i wolności osób będą decydować o tym, jaki jest poziom ryzyka, a w konsekwencji – jaki poziom zabezpieczeń wybrać**.

1.9. Nadzór nad bezpieczeństwem danych

Przepisy art. 37–39 RODO dotyczą inspektora ochrony danych osobowych (ang. *data protection officer*). Jego zadania w związku z bezpieczeństwem danych osobowych opisuje art. 39 RODO. Należą do nich m.in:

1) informowanie zainteresowanych stron (kierownictwa, pracowników) o obowiązkach wynikających z przepisów o ochronie danych osobowych[10],
2) doradzanie w sprawach ochrony danych osobowych,
3) monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych,

[10] Przepisy RODO odnoszą się do obowiązków spoczywających „na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych" – chodzi więc o dowolne regulacje dotyczące ochrony danych, a nie tylko o samo RODO.

4) działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
5) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO.

Jednym z obowiązków IOD jest monitorowanie przestrzegania przepisów o ochronie danych osobowych. Ponieważ zabezpieczenia danych osobowych stanowią wymagania RODO, inspektor ochrony danych jest zobowiązany monitorować także, czy i jak są one realizowane. Nie oznacza to, że on ma dobierać zabezpieczenia, ale powinien ocenić, czy metody wyboru zabezpieczeń są odpowiednie. Niezależnie od tego byłoby dobrze, aby IOD rozumiał problem bezpieczeństwa i znał chociaż podstawowe kwestie dotyczące cyberbezpieczeństwa. Jeśli organizacja go powoła, powinien być on ważnym partnerem do dyskusji i konsultowania wszelkich zabezpieczeń. Analiza zapisów art. 39 RODO pozwala na wysnucie wniosku, że **IOD ma być pojedynczym miejscem, w którym każdy może uzyskać wyczerpujące informacje na temat wymagań i zgodności przetwarzania z przepisami o ochronie danych, w tym także tego jak dane osobowe są zabezpieczone**.

Inspektor ochrony danych powinien zostać powoływany wówczas, gdy:
1) dane osobowe przetwarza organ lub podmiot publiczny (wykaz takich organów znajduje się w OchrDanychU),
2) 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,
3) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych.

Jeśli jednak administrator nie wyznaczył IOD, gdyż nie był do tego zobowiązany, powinien zapewnić realizację zadań, o których mowa w art. 39 RODO, w inny sposób, przez inne osoby. Jak wskazuje *P. Fajgielski*: „w niewielkich strukturach organizacyjnych może oznaczać to konieczność samodzielnego nadzorowania przestrzegania przepisów o ochronie danych osobowych przez administratora (np. osobę fizyczną prowadzącą działalność gospodarczą)”[11].

2. Wymagania wynikające z Kodeksu pracy

Kodeks pracy dotyczy każdego pracodawcy. Choć może wydać się to zaskakujące, reguluje on również niektóre kwestie dotyczące bezpieczeństwa danych.

[11] *P. Fajgielski*, Ogólne rozporządzenie o ochronie..., s. 429.

2.1. Monitoring w miejscu pracy

Wielu pracodawców stosuje w swoich systemach informatycznych rozmaite formy monitorowania. Przykładowo monitoring stanowi skanowanie stron internetowych, które są przeglądane przez pracowników, w celu wykrycia zagrożeń, korzystanie z systemów zapobiegających wyciekom danych (DLP – ang. *data loss prevention*) w celu ochrony firmowych informacji przed kradzieżą i wyciekiem czy zarządzanie smartfonami przez centralny system zarządzania urządzeniami mobilnymi (MDM – ang. *mobile device management* oraz EMM – ang. *enterprise mobile management*).

Przepis art. 22^2 KP reguluje rejestrowanie obrazu przez pracodawcę na terenie lub wokół zakładu pracy (chodzi o CCTV – telewizję przemysłową, ang. *closed circuit television*). Obraz można rejestrować, jeśli jest to niezbędne w celach bezpieczeństwa lub ochrony mienia, lub kontroli produkcji, lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.

Z kolei art. 22^3 KP zezwala na monitorowanie (kontrolę) służbowej poczty elektronicznej, jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Należy pamiętać, że monitoring poczty elektronicznej nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika. Te same zasady stosuje się do innych form monitoringu – co oznacza, że art. 22^3 KP odnosi się do wszelkich informatycznych form monitorowania.

2.2. Upoważnienia do przetwarzania danych

Upoważnienie do przetwarzania danych stanowi uprawnienie do przetwarzania określonych danych osobowych, nadane pracownikowi przez administratora danych. Jest to nic innego jak udzielenie swojego rodzaju zgody przez przedsiębiorcę na przetwarzanie. Forma upoważnienia może być dowolna: może zostać nadane przez wysłanie do pracownika służbowego e-maila lub po wypełnieniu przez niego wniosku (czy ich zestawu) o nadanie uprawnień (dostępu) w systemach informatycznych. Upoważnienie może być również zawarte w zakresie obowiązków pracowniczych. Warto jednak wiedzieć, że niektóre rodzaje przetwarzania wymagają upoważnień w formie pisemnej.

Osoby mające dostęp do danych pracowniczych tzw. szczególnych kategorii (danych wrażliwych) muszą posiadać pisemne upoważnienia do ich przetwarzania, wydane przez pracodawcę. Zgodnie z art. 22^{1b} § 3 KP osoby dopuszczone do przetwarzania takich danych są obowiązane do zachowania ich w tajemnicy. Niekiedy dostęp do wyjątkowo ważnych miejsc lub systemów może wymagać kontroli biometrycznej jako dodatkowego środka zabezpieczenia. Przepis art. 22^{1b} § 2 KP pozwala na przetwarzanie danych biometrycznych pracownika wtedy, gdy podanie takich danych 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.