OCHRONA DANYCH OSOBOWYCH

Ocena ryzyka i skutków
Metody i praktyczne przykłady

redakcja Mirosław Gumularz, Tomasz Izydorczyk

Marcin Błoński, Mirosław Gumularz, Tomasz Izydorczyk
Maciej Kołodziej, Beata Konieczna-Drzewiecka
Maciej Otmianowski, Monika Sobczyk, Mariola Więckowska

PRAWO W PRAKTYCE

Wolters Kluwer

OCHRONA DANYCH OSOBOWYCH

Ocena ryzyka i skutków
Metody i praktyczne przykłady

redakcja Mirosław Gumularz, Tomasz Izydorczyk

Marcin Błoński, Mirosław Gumularz, Tomasz Izydorczyk
Maciej Kołodziej, Beata Konieczna-Drzewiecka
Maciej Otmianowski, Monika Sobczyk, Mariola Więckowska

PRAWO W PRAKTYCE

Wolters Kluwer

WARSZAWA 2021

Stan prawny na 1 lutego 2021 r.

Recenzent
Dr hab. Agnieszka Grzelak, prof. ALK

Wydawca
Monika Pawłowska

Redaktor prowadzący
Małgorzata Jarecka

Opracowanie redakcyjne
JustLuk

Projekt okładek serii
Wojtek Kwiecień-Janikowski, Przemek Dębowski

Poszczególne części napisali:
Marcin Błoński i Maciej Otmianowski – praktyczny przykład nr 14
Mirosław Gumularz – rozdział 5, praktyczny przykład nr 1
Mirosław Gumularz, Tomasz Izydorczyk – rozdziały 1– 4, rozdział 7
Tomasz Izydorczyk – rozdział 6, praktyczne przykłady nr. 2–8
Beata Konieczna-Drzewiecka – praktyczne przykłady nr. 12 i 13
Maciej Kołodziej – praktyczny przykład nr 9
Monika Sobczyk – praktyczny przykład nr 10
Mariola Więckowska – praktyczny przykład nr 11

ISBN 978-83-8223-533-3 *ISBN PDF-a: 978-83-8223-978-2*

Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: ksiazki@wolterskluwer.pl

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

WYKAZ SKRÓTÓW

1. Akty prawne

k.c.	– ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2020 r. poz. 1740 ze zm.)
k.p.	– ustawa z 26.06.1974 r. – Kodeks pracy (Dz.U. z 2020 r. poz. 1320 ze zm.)
k.p.a.	– ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2020 r. poz. 256 ze zm.)
pr. tel.	– ustawa z 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. z 2019 r. poz. 2460 ze zm.)
RODO	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, s. 1, ze zm.)
u.o.d.o.	– ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781 ze zm.)
u.p.p.	– ustawa z 6.11.2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2020 r. poz. 849)
ustawa covidowa	– ustawa z 2.03.2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz.U. z 2020 r. poz. 1842 ze zm.)
u.ś.u.d.e.	– ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344 ze zm.)

2. Inne

AEPD	– Agencia Española de Protección de Datos
CNIL	– Commission nationale de l'informatique et des libertés
EIOD	– Europejski Inspektor Ochrony Danych Osobowych
ENISA	– Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji

EROD	– Europejska Rada Ochrony Danych
GIODO	– Generalny Inspektor Ochrony Danych Osobowych
GR29	– Grupa Robocza art. 29
ICO	– Information Commissioner's Office
IZSI	– instrukcja zarządzania systemami informatycznymi
LIA	– legitimate interests assessment
M. Praw.	– Monitor Prawniczy
NSA	– Naczelny Sąd Administracyjny
OSOD	– ocena skutków dla ochrony danych
RCP	– rejestr czynności przetwarzania
SLA	– Service Level Agreement
UODO	– Urząd Ochrony Danych Osobowych
WHO	– Światowa Organizacja Zdrowia
WSA	– wojewódzki sąd administracyjny

Część 1

POJĘCIE RYZYKA NARUSZENIA PRAW LUB WOLNOŚCI

Rozdział 1

WSTĘP – POJĘCIE RYZYKA NARUSZENIA PRAW LUB WOLNOŚCI

1. Przypadki oceny ryzyka w RODO – informacje ogólne

Przepisy RODO odwołują się do problemu oceny ryzyka naruszenia praw lub wolności w różnych obszarach (w różnych kontekstach). W związku z tym można wyszczególnić kilka typów oceny ryzyka z uwagi na:

- redakcyjne umiejscowienie przepisu dotyczącego oceny ryzyka, tj. w danym rozdziale lub sekcji RODO;
- wskazanie podmiotu odpowiedzialnego za dokonanie oceny ryzyka (np. administrator lub podmiot przetwarzający);
- rozumienie (ideę) danego ryzyka i jego składowych (np. w zakresie bezpieczeństwa i innych wymogów będzie o tym mowa poniżej);
- funkcję oceny ryzyka w systemie ochrony danych osobowych (np. to, czy w konsekwencji identyfikacji ryzyka należy podjąć określone działanie, np. powiadomić organ nadzorczy o naruszeniu ochrony danych osobowych).

Przepisy dotyczące oceny ryzyka

W związku z powyższym można wskazać następujące przepisy RODO dotyczące oceny ryzyka. W części A zostaną przedstawione przepisy RODO, które wprost odwołują się do pojęcia ryzyka naruszenia praw lub wolności. Natomiast w części B zostaną przedstawione szczególne przypadki oceny ryzyka, które pośrednio wynikają z przepisów RODO.

A. Ogólny wymóg monitorowania ryzyka dla praw lub wolności (art. 24 ust. 1 RODO)

Zgodnie z treścią art. 24 ust. 1 RODO administrator danych ma obowiązek wdrożyć odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać. Środki te muszą być odpowiednie w stosunku do ryzyka naruszenia praw i wolności osób fizycznych w związku przetwarzaniem danych osobowych. Zgodnie z treścią tego przepisu, aby zrealizować ten obowiązek, należy uwzględnić charakter, zakres, kontekst i cele przetwarzania danych osobowych oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze.

Komentarz:

Artykuł 24 ust. 1 RODO dotyczy ogólnego wymogu oceny ryzyka, która ma na celu „dostosowanie" środków (technicznych i organizacyjnych) do poziomu tego ryzyka, tak aby przetwarzanie odbywało się zgodnie z wymogami ochrony danych osobowych (RODO), a jednocześnie żeby administrator danych mógł tę zgodność wykazać.

Na gruncie art. 24 ust. 1 RODO ocena ryzyka służy trzem podstawowym celom:

1) weryfikacji tego, w jaki sposób spełnić wymogi RODO (nie „czy spełnić" wymogi, ale jakimi środkami bądź czy środki są odpowiednie do poziomu ryzyka);
2) weryfikacji tego, jakimi środkami wykazać, że wymogi RODO zostały zrealizowane;
3) pośrednio także weryfikacji samej metodologii (procedury) oceny ryzyka – np. czy sposób prowadzenia oceny ryzyka nie jest sam w sobie źródłem ryzyka naruszenia praw lub wolności osób fizycznych (np. procedura oceny ryzyka zakładająca jej ponawianie raz na 5 lat może być niewystarczająca w przypadku skomplikowanych procesów, tj. może nie być odpowiednia do poziomu ryzyka).

B. Ocena ryzyka w fazie projektowania (art. 25 ust. 1 i 2 RODO)

Administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – ma obowiązek wdrożyć odpowiednie środki techniczne i organizacyjne (np. pseudonimizacja) zaprojektowane w celu skutecznej realizacji zasad ochrony danych (np. minimalizacja danych) oraz nadania przetwarzaniu niezbędnych zabezpieczeń, tak aby spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą (art. 25 ust. 1 RODO).

Rozwinięciem tego wymogu jest domyślna ochrona danych (art. 25 ust. 2 RODO). Zgodnie z art. 25 ust. 2 RODO administrator ma obowiązek wdrożyć „odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te

dane osobowe, które są niezbędne do osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych".

W ramach powyższej oceny ryzyka naruszenia praw lub wolności należy uwzględnić stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze ryzyka.

Komentarz:

Artykuł 25 ust. 1 RODO dotyczy oceny ryzyka w fazie projektowania. Przepis ten kładzie nacisk na początkową fazę planowania przetwarzania danych. Już w tej fazie musi nastąpić ocena ryzyka, która służy weryfikacji, czy planowane środki realizacji wymogów są adekwatne do poziomu ryzyka, jaki może łączyć się z przetwarzaniem danych. Niemniej przepis ten nie ogranicza się wyłącznie do fazy projektowania. Jak wskazuje art. 25 ust. 1 RODO, chodzi o ocenę ryzyka dokonywaną zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania. Można zatem uznać, że komentowany przepis nakłada obowiązek oceny ryzyka wszystkich procesów (i w ramach tych procesów poszczególnych operacji na danych) przetwarzania, zarówno tych planowanych w przyszłości, jak i tych, które realizowane są aktualnie.

Komentowany przepis dotyczy wszystkich kategorii źródeł ryzyka, tj. zagrożeń (zob. szerzej odnośnie do zagrożeń część 1, rozdział 2), które mogą prowadzić do wystąpienia ryzyka naruszenia praw lub wolności. Oznacza to, że dotyczy on zarówno aspektu bezpieczeństwa przetwarzania danych, jak i pozostałych wymogów, tj. ogólnie „prywatności" (np. minimalizacji).

Jak się wskazuje, koncepcja *privacy by design* została opracowana przez Anne Cavoukian, Komisarza ds. Ochrony Danych w Ontario w latach 90. XX w. i zaprezentowana na 31. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności w 2009 r. pt. *Privacy by Design: The Definitive Workshop*. Został on przyjęty na arenie międzynarodowej na 32. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności, która odbyła się w Jerozolimie w 2010 r., wraz z przyjęciem Rezolucji w sprawie poszanowania prywatności od samego początku[1].

[1] AEPD, *A Guide to Privacy by Design*, https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf, s. 5. Jeśli nie wskazano inaczej, data dostępu do stron internetowych powoływanych w pracy to 2.02.2020 r.

W rezolucji tej uznano znaczenie uwzględnienia zasad prywatności w procesie projektowania, obsługi i zarządzania systemami organizacyjnymi w celu osiągnięcia ram integralnej ochrony w zakresie ochrony danych. Zachęcała również do przyjęcia Podstawowych zasad ochrony prywatności w fazie projektowania, zgodnie z definicją Anne Cavoukian, na podstawie następujących zasad:

- proaktywny, nie reaktywny; zapobiegawcze, a nie naprawcze;
- prywatność jako ustawienie domyślne;
- prywatność osadzona w projekcie[2];
- pełna funkcjonalność: suma dodatnia, a nie zero;
- kompleksowe zabezpieczenia: pełna ochrona przez cały okres eksploatacji;
- widoczność i przejrzystość;
- poszanowanie prywatności użytkowników: skupiaj się na użytkowniku.

AEPD wskazuje słusznie, że zasada *privacy by design* to *de facto* całościowe ujęcie (łącznie) dwóch zasad: podejścia opartego na ocenie ryzyka (*risk based aproach*) oraz rozliczalności[3].

AEPD wskazuje następujące elementy *privacy by design* (które można traktować jako ogólne zabezpieczenia systemu ochrony prywatności)[4]:

1) podejście proaktywne, nie reaktywne (zapobiegawcze, a nie naprawcze), na co składa się m.in.: rozwijanie kultury zaangażowania i ciągłego doskonalenia przez wszystkich pracowników, ponieważ polityka nic nie znaczy, dopóki nie zostanie przełożona na konkretne działania napędzane wynikami;
2) prywatność jako ustawienie domyślne, na co składa się m.in. tworzenie barier technologicznych i proceduralnych dla nieuprawnionego łączenia niezależnych źródeł danych;
3) prywatność osadzona w projekcie – w ramach tej zasady prywatność należy traktować jako zasadniczy wymóg w cyklu życia systemów i usług, a także w projektowaniu procesów organizacyjnych;
4) pełna funkcjonalność, m.in. jeżeli proponowane rozwiązania zagrażają prywatności, poszukaj nowych rozwiązań i alternatyw, aby osiągnąć zamierzone funkcje i cele, nie zapominając jednak o tym, że należy odpowiednio zarządzać zagrożeniami dla prywatności użytkownika;
5) kompleksowe zabezpieczenia: pełna ochrona przez cały okres eksploatacji, m.in. bezpieczne i gwarantowane zniszczenie informacji pod koniec ich cyklu życia;
6) przejrzystość – m.in. chociaż nie jest to obowiązkowe dla wszystkich administratorów, upublicznianie lub co najmniej łatwy dostęp dla osób, których dane

[2] AEPD, *A Guide to Privacy…*, s. 5.
[3] AEPD, *A Guide to Privacy…*, s. 6.
[4] AEPD, *A Guide to Privacy…*, s. 6.

dotyczą, wykaz wszystkich operacji przetwarzania przeprowadzanych w organizacji:
   a) udostępnianie tożsamości i danych kontaktowych administratora danych organizacji,
   b) stworzenie dostępnych, prostych i skutecznych mechanizmów komunikacji,
   c) odszkodowania i reklamacje dla podmiotów danych;
7) szanuj prywatność użytkowników – m.in. zapewnienie osobom, których dane dotyczą, dostępu do ich danych oraz szczegółowych informacji o celach przetwarzania i prowadzonej komunikacji.

Natomiast EROD zwraca uwagę na to, że zasada *privacy by default* przede wszystkim dotyczy zasady minimalizacji danych[5].

Należy przyjąć, że poprawna realizacja wymogu wskazanego w art. 25 ust. 1 RODO (*privacy by design*) w połączeniu z wymaganiami art. 25 ust. 2 (*privacy by default*) będzie przejawiała się w szczególności tym, że:

- zakres danych osobowych przetwarzanych w danym procesie przetwarzania będzie minimalny (czyli tylko tyle danych, ile jest niezbędne i minimalne, aby administrator osiągnął zaplanowane przez siebie cele przetwarzania);
- liczba operacji w każdym procesie przetwarzania także będzie ograniczona do minimum pozwalającego na osiągnięcie założonych celów przetwarzania;
- okres przetwarzania danych we wszystkich procesach (tzw. retencja danych) będzie skrócona do absolutnego minimum i w momencie osiągnięcia celu przez administratora dane będą usuwane;
- liczba osób, którym będą udostępnione dane osobowe, będzie ograniczona do niezbędnego minimum; natomiast przypadki, w których dane osobowe są ujawnione bliżej nieokreślonej liczbie osób, będą przeważnie wynikiem działania (interwencji) podmiotów danych, a nie administratora.

Z powyższego wynika, że wymogi postawione administratorom w art. 25 ust. 2 są zbieżne z zasadami ogólnymi przetwarzania określonymi w art. 5 RODO, a przynajmniej ich częścią, stanowią ich uszczegółowienie.

Szczegółowy wykaz środków (zabezpieczeń) realizacji zasad ogólnych – przy uwzględnieniu art. 25 RODO – zostanie omówiony w części 1, w rozdziale 4.

---

[5] EROD, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Adopted on 13 November 2019*, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf, pkt 44. W. Wiewiórowski, zwraca uwagę, że zasada *privacy by default* jest tylko jednym z postulatów szerszej idei *privacy by design*, dotyczy ustawień systemów w fazie podłączania się do niego użytkownika. Zdaniem autora zasada *privacy by design* oznacza, że bierny użytkownik nie staje się ofiarą swojej bierności, a beneficjentem ustawień domyślnych systemu (W.R. Wiewiórowski, *Privacy by design jako paradygmat ochrony prywatności* [w:] *Internet. Prawno-informatyczne problemy sieci, portali i e-usług*, red. G. Szpor, W.R. Wiewiórowski, Warszawa 2012, s. 17.

C. Ocena ryzyka pod kątem obowiązku prowadzenia rejestru czynności (art. 30 ust. 5 RODO)

Stosownie do treści art. 30 ust. 5 RODO obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych oraz rejestru wszystkich kategorii czynności przetwarzania nie dotyczy przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że m.in. „przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą".

Komentarz:

Komentowany przepis dotyczy zarówno administratora danych, jak i podmiotu przetwarzającego. W tym przypadku ocena ryzyka nie ma na celu weryfikacji prawidłowego wdrożenia środków realizujących poszczególne wymogi RODO, a bardziej ustalenie, czy określony wymóg w ogóle należy realizować (wymóg związany z dokumentacją przetwarzania danych). Jeśli w wyniku oceny ryzyka dotyczącej procesów przetwarzania danych osobowych przez administratora lub podmiot przetwarzanych danych okaże się, że nie wiążą się one z ryzykiem naruszenia praw lub wolności podmiotów danych, to obowiązek prowadzenia odpowiedniego rejestru nie będzie miał zastosowania.

Należy zwrócić uwagę, że komentowany przepis nie odwołuje się do określonego poziomu ryzyka naruszenia praw lub wolności, ale zawiera bardzo ogólne określenie „ryzyka naruszenia praw lub wolności". W szczególności nie odwołuje się do pojęcia wysokiego ryzyka. Ogranicza to praktyczne znaczenie tego wyłączenia (obowiązku prowadzenia rejestru czynności lub rejestru kategorii), ponieważ trudno sobie wyobrazić przetwarzanie danych, które w ogóle nie rodzi jakiegokolwiek (nawet niskiego) ryzyka naruszenia praw lub wolności.

D. Ocena ryzyka w ramach oceny środków służących bezpieczeństwu (art. 32 ust. 1 RODO)

Zgodnie z treścią art. 32 ust. 1 RODO administrator i podmiot przetwarzający mają obowiązek wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić odpowiedni stopień bezpieczeństwa przetwarzania danych. W tym kontekście należy uwzględnić 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 zagrożenia.

Artykuł 32 RODO zawiera także przykładowy wykaz środków realizacji wymogu bezpieczeństwa, np. pseudonimizację.

Komentarz:

Celem oceny ryzyka dokonywanej w ramach art. 32 RODO jest zapewnienie, aby zaplanowane lub wdrożone środki służące bezpieczeństwu były odpowiednie do poziomu ryzyka, jaki łączy się z przetwarzaniem danych. Nie chodzi więc o źródła ryzyka (zagrożenia) identyfikowane w ramach wszystkich wymogów ochrony danych osobowych (np. przejrzystości przetwarzania), a wyłącznie w aspekcie bezpieczeństwa, tj. atrybutów poufności, dostępności i integralności danych. Wskazany przepis dotyczy zarówno etapu projektowania przetwarzania danych, jak i późniejszych etapów (już samego przetwarzania). Artykuł 32 RODO znajdzie zastosowanie także w przypadku naruszenia bezpieczeństwa (naruszenia ochrony danych osobowych), o czym mowa w art. 33 i 34 RODO, w tym sensie, że w przypadku naruszenia należy ponownie zweryfikować, czy środki już wdrożone w celu zapewnienia bezpieczeństwa są odpowiednie do poziomu ryzyka (np. wystąpienie zagrożenia oznacza, że rośnie parametr „prawdopodobieństwa" w przyszłości).

W przypadku administratora danych art. 32 RODO stanowi uszczegółowienie wymogu oceny ryzyka w fazie projektowania. Posługuje się tymi samymi kryteriami co art. 25 ust. 1 RODO. Co istotne, ocenę ryzyka w zakresie bezpieczeństwa przeprowadza także podmiot przetwarzający, którego z kolei art. 25 ust. 1 RODO nie dotyczy (a przynajmniej nie dotyczy bezpośrednio).

Artykuł 32 ust. 1 RODO nie przesądza, czy przedmiotem oceny ma być proces przetwarzania danych (np. marketing mailowy), czy każde aktywo w ramach tego procesu (np. system CRM). Każdy wariant jest dopuszczalny, o ile sposób szacowania ryzyka jest zgodny z treścią art. 24 i 25 RODO, w tym jest rozliczalny.

Komentowany przepis rodzi następujące wątpliwości dotyczące relacji pomiędzy administratorem danych i podmiotem przetwarzającym:

- **Czy i ewentualnie na ile podmiot przetwarzający ma obowiązek uwzględnić cele przetwarzania realizowane przez administratora?**
  Artykuł 32 ust. 1 RODO wyraźnie wskazuje, że elementem tła oceny ryzyka, dokonywanej także przez podmiot przetwarzający, są cele przetwarzania. Podmiot przetwarzający musi te cele uwzględnić, chociaż to administrator danych (zgodnie z definicją pojęcia administratora) jest podmiotem decydującym o celach i środkach przetwarzania danych. Cele te powinny wynikać z treści umowy powierzenia danych. Zgodnie z art. 28 ust. 3 RODO elementem umowy powierzenia danych jest określenie przedmiotu i czasu trwania przetwarzania, charakteru i celów przetwarzania, rodzaju danych osobowych oraz kategorii osób, których dane dotyczą, obowiązków i praw administratora.
  Wskazana ocena ryzyka – dokonywana przez podmiot przetwarzający – musi jednak nastąpić jeszcze przed rozpoczęciem przetwarzania przez podmiot przetwarzający. W przeciwnym razie cel art. 32 ust. 1 RODO nie zostanie zrealizowany. Na-

tomiast art. 32 RODO nie przesądza, czy podmiot przetwarzający musi taką ocenę przeprowadzić jeszcze przed zawarciem umowy powierzenia. W końcu dopiero w tej umowie uzgodnione zostanie tło (parametry) przetwarzania danych. Inaczej jest z administratorem danych – w jego przypadku art. 28 ust. 1 RODO wyraźnie wymaga wstępnej weryfikacji podmiotu przetwarzającego (jeszcze przed zawarciem umowy). Należy przyjąć, że ocena ryzyka realizowana przez podmiot przetwarzający musi nastąpić przed rozpoczęciem przetwarzania (oraz musi być ponawiana w czasie samego przetwarzania jako element ciągłego zapewniania bezpieczeństwa), natomiast może nastąpić już po zawarciu umowy powierzenia danych osobowych.

- **Na podstawie jakich informacji uzyskanych od administratora danych podmiot przetwarzający dokonuje oceny ryzyka, w szczególności czy powinien także uwzględnić informacje znane podmiotowi przetwarzającemu w ramach innych procesów przetwarzania danych, np. realizowanych we własnym imieniu (np. przetwarza dane innych kategorii w podobnych celach jako administrator danych – pracodawca)?**
  Podmiot przetwarzający (obok administratora danych) samodzielnie dokonuje oceny ryzyka, o której mowa w art. 32 RODO. Oznacza to, że musi samodzielnie zidentyfikować zagrożenia (źródła ryzyka) i ich możliwe negatywne konsekwencje. Natomiast należy przyjąć, że w zakresie regulowanym przez art. 28 ust. 3 RODO podmiot przetwarzający bazuje na informacjach przekazanych przez administratora, np. co do rodzaju przetwarzanych danych w danym procesie.
- **Czy administrator danych musi udzielić (z własnej inicjatywy czy na żądanie podmiotu przetwarzającego) podmiotowi przetwarzającemu informacji, które umożliwiają dokonanie oceny ryzyka (np. podmiot przetwarzający hostujący dane żąda informacji, jakie kategorie danych będą przechowywane na jego serwerach)?**
  Artykuł 28 RODO reguluje całościowo, jakie informacje są ujawniane podmiotowi przetwarzającemu w ramach współpracy pomiędzy podmiotem przetwarzającym i administratorem danych. Podmiot przetwarzający, zgodnie z art. 28 ust. 3 RODO, uzyska informacje m.in. o celach przetwarzania danych. Są to parametry umowy powierzenia, które są elementem jej treści.
  Natomiast trzeba zwrócić uwagę, że – w przeciwieństwie do uprawnień administratora wskazanych w art. 28 ust. 3 lit. h RODO – podmiot przetwarzający nie jest uprawniony do żądania od administratora informacji niezbędnych do wykazania spełnienia obowiązków określonych w RODO.
- **Czy ocena ryzyka przeprowadzona przez podmiot przetwarzający jest wiążąca dla administratora danych (np. podmiot przetwarzający ocenił, że ryzyko jest wysokie, a administrator – że niskie)?**
  Brak przepisu RODO, który w tym zakresie wprowadzałby rodzaj „związania" administratora danych oceną dokonaną przez podmiot przetwarzający. Można jednak przyjąć, że wyniki tej oceny – dokonanej przez podmiot przetwarzający – będą wpływać na „tło" oceny ryzyka przeprowadzanej przez samego administratora danych.

Należy zwrócić też uwagę, że zarówno administrator danych, jak i podmiot przetwarzający samodzielnie podejmują decyzje odnośnie do akceptacji ryzyka oraz wdrożenia środków bezpieczeństwa odpowiednich do poziomu ryzyka. Oczywiście podmiot przetwarzający musi uwzględnić wymogi postawione mu w umowie powierzenia (np. minimalny standard wdrożenia określonych środków dotyczących szyfrowania). Co istotne, niezależnie od treści umowy powierzenia podmiot przetwarzający ma obowiązek dostosować środki bezpieczeństwa do poziomu ryzyka. Nie może on obniżyć poziomu środków bezpieczeństwa „poniżej" tego, co wynika z art. 32 RODO, nawet jeżeli ten niższy poziom wynika z umowy powierzenia (inną kwestią jest to, że taki zapis umowy powierzenia naruszy art. 28 ust. 3 RODO).

Natomiast art. 28 ust. 3 lit. f RODO wymaga, aby podmiot przetwarzający pomagał administratorowi realizować obowiązki, m.in. wynikające z art. 32 RODO. Natomiast art. 28 ust. 3 lit. h RODO wskazuje, że podmiot przetwarzający ma obowiązek udostępnić administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO.

W związku z tym wydaje się, że przynajmniej w przypadku zidentyfikowania wysokich ryzyk dla praw lub wolności podmiot przetwarzający powinien – z własnej inicjatywy – poinformować o tym administratora. Jednocześnie należy przyjąć, że:

- administrator danych nie może zaakceptować ryzyka „za" podmiot przetwarzający (i oczywiście *vice versa*);
- administrator danych nie może „wymóc" na podmiocie przetwarzającym akceptację ryzyka w sytuacji, gdy podmiot przetwarzający uważa, że należy wdrożyć dodatkowe środki bezpieczeństwa.

- **Czy ocena ryzyka przeprowadzona przez podmiot przetwarzający może rodzić obowiązek przeprowadzenia oceny skutków (zob. szerzej rozdział 5)?**
  Należy przyjąć, że tak. Oczywiście oceny skutków będzie dokonywać administrator danych.
- **Jak powinien postąpić administrator, gdy jego ocena ryzyka identyfikuje inny jego poziom niż w przypadku podmiotu przetwarzającego?**
  Wydaje się, że w takim przypadku administrator danych musi zweryfikować przyczynę rozbieżności. W ramach swojego szacowania ryzyka powinien (w ramach tła oceny ryzyka) uwzględnić ocenę dokonaną przez podmiot przetwarzający.
  Ciekawym przykładem próby uregulowania rozkładu ról i odpowiedzialności w zakresie oceny ryzyka pomiędzy administratorem danych i podmiotem przetwarzającym jest treść – zatwierdzonych przez EROD – standardowych klauzul powierzenia przygotowanych przez duński organ nadzorczy. Zgodnie z treścią pkt 6 wskazanych klauzul[6]:

[6] Standardowe klauzule umowne do celów art. 28 ust. 3 rozporządzenia 2016/679 (RODO), źródło: https://edpb.europa.eu/our-work-tools/our-documents/decision-sa/dk-sa-standard-contractual-clauses--purposes-compliance-art_pl.

„Administrator danych szacuje ryzyko dla praw i wolności osób fizycznych związane z przetwarzaniem i wdraża środki mające na celu ograniczenie tego ryzyka. W zależności od ich znaczenia środki te mogą obejmować:

- pseudonimizację i szyfrowanie danych osobowych;
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Zgodnie z art. 32 ogólnego rozporządzenia o ochronie danych, podmiot przetwarzający – niezależnie od administratora danych – ocenia również ryzyko dla praw i wolności osób fizycznych nierozerwalnie związane z przetwarzaniem i wdraża środki mające na celu ograniczenie tego ryzyka. W tym celu administrator danych przekazuje podmiotowi przetwarzającemu dane wszelkie informacje niezbędne do zidentyfikowania i oceny takiego ryzyka.

Ponadto podmiot przetwarzający pomaga administratorowi danych zapewnić przestrzeganie obowiązków administratora danych na podstawie art. 32 ogólnego rozporządzenia o ochronie danych, między innymi przekazując administratorowi danych informacje dotyczące środków technicznych i organizacyjnych już wdrożonych przez podmiot przetwarzający zgodnie z art. 32 ogólnego rozporządzenia o ochronie danych wraz ze wszystkimi innymi informacjami niezbędnymi do tego, by administrator danych przestrzegał obowiązków administratora danych na podstawie art. 32 ogólnego rozporządzenia o ochronie danych.

Jeżeli następnie – w ocenie administratora danych – ograniczenie zidentyfikowanego ryzyka wymaga podjęcia innych środków przez podmiot przetwarzający niż środki już wdrożone przez podmiot przetwarzający na podstawie art. 32 ogólnego rozporządzenia o ochronie danych, administrator danych określa te dodatkowe środki w załączniku C".

Jak wynika z treści przywołanych klauzul, duński organ nadzorczy dostrzegł problem przepływu informacji w kierunku: administrator danych -> podmiot przetwarzający i wyraźnie, wprowadził obowiązek administratora w tym zakresie („administrator danych przekazuje podmiotowi przetwarzającemu dane wszelkie informacje niezbędne do zidentyfikowania i oceny takiego ryzyka").

E. Ocena ryzyka w ramach oceny incydentów bezpieczeństwa danych osobowych w kontekście obowiązku zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33 ust. 1 RODO)

W przypadku wystąpienia naruszenia ochrony danych osobowych administrator ma obowiązek „bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia" zgłosić to naruszenie organowi nadzorczemu. Nie do-

tyczy to sytuacji, gdy „jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych". Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin należy dołączyć wyjaśnienie przyczyn opóźnienia.

Komentarz:

Komentowany art. 33 RODO dotyczy aspektu bezpieczeństwa przetwarzania danych, ale wyłącznie w przypadku naruszenia ochrony danych osobowych, czyli w fazie materializacji zagrożenia. Można to przedstawić na następującym przykładzie: w fazie projektowania szacowane jest prawdopodobieństwo wystąpienia źródła ryzyka, np. naruszenie poufności przez kradzież laptopa, natomiast w tej fazie (naruszenia ochrony danych osobowych) do tej kradzieży już doszło.

Sytuacja ta nie dotyczy więc fazy projektowania procesów przetwarzania, a odnosi się do fazy przetwarzania danych. W tym przypadku ocena ryzyka nie służy odpowiedzi na pytanie, czy wdrożone środki bezpieczeństwa są odpowiednie do poziomu ryzyka. Chodzi bardziej o to, czy w związku z naruszeniem, które nastąpiło (zagrożenie się zmaterializowało, np. doszło do kradzieży nośnika danych – naruszenie poufności danych), dojdzie lub już doszło do naruszenia praw lub wolności i w związku z tym należy zgłosić do organu nadzorczego informacje o wystąpieniu naruszeniu ochrony danych. Oczywiście wystąpienie naruszenia (materializacja zagrożenia) będzie wpływało na poziom prawdopodobieństwa wystąpienia zagrożenia w przyszłości.

Jeśli w sytuacji naruszenia ochrony danych w przetwarzanie danych zaangażowany jest w jakikolwiek sposób podmiot przetwarzający, to jego rola ogranicza się do dwóch ważnych działań:

1) niezwłocznego powiadomienia administratora o naruszeniu danych (konkretny termin będzie zwykle uzgodniony przez strony umowy powierzenia; RODO w art. 28 ust. 3 jednak wyraźnie takiego obowiązku uzgodnienia nie zawiera; w przypadku braku uzgodnienia tej kwestii zastosowanie znajdzie art. 33 ust. 2 RODO, który ogólnie stwierdza, że podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi);
2) wsparcia administratora w ocenie całej sytuacji związanej z naruszeniem ochrony danych lub podejrzeniem naruszenia na zasadach określonych zgodnie z art. 28 ust. 3 lit. f w ramach mechanizmu współpracy pomiędzy stronami umowy powierzenia.

Przykładowo, duński organ nadzorczy w swoich – zatwierdzonych przez EROD – wzorcowych klauzulach powierzenia przyjmuje następujące postanowienia w zakresie zgłoszenia naruszenia przez podmiot przetwarzający[7]:

[7] Zob. https://edpb.europa.eu/sites/edpb/files/files/file1/dk_sa_standard_contractual_clauses_january_2020_pl.pdf.

„1. W przypadku naruszenia ochrony danych osobowych, podmiot przetwarzający bez zbędnej zwłoki po otrzymaniu wiadomości o tym fakcie powiadamia administratora danych o naruszeniu ochrony danych osobowych.
2. Powiadomienie administratora danych przez podmiot przetwarzający odbywa się, w miarę możliwości, w ciągu [LICZBA GODZIN] od chwili, gdy podmiot przetwarzający dowiedział się o naruszeniu ochrony danych osobowych, by umożliwić administratorowi danych wywiązanie się z obowiązku zawiadomienia właściwego organu nadzorczego o naruszeniu ochrony danych osobowych, por. art. 33 ogólnego rozporządzenia o ochronie danych".

Powyższe jest tylko potwierdzeniem, że:
- RODO ogólnie wskazuje termin realizacji obowiązku informowania administratora przez podmiot przetwarzający o naruszeniu ochrony danych osobowych;
- RODO nie wymaga wprost, aby w umowie powierzenia wskazano dokładny termin realizacji ww. obowiązku;
- należy rekomendować wprowadzenie do umowy wymogu informacyjnego w określonym terminie;
- ww. obowiązek informacyjny podmiotu przetwarzającego dotyczy naruszenia ochrony danych osobowych, a nie samego podejrzenia, niemniej nie można wykluczyć takiego podejścia, że strony umowy powierzenia wprowadzają obowiązek informowania zarówno o naruszeniach, jak i o podejrzeniach naruszenia ochrony danych.

F. Ocena ryzyka w ramach weryfikacji potrzeby zawiadamiania osoby, której dane są przetwarzane, w związku z incydentem bezpieczeństwa (art. 34 ust. 1 RODO)

Administrator danych ma obowiązek – bez zbędnej zwłoki – zawiadomić osobę, której dane dotyczą, o naruszeniu ochrony jej danych osobowych. Dotyczy to sytuacji, gdy „naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych".

Komentarz:

Wskazany art. 34 RODO dotyczy aspektu bezpieczeństwa, ale wyłącznie na etapie naruszenia ochrony danych osobowych. Nie odnosi się więc do fazy projektowania. Podobnie jak w przypadku art. 33 RODO, także w tym przypadku ocena ryzyka nie służy odpowiedzi na pytanie, czy wdrożone środki bezpieczeństwa są odpowiednie do poziomu ryzyka. Chodzi bardziej o to, czy w związku z naruszeniem, które nastąpiło (zagrożenie się zmaterializowało, np. doszło do kradzieży nośnika danych), możliwe, że wystąpi negatywny skutek, np. kradzież tożsamości (lub wręcz skutek się zmaterializował, np. znane są przypadki kradzieży toż-

samości), i w związku z tym należy zawiadomić o naruszeniu osoby, których ono dotyczy.

Poziom ryzyka oceniony w ramach naruszenia ochrony danych służy przede wszystkim określeniu przez administratora konkretnych dalszych działań. I tak, zgodnie z art. 33 i 34 RODO można wyróżnić trzy poziomy ryzyka determinujące odpowiednie zachowanie się administratora:

Poziom ryzyka	Działania administratora
1) ryzyko naruszenia praw lub wolności jest mało prawdopodobne	udokumentowanie naruszenia, nie ma konieczności zawiadamiania organu nadzorczego ani osób, których dane są objęte tym zdarzeniem
2) prawdopodobieństwo ryzyka jest wyższe niż „mało prawdopodobne"	konieczność zawiadamiania organu nadzorczego
3) ryzyko naruszenia praw lub wolności jest na wysokim poziomie	konieczność zawiadamiania organu nadzorczego oraz podmiotów danych

W kontekście powyższego należy przywołać następujące stanowisko UODO[8]:

1) nie każda czasowa niedostępność danych jest naruszeniem. Jest nią tylko taka niedostępność danych, która może stanowić ryzyko dla praw lub wolności osób fizycznych, np. w przypadku szpitala brak dostępu do danych pacjentów może prowadzić do uniemożliwienia przeprowadzenia operacji medycznej, a zatem narażenia życia, co należy zaklasyfikować jako wysokie ryzyko dla praw lub wolności osób fizycznych (s. 4);
2) zdolność do zapobiegania naruszeniom w przypadkach, w których jest to możliwe, oraz zdolność do niezwłocznego reagowania na naruszenia w sytuacjach, w których mimo to dojdzie do ich wystąpienia stanowi kluczowy element każdej polityki w zakresie bezpieczeństwa danych (s. 5);
3) dobrze zaprojektowana i wdrożona procedura postępowania na wypadek wystąpienia naruszenia ochrony danych pozwala dokonać klasyfikacji zidentyfikowanych naruszeń ochrony danych, czyli określić poziom wystąpienia ryzyka naruszenia praw i wolności osób fizycznych (s. 5);
4) uzgodnienia umowne między współadministratorami uwzględniały postanowienia wskazujące administratora, który będzie zajmował się dbaniem o wypełnianie ustanowionych w RODO obowiązków w zakresie zgłaszania naruszeń lub który będzie odpowiedzialny za wypełnianie tych obowiązków (s. 6);
5) zgodnie z art. 33 ust. 2 RODO podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi. Bez zbędnej zwłoki oznacza najszybciej jak to możliwe i taki termin wywiązywania się z tego obowiązku powinien być nałożony na podmioty przetwarza-

[8] UODO, *Obowiązki administratorów związane z naruszeniami ochrony danych osobowych*, https://uodo.gov.pl/pl/134/1029. Numery stron wskazane w pkt 1–12 dotyczą wskazanego stanowiska UODO.

jące w umowach powierzenia. Jeżeli podmiot przetwarzający świadczy usługi na rzecz wielu administratorów, a dany incydent wywiera wpływ na wszystkich z nich, podmiot przetwarzający będzie zobowiązany do zgłoszenia naruszenia bez zbędnej zwłoki każdemu z tych administratorów (s. 6);

6) wprowadzenie procedur umożliwiających stwierdzanie i ocenę naruszeń pod kątem wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych jest obowiązkiem administratora niezależnie od zaistnienia naruszenia ochrony danych osobowych (s. 13);
7) podczas oceny ryzyka naruszenia praw lub wolności osób fizycznych powstałego w wyniku wystąpienia naruszenia kładzie się nacisk na inne kwestie niż uwzględniane w ocenie skutków dla ochrony danych. W ocenie skutków dla ochrony danych bierze się pod uwagę zarówno ryzyko dla planowego przetwarzania danych, jak i ryzyko powstałe w przypadku wystąpienia naruszenia. Badając możliwe naruszenie, rozpatruje się w ujęciu ogólnym prawdopodobieństwo jego wystąpienia oraz szkody dla osób, których dane dotyczą, jakie mogą z niego wyniknąć. Innymi słowy, jest to ocena wydarzenia hipotetycznego. W przypadku faktycznego naruszenia zdarzenie już nastąpiło, więc nacisk kładzie się w całości na powstałe ryzyko, że naruszenie będzie skutkowało wpływem na osoby fizyczne (s. 13);
8) dlatego oceniając ryzyko naruszenia praw i wolności osób, których dane dotyczą, osoby odpowiedzialne za przeprowadzenie tego procesu powinny przyjąć perspektywę osób, których dane są przetwarzane, i właśnie z tej perspektywy oceniać stopień dotkliwości w przypadku zmaterializowania się zagrożenia (s. 13);
9) jeżeli naruszenie dotyczy danych osobowych ujawniających: pochodzenie etniczne; poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane dotyczące zdrowia, dane dotyczące życia seksualnego, należy uznać, że występuje duże prawdopodobieństwo takiej szkody. Niemniej jednak każde z takich zdarzeń należy rozpatrywać indywidualnie (s. 15);
10) to, czy administrator wie, że dane osobowe znajdują się w rękach osób, których zamiary są nieznane lub które mogą mieć złe intencje, może mieć znaczenie dla poziomu potencjalnego ryzyka. Nie budzi więc żadnych wątpliwości, że np. naruszenie poufności danych będące wynikiem kradzieży dokumentów wiąże się z wysokim ryzykiem dla osób, których dane dotyczą. W każdym przypadku, rozpatrując zgłoszone naruszenie, organ nadzorczy przyjmuje perspektywę osób, których dane dotyczą i właśnie z tej perspektywy ocenia stopień dotkliwości w przypadku zmaterializowania się zagrożenia (s. 17);
11) UODO (s. 16) za GR29 wskazuje następujące kryteria oceny ryzyka:
    a) rodzaj naruszenia;
    b) charakter, wrażliwość i ilość danych osobowych;
    c) łatwość identyfikacji osób fizycznych;
    d) waga konsekwencji dla osób fizycznych;

e) cechy szczególne danej osoby fizycznej;
f) cechy szczególne administratora danych;
g) liczba osób fizycznych, na które naruszenie wywiera wpływ;

12) w ewidencji naruszeń powinno się dokumentować zarówno naruszenia ochrony danych osobowych podlegające obowiązkowi notyfikacyjnemu Prezesowi UODO, jak i te, które nie podlegają zgłoszeniu organowi nadzorczemu ze względu na to, że mało prawdopodobne jest, by skutkowały one ryzykiem naruszenia praw lub wolności osób fizycznych.

Na koniec tej części analizy należy zwrócić uwagę, że naruszenie bezpieczeństwa (np. poufności danych) może być następstwem naruszenia innego wymogu, np. poprawności danych – np. brak zmiany adresu doręczenia pomimo zgłoszenia klienta i dalsze przesyłanie korespondencji z możliwością zapoznania się z nią przez inne (nieuprawnione) osoby.

G. Ocena ryzyka w ramach oceny skutków dla ochrony danych osobowych (art. 35 ust. 1 RODO)

Administrator przed rozpoczęciem przetwarzania ma obowiązek dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, jeżeli „dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych". Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę. Zawiera ona m.in. ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą.

Komentarz:

Artykuł 35 RODO nie jest źródłem ogólnego obowiązku oceny ryzyka. Jak wskazano powyżej, tym źródłem są art. 24 i 25 RODO. Komentowany przepis nie może być rozumiany w ten sposób, że wyłącznie w przypadku, o którym mowa w art. 35 ust. 1 RODO, tj. dużego prawdopodobieństwa wysokiego ryzyka, należy przeprowadzić ocenę ryzyka naruszenia praw lub wolności.

Jak wynika z treści art. 35 ust. 7 lit. c RODO, ocena skutków zawiera ocenę ryzyka naruszenia praw lub wolności podmiotów danych. Uzasadnia to stanowisko, że aby dokonać oceny skutków, należy wcześniej przeprowadzić ocenę ryzyka zgodnie z art. 24 i 25 RODO, a ocena skutków jest dalszym etapem „pogłębionej" analizy, uzupełniona o dodatkowe elementy (poza samą oceną ryzyka), wskazane w ust. 7 art. 35 RODO.

Potrzeba dokonania oceny skutków (czyli „pogłębionej" oceny ryzyka) może ujawniać się w dwóch przypadkach:

- już wstępna ocena procesu przetwarzania danych (realizowanych operacji na danych) ujawnia, że jedna z tych operacji spełnia kryteria wykazu organu nadzorczego, o czym mowa w art. 35 ust. 4 RODO (co najmniej 2)[9];
- wstępna ocena procesu przetwarzania danych (realizowanych operacji na danych) nie ujawnia, że jedna z tych operacji spełnia kryteria wykazu organu nadzorczego, o czym mowa w art. 35 ust. 4 RODO, ale wstępna ocena ryzyka wykazuje, że występuje duże prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności.

Analizując dalej ust. 7 art. 35, można zdefiniować proces dokonywania oceny skutków w ramach następujących etapów:

1) określenie tła oceny ryzyka m.in. celów i planowanych operacji (zob. szerzej rozdział 1, pkt 11 poniżej);
2) przeprowadzenie „wstępnej" oceny ryzyka naruszenia praw lub wolności;
3) identyfikacja, czy występuje przypadek dużego prawdopodobieństwa wysokiego ryzyka;
4) przeprowadzenie analizy, o której mowa w art. 35 ust. 7 RODO, m.in. proporcjonalności i niezbędności;

[9] Chodzi o następujące operacje (Komunikat Prezesa UODO z 17.06.2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony M.P. z 2019 r. poz. 666):

- ewaluacja lub ocena, w tym profilowanie i przewidywanie (analiza behawioralna) w celach wywołujących negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych;
- zautomatyzowane podejmowanie decyzji wywołujących skutki prawne, finansowe lub podobne istotne skutki;
- systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajdą się w monitorowanej przestrzeni. Do tej grupy systemów nie są zaliczane systemy monitoringu wizyjnego, w których obraz jest nagrywany i wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa;
- przetwarzanie szczególnych kategorii danych osobowych i dotyczących wyroków skazujących i czynów zabronionych (danych wrażliwych wg opinii WP 29);
- przetwarzanie danych biometrycznych wyłącznie w celu identyfikacji osoby fizycznej bądź w celu kontroli dostępu;
- przetwarzanie danych genetycznych;
- dane przetwarzane na dużą skalę, gdzie pojęcie dużej skali dotyczy: liczby osób, których dane są przetwarzane, zakresu przetwarzania, okresu przechowywania danych oraz geograficznego zakresu przetwarzania;
- przeprowadzanie porównań, ocena lub wnioskowanie na podstawie analizy danych pozyskanych z różnych źródeł;
- przetwarzanie danych dotyczących osób, których ocena i świadczone im usługi są uzależnione od podmiotów lub osób, które dysponują uprawnieniami nadzorczymi i/lub ocennymi;
- innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych;
- gdy przetwarzanie samo w sobie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy;
- przetwarzanie danych lokalizacyjnych.

5) wskazanie planowanych środków w celu zaradzenia ryzyku, mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO;
6) wskazanie, czy administrator nie jest członkiem kodeksu postępowania w ramach mechanizmów określonych w art. 40 RODO;
7) zasięgnięcie opinii osób, których będzie dotyczyło przyszłe przetwarzanie danych osobowych;
8) zasięgnięcie opinii Inspektora Ochrony Danych (jeśli został wyznaczony u danego administratora).

Na szczególną uwagę zasługuje pierwsza część lit. a ust. 7 art. 35 RODO: „systematyczny opis planowanych operacji przetwarzania danych". Przepis ten wymaga nie tylko identyfikacji operacji na danych osobowych, ale także aby dokonać systematycznego opisu tych operacji. Natomiast przepisy art. 24 i 25 RODO nie nakazują (wprost) brania pod uwagę operacji przetwarzania danych. Zatrzymując się na chwilę nad tym zagadnieniem, należy zadać pytanie, czy w ogóle można dokonać jakiejkolwiek analizy ryzyka przetwarzania danych osobowych, jeśli nie zna się operacji przetwarzania. „Przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych; aby dokonać jakiejkolwiek analizy czy oceny procesu przetwarzania, wpierw należy zrozumieć proces przetwarzania, na który składają się poszczególne operacje. Dlatego w praktyce należy rekomendować, aby w każdej ocenie ryzyka (także z uwagi na zasadę rozliczalności z art. 5 ust. 2 RODO oraz motyw 76 RODO), w tym w fazie projektowania (art. 24 i 25), sporządzać opis operacji przetwarzania danych osobowych składających się na dany proces przetwarzania. Oczywiście w przypadku, o którym mowa w art. 35 ust. 7 RODO, ten opis musi być systematyczny. Wydaje się, że w tym przypadku poziom opisu musi być bardziej pogłębiony. Taką wykładnię wspiera także lektura motywów 75 i 76 RODO. Zgodnie z motywem 76 (który jest bardzo ogólny i dotyczy wszystkich aspektów oceny ryzyka), „ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko". Kwestia ta zostanie rozwinięta w pkt 11 poniżej.

Dodatkową, szczególną uwagę, należy zwrócić na brzmienie przepisu lit. e ust. 7 art. 35. Nakazuje on zaplanowanie środków w celu zaradzenia ryzyku i mających zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO. Skoro, jak zostało wskazane wcześniej, ocena ryzyka, zgodnie z art. 24 i 25 RODO, została już przeprowadzona wcześniej, przed oceną skutków, i zawiera ona również środki zabezpieczające, to czy planowane środki w ramach oceny skutków są tymi samymi czy innymi środkami? Oczywiście pytanie dotyczy sytuacji, gdy wcześniej taka wstępna ocena została dokonana. Biorąc pod uwagę, że:
- ocena skutków jest bardziej pogłębioną i bardziej sformalizowaną oceną (niż „zwykła" ocena ryzyka);
- ocena skutków jest konieczna do przeprowadzenia, kiedy w wyniku wcześniej przeprowadzonej (wstępnej) oceny ryzyka jego poziom został określony jako wysoki,

– w ramach oceny skutków należy zaplanować (a przynajmniej rozważyć) dodatkowe środki, które nie zostały zaplanowane na etapie ogólnej oceny ryzyka dokonywanej na podstawie art. 24 i 25.

H. Ocena ryzyka dokonywana w ramach uprzednich konsultacji (art. 36 RODO)

Zgodnie z art. 36 ust. 1 RODO, jeżeli ocena skutków dla ochrony danych, o której mowa w art. 35 RODO, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym. Natomiast art. 36 ust. 3 RODO wskazuje, że administrator w ramach uprzednich konsultacji przedstawia organowi nadzorczemu:

1) gdy ma to zastosowanie – odpowiednie obowiązki administratora, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu, w szczególności w przypadku przetwarzania w ramach grupy przedsiębiorstw;
2) cele i sposoby zamierzonego przetwarzania;
3) środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą, zgodnie z niniejszym rozporządzeniem;
4) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
5) ocenę skutków dla ochrony danych, o której mowa w art. 35 RODO;
6) wszelkie inne informacje, których żąda organ nadzorczy.

Komentarz:

Komentowany przepis nie jest źródłem obowiązku oceny ryzyka, ale określa konsekwencje przeprowadzenia oceny skutków w sytuacji, gdy przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka. W takiej sytuacji przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym.

Jak wskazała Grupa Robocza art. 29 (obecnie EROD) w opinii nr WP 248 rev.01[10] (s. 18), obowiązek przeprowadzenia uprzednich konsultacji aktualizuje się zawsze, gdy administrator danych nie może znaleźć środków wystarczających do zmniejszenia ryzyka do dopuszczalnego poziomu (np. ryzyko szczątkowe wciąż jest wysokie). Ponadto administrator będzie zobowiązany skonsultować się z organem nadzorczym, zawsze gdy prawo państwa członkowskiego wymaga, by administratorzy konsultowali się z organem nadzorczym lub uzyskiwali jego uprzednią zgodę w odniesie-

[10] GR29, Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, WP 248, rev.01, https://giodo.gov.pl/pl/file/13177, s. 18.

niu do przetwarzania danych osobowych przez administratora do celów wykonania zadania realizowanego przez niego w interesie publicznym, w tym przetwarzania w związku z ochroną socjalną i zdrowiem publicznym (art. 36 ust. 5). Warto wyjaśnić, że RODO nie posługuje się pojęciem ryzyka szczątkowego tylko GR29 (EROD) w swoim dokumencie WP 248. Pojęcie to należy rozumieć zgodnie z definicjami w dziedzinie nauki o zarządzaniu i oznacza ono ryzyko, które pozostało po zastosowaniu określonych środków bezpieczeństwa. Ryzyko „szczątkowe" jest zazwyczaj niższe niż ryzyko pierwotnie szacowane właśnie z uwagi na zastosowanie kolejnych środków obniżających przedmiotowe ryzyko.

I. Ocena ryzyka dokonywana w kontekście sposobu realizacji zadań IOD (art. 39 ust. 2 RODO)

Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

Komentarz:

Komentowany przepis nakłada na inspektorów ochrony danych obowiązek, aby tak planowali i realizowali swoje zadania kontrolno-monitorujące wskazane w art. 39 ust. 1 lit. b RODO, aby więcej czasu i wysiłku poświęcali tym obszarom działalności administratora (lub podmiotu przetwarzającego), w których przetwarzanie danych osobowych może wiązać się z większym ryzykiem. Jeśli jakiś obszar działalności administratora jest bardziej podatny na zagrożenia naruszenia praw lub wolności osób fizycznych, tym więcej audytów lub innych form monitorowania zgodności inspektorów należy się spodziewać.

Wątpliwości budzi odpowiedź na pytanie, którym ryzykiem powinien kierować się inspektor ochrony danych. Czy tym ryzykiem oszacowanym przez administratora, czy może swoją wiedzą, swoim punktem widzenia, które obszary wiążą się z większym ryzykiem naruszenia praw lub wolności? Łączy się to ściśle z jeszcze jednym problemem: kto powinien wyżej wymienioną ocenę przeprowadzać? Administrator danych (odpowiednio podmiot przetwarzający)? Czy może sam IOD? I co się stanie, jeśli te dwie oceny wykonane przez administratora (lub podmiot przetwarzanym) różnią się od oceny ryzyka wykonanej przez inspektora?

Przepisy rozporządzenia nadkładają na administratora (czasem także na podmiot przetwarzający), a nie inspektorów, obowiązek oceny ryzyka. Co oznacza, że to administrator decyduje o tym, które obszary jego działalności, które procesy przetwarzania (aktywności przetwarzania) są związane z jakim ryzykiem. Inspektorzy są włączani obowiązkowo do takiej oceny, dopiero gdy zachodzą przesłanki z art. 35 – czyli w pro-

cesie oceny skutków dla ochrony danych. Wyobraźmy sobie zatem, że administrator oceniał, że ryzyko naruszenia praw podmiotów danych jest wyższe w obszarze kadrowym, natomiast w obszarze działania sprzedaży i marketingu ocenił ryzyko na znacznie niższym poziomie. To oznaczałoby dla Inspektora, że powinien on bardziej skupić swoją uwagę na procesach kadrowych (np. rekrutacje, zatrudnianie, obsługa ZFŚS, zwalnianie, szkolenia, zapewnienie BHP, awansowanie, ocena pracownicza itd.) niż na procesach sprzedażowo-marketingowych (np. pozyskiwanie nowych kontaktów handlowych, kupowanie/licencjonowanie baz danych, przesyłanie informacji handlowej drogą elektroniczną, prowadzenie konkursów marketingowych, badania marketingowe, profilowanie klientów itd.). Inspektor natomiast na podstawie np. liczby wniosków podmiotów danych, skarg składanych do organu ochrony, zakresu danych z wykorzystaniem nowych technologii, mógłby mieć zupełnie inny obraz ryzyka naruszenia praw podmiotów danych w obszarach omawianych jako przykłady[11].

Nie wydaje się racjonalne, aby prawodawca unijny nakładał na inspektorów ochrony danych obowiązek dokonywania odrębnej oceny ryzyka i powinien się kierować tą oceną, która została dokonana przez administratora (podmiot przetwarzający). Jednakże jeśli dochodziłoby do nieprawidłowości, jakie zostały przykładowo wskazane powyżej, inspektor powinien kierować się ochroną prywatności podmiotów danych i w ramach swoich kompetencji określonych w art. 37–39 powinien doprowadzić do zmiany poziomu ryzyka ocenianego przez administratora (podmiot przetwarzający). Taka zmiana mogłaby np. polegać na zaleceniu wprowadzenia dodatkowego czynnika podwyższającego ryzyko naruszenia praw lub podmiotów danych w procedurze lub procesie oceny ryzyka. Tym czynnikiem podwyższającym ryzyko może być występowanie zasadnych wniosków czy skarg podmiotów danych na administratora w danym obszarze jego działalności. Z funkcji, jaką ma realizować inspektor, i jego niezależności można zatem wyinterpretować, że w przypadku gdy stwierdza on, że poziom określonego ryzyka został przez administratora (podmiot przetwarzający) zaniżony, powinien on powiadomić o takim zaniżeniu, a administrator (podmiot przetwarzający), jeśli uzna za stosowane, powinien zmienić swoją pierwotną ocenę. Jeśli natomiast administrator (podmiot przetwarzający) nie dokona takiej korekty ryzyka, inspektor powinien kierować swoje działania kontrolne (monitorujące) z uwzględnieniem swojej wiedzy na temat ryzyka w sposób niezależny. Pozwoli mu to wykonywać swoje zadania z należytą starannością i z uwzględnieniem spoczywających na nim obowiązków z art. 39 ust. 2.

[11] W decyzji nr ZSOŚS.421.25.2019 z 21.08.2020 r., https://uodo.gov.pl/decyzje/ZSOŚS.421.25.2019, PUODO stwierdził, że: „Inspektor ochrony danych powinien być angażowany w proces decyzyjny obejmujący procesy przetwarzania danych osobowych poprzez zapewnienie mu możliwości wyrażenia stanowiska w kontekście przyjmowanych rozwiązań technicznych, organizacyjnych i prawnych. Włączanie inspektora w sprawy dotyczące danych osobowych wpisuje się w koncepcję ochrony danych w fazie projektowania wyrażoną w art. 25 ust. 1 rozporządzenia 2016/679, która zobowiązuje administratora do wdrożenia odpowiednich środków technicznych i organizacyjnych – zarówno przy określaniu sposobu przetwarzania, jak i w czasie samego przetwarzania".

J. Ocena ryzyka w kontekście transferu danych poza EOG

Zgodnie z art. 44 RODO wszystkie przepisy rozdziału V, dotyczącego przekazywania danych poza Europejski Obszar Gospodarczy (EOG), należy stosować z myślą o zapewnieniu, by nie został naruszony stopień ochrony osób fizycznych zagwarantowany w niniejszym rozporządzeniu. Natomiast stosownie do treści art. 46 ust. 1 RODO w razie braku decyzji na mocy art. 45 ust. 3 administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej. Natomiast stosownie do treści art. 49 ust. 6 RODO administrator lub podmiot przetwarzający dokumentują ocenę oraz odpowiednie zabezpieczenia, o których mowa w ust. 1 akapit drugi niniejszego artykułu, w rejestrach wskazanych w art. 30 RODO.

Komentarz:

Trybunał Sprawiedliwości w sprawie C-311/18, Data Protection Commissioner v. Facebook Ireland Limited i Maximillian Schrems, EU:C:2020:559, zwrócił uwagę na ogólny obowiązek oceny ryzyka w przypadku transferu danych poza EOG. Oczywiście nie wyłącza on ogólnego obowiązku oceny ryzyka z art. 24, 25 i 32 oraz 35 RODO. Trybunał podkreślił jednak, że nawet w przypadku powoływania się na jedną z przesłanek przekazywania danych poza EOG (np. standardowe klauzule umowne) należy ocenić ryzyko związane z transferem danych. W szczególności Trybunał podkreśla, że istotna jest weryfikacja zagrożeń związanych z funkcjonowaniem systemu prawnego państwa odbiorcy i zakresu dostępu do danych podmiotów publicznych, np. w ramach działalności służb[12]. Powyższe orzeczenie bardzo mocno podkreśla, że w tym przypadku chodzi o często pomijany (dodatkowy) obowiązek dokonania oceny ryzyka transferu danych osobowych. Można tę kwestię ująć jeszcze inaczej. Po prostu administrator danych musi – w ramach ogólnej oceny ryzyka – uwzględnić szczególne zagrożenia, które mogą być związane z transferem danych poza EOG. Czyli nie wystarcza wdrożenie zabezpieczeń wskazanych w poszczególnych artykułach rozdziału V. Poziom zidentyfikowanego ryzyka może prowadzić do konieczności wdrożenia dodatkowych środków lub nawet zaprzestania transferu danych poza EOG.

W cały zagadnieniu dotyczącym oceny ryzyka w RODO jest to chyba najtrudniejszy pod względem merytorycznym, ale i ekonomicznym obowiązek prawny do spełnienia przez administratorów danych osobowych. Trudność tego obowiązku pod względem

[12] Zob. szerzej K. Irion, *Schrems II and Surveillance: Third Countries' National Security Powers in the Purview of EU Law*, https://europeanlawblog.eu/2020/07/24/schrems-ii-and-surveillance-third-countries-national-security-powers-in-the-purview-of-eu-law/.

merytorycznym polega na tym, że administrator danych musiałby dokonać oceny nie samego odbiorcy danych w państwie trzecim, ale całego systemu prawnego danego państwa trzeciego pod względem adekwatności z przepisami Unii Europejskiej w zakresie ochrony danych osobowych (RODO). Trudno wyobrazić sobie sytuację, w której każdy przedsiębiorca czy każdy podmiot publiczny jako administrator będzie w stanie merytorycznie ocenić system prawny danego państwa trzeciego. Skoro na poziomie Unii Europejskiej taką ocenę systemu prawnego dokonuje Komisja Europejska (zgodnie z art. 45 RODO) i nie jest to proces ani łatwy, ani krótkotrwały[13], to na poziomie pojedynczego analizatora danych osobowych będzie to zadanie wręcz niemożliwe. Pod względem ekonomicznym trudność takiego wykonania oceny ryzyka związanego z transferem danych do państwa trzeciego będzie polegała na tym, że albo administrator danych zleci dokonanie takiej oceny wyspecjalizowanym podmiotom, np. kancelariom prawnym, albo będzie musiał zrezygnować z korzystania z usług dostawców z państw trzecich, w tym USA, które niejednokrotnie są tańsze lub jakościowo nieosiągane dla podmiotów krajowych.

K. Obowiązek informacyjny dotyczący ryzyka w kontekście transferu danych poza EOG

Zgodnie z art. 49 ust. 1 lit. a RODO w razie braku decyzji stwierdzającej odpowiedni stopień ochrony określonej w art. 45 ust. 3 lub braku odpowiednich zabezpieczeń określonych w art. 46, w tym wiążących reguł korporacyjnych, jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej mogą nastąpić wyłącznie pod warunkiem, że m.in. osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którymi – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę.

Komentarz:

Komentowany przepis dotyczy jednej (nie wyłącznej) z podstaw transferu (przekazania) danych poza EOG. Wskazany przepis zawiera obowiązki informacyjne dotyczące kwestii ryzyka związanego z takim transferem danych. Nie można komentowanego przepisu rozumieć w ten sposób, że wprowadza on (tylko w przypadku transferu w oparciu o wyraźną zgodę) obowiązek przeprowadzania oceny ryzyka. Taki obo-

[13] Przykładowo, rozmowy UE dotyczące transferu danych do Japonii rozpoczęły się w styczniu 2017 r. a zakończyły się dopiero po 2 latach decyzją wykonawczą Komisji (UE) 2019/419 z 23.01.2019 r. na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzającą odpowiedni stopień ochrony danych osobowych przez Japonię na mocy ustawy o ochronie informacji osobowych (notyfikowana jako dokument nr C(2019) 304, Dz.Urz. UE L 76, s. 1), Key elements of the EU-Japan Economic Partnership Agreement Brussels, 12.12.2018.

wiązek wynika z art. 24, 25 i 32, a także art. 44 i 46 ust. 1 RODO, o czym była mowa powyżej. Celem realizacji obowiązków informacyjnych jest zapewnienie, aby zgoda została wyrażona w sposób świadomy, czyli w omawianym przypadku zgodnie z motywem 39 RODO; osobom fizycznym należy uświadomić ryzyka związane z takim przetwarzaniem danych.

Należy zwrócić także uwagę, że ogólny obowiązek informacyjny w zakresie transferu danych wynika z art. 13 i 14 RODO. Zgodnie z art. 13 ust. 1 lit. f RODO (podobnie w art. 14 ust. 1 lit. f RODO), jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje, gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, 47 lub 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia.

Natomiast w przypadku komentowanego przepisu chodzi o szczególny obowiązek informacyjny dotyczący zidentyfikowanych ryzyk związanych z transferem danych. Obejmuje on informacje o ryzykach, których źródłem może być transfer danych do takich krajów poza EOG, co do których brak jest decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony oraz brak odpowiednich zabezpieczeń prawnych. Przykładem takiego ryzyka dla podmiotu danych może być brak możliwości złożenia skutecznej skargi do organu ochrony danych w danym kraju czy brak możliwości uzyskania dostępu bądź kopii swoich danych osobowych. Głównym powodem ryzyka związanego z transferem danych poza EOG jest brak regulacji prawnych w danym kraju dających adekwatny poziom ochrony praw osób fizycznych.

L. Problem oceny ryzyka dla praw lub wolności w kontekście zadań organu nadzorczego (art. 57 ust. 1 lit. b RODO)

Stosownie do treści art. 57 ust. 1 lit. b RODO każdy organ nadzorczy na swoim terytorium m.in. upowszechnia w społeczeństwie wiedzę o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz rozumienie tych zjawisk. Szczególną uwagę poświęca działaniom skierowanym do dzieci.

Komentarz:

Problematyka ryzyka także dotyczy organu ochrony. Pomijając fakt, że organ ochrony także jest odrębnym administratorem (np. w stosunku do zatrudnianych pracowników, interesantów, którzy załatwiają swoje sprawy w urzędzie, uczestników czy szko-

leń organizowanych przez organ itd.), ma on w zakresie swoich obowiązków także swoisty obowiązek edukacyjny. Istotą tej edukacji jest budowanie świadomości, ale i ostrzeganie o ryzyku, jakie jest związane z przetwarzaniem danych osobowych. Wykonując to konkretne zadanie, organ nie musi dokonywać oceny poziomu ryzyka, jednak powinien ostrzegać o potencjalnych negatywnych skutkach konkretnego przetwarzania danych osobowych.

M. Ocena ryzyka a zadania EROD (art. 64 ust. 1 lit. a)

Europejska Rada Ochrony Danych zapewnia spójne stosowanie niniejszego rozporządzenia. W tym celu z własnej inicjatywy lub w stosownych przypadkach na wniosek Komisji podejmuje w szczególności następujące działania: m.in. wydaje wytyczne, zalecenia i określa najlepsze praktyki zgodnie z lit. e niniejszego ustępu, wskazujące, w jakich okolicznościach naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych w rozumieniu art. 34 ust. 1.

Komentarz:

Komentowany przepis dotyczy obowiązków EROD, ale nie jako administratora danych (oceniającego ryzyka w ramach procesów/aktywów, którymi dysponuje, lecz jako organu uprawnionego i zobowiązanego do podejmowania działań w zakresie budowy świadomości w zakresie przestrzegania przepisów o ochronie danych osobowych.

Szczególne przypadki oceny ryzyka

N. Ocena ryzyka w kontekście stosowania RODO

Zgodnie z art. 2 ust. 1 RODO rozporządzenie 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.

Definicja danych osobowych i samego przetwarzania została zawarta w art. 4 RODO. Zgodnie z art. 4 pkt 1 RODO dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Natomiast pojęcie przetwarzania danych definiuje art. 4

pkt 2 RODO, zgodnie z jego treścią „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Komentarz:

Tylko przetwarzanie danych osobowych w rozumieniu art. 4 pkt 1 i 2 i w sposób wskazany w art. 2 ust. 1 RODO podlega RODO. Oczywiście należy uwzględnić także przesłanki wyłączające stosowanie RODO wskazane np. w art. 2 ust. 2 RODO. Przykładowo mierzenie temperatury pracownikowi[14], jeżeli nie prowadzi do przetwarzania danych w sposób wskazany w art. 2 ust. 1 RODO, nie podlega RODO, chociaż może dotyczyć informacji o możliwej do identyfikacji osoby fizycznej.

W tych przypadkach ocena ryzyka i wdrażane środki dotyczyć mogą identyfikacji zagrożeń związanych z błędnym przyjęciem, że RODO nie znajduje zastosowania lub niekontrolowanym rozpoczęciem przetwarzania danych w rozumieniu art. 2 ust. 2 RODO. Przykładowo szacowane jest ryzyko, którego źródłem może być utrwalanie (pomimo zakazu administratora) przez pracowników wyników badania temperatury. W tym przypadku środkiem mitygującym ryzyko może być wprowadzenie procedury regulującej kwestie mierzenia temperatury. Oczywiście można powiedzieć, że ocena ryzyka w tym przypadku nie jest wymagana, ponieważ nie jest stosowane RODO. Takie podejście jednak nie byłoby zgodne z celem zasady *privacy by design* wyrażonej w art. 25 RODO. Podobnie przyjmuje się, że stwierdzenie, czy doszło do prawidłowej anonimizacji, czy informacje mają charakter danych osobowych, czy anonimowych podlega ocenie ryzyka (zob. szerzej tabela 7 poniżej i przypisy do niej). Ideą zasady *privacy by design* jest takie projektowanie przyszłych procesów przetwarzania danych osobowych, aby w przyszłości, gdy będą one miały miejsce, nie dochodziło do naruszenia praw lub wolności osób fizycznych z związku z przetwarzaniem danych osobowych.

O. Ocena procesora (podmiotu przetwarzającego)

Zgodnie z art. 28 ust. 1 RODO, w przypadku gdy przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwa-

[14] EIOD, *Orientations from the EDPS: Body temperature checks by EU institutions in the context of the COVID-19 crisis*, s. 2, wskazano, że kontrole temperatury ciała, obsługiwane ręcznie i po których nie następuje rejestracja, dokumentacja lub inne przetwarzanie danych osobowych danej osoby, z zasady nie podlegałyby zakresowi rozporządzenia. Wprawdzie EIOD odnosi się do rozporządzenia 2018/1725, niemniej w tym zakresie wskazane rozporządzenie jest zbliżone do RODO.

rzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.

Komentarz:

Komentowany przepis nie odwołuje się do pojęcia ryzyka naruszenia praw lub wolności. Nie może budzić wątpliwości, że wstępna ocena (przed zawarciem umowy) podmiotu przetwarzającego stanowi element wymogu *privacy by design* (czyli projektowania prywatności), o czym mowa w art. 25 ust. 1 RODO.

P. Przetwarzanie danych osobowych w celach wskazanych w treści art. 89 ust. 1 RODO

Stosownie do treści art. 89 ust. 1 RODO przetwarzanie danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych bądź do celów statystycznych podlega odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą, zgodnie z rozporządzeniem. Zabezpieczenia te polegają na wdrożeniu środków technicznych i organizacyjnych zapewniających poszanowanie zasady minimalizacji danych. Środki te mogą też obejmować pseudonimizację danych, o ile pozwala ona realizować powyższe cele. Jeżeli cele te można zrealizować w drodze dalszego przetwarzania danych, które nie pozwalają albo przestały pozwalać na zidentyfikowanie osoby, której dane dotyczą, cele należy realizować w ten sposób.

Komentarz:

Komentowany przepis posługuje się pojęciem i wymogiem wdrożenia odpowiednich zabezpieczeń. Dotyczy to przetwarzania danych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych. Jest to uszczegółowienie mechanizmu *privacy by design*, wyrażonego – jako ogólna reguła – w art. 25 ust. 1 RODO. Jakie jest uzasadnienie tego dookreślenia? Chodzi o to, że przetwarzanie danych we wskazanych celach korzysta z wielu „udogodnień", m.in. w zakresie realizacji praw osób, których dane dotyczą (zob. 89 ust. 2 RODO).

Analizowany przepis nie wskazuje jednak, co jest tym „probierzem" (punktem odniesienia) weryfikacji czy zabezpieczenia są odpowiednie. Nie może budzić wątpliwości, że jest nim zidentyfikowany poziom ryzyka naruszenia praw lub wolności w sensie ogólnym.

Komentowany przepis dotyczy głównie aspektu minimalizacji zakresu przetwarzanych danych. Wynika to z tego, że inne przepisy RODO (np. art. 5 ust. 1 lit. b RODO)

„luzują" inne wymogi, np. ograniczenie czasu przetwarzania danych. Sama natura przetwarzania danych osobowych do celów naukowych czy historycznych pozwala sądzić, że czas przetwarzania najprawdopodobniej będzie nieskończony. Przyjmując bowiem założenie, że na podstawie danych osobowych pierwotnych, po zastosowaniu środków np. częściowej anonimizacji czy pseudonimizacji, okrojeniu zakresu danych do niezbędnego minimum, te dane, które pozostaną – wynikowe (np. statystyczne, zbiorcze), będą na dłuższy okres, równolegle do czasu przechowywania np. wyników badań naukowych czy danych. Nie może to jednak oznaczać, że ocena ryzyka – w przypadku realizacji celów wskazanych w art. 89 ust. 1 RODO – powinna dotyczyć wyłączenie zagrożeń, które są związane z realizacją zasady minimalizacji. Wskazany przepis należy raczej traktować podobnie jak art. 25 ust. 2 RODO, jako dodatkowy wymóg szczególnej staranności w zakresie oceny ryzyka i wdrożenia zabezpieczeń, które będą eliminować lub minimalizować ryzyko, którego źródłem może być naruszenie zasady minimalizacji danych.

Q. Uzasadniony interes

Zgodnie z treścią art. 6 ust. 1 lit. f RODO przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków, m.in. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Komentarz:

Brytyjski organ ochrony ICO zwraca uwagę, że elementem testu, którego celem jest weryfikacja istnienia uzasadnionego interesu (tzw. *LIA – legitimate interest assessment*[15]), jest ocena ryzyka naruszenia praw lub wolności związanego z przetwarzaniem danych na podstawie tej przesłanki. ICO wskazuje, że LIA to rodzaj „lekkiej oceny ryzyka", opartej na konkretnym kontekście i okolicznościach. Pomaga zapewnić zgodność przetwarzania z prawem. Rejestrowanie LIA pomaga wykazać zgodność z wymogami wynikającymi z art. 5 ust. 2 i art. 24 RODO. LIA jest narzędziem 35 pytań proponowanym przez ICO, służącym do wsparcia administratorów w podjęciu decyzji, czy w konkretnym przetwarzaniu danych osobowych administrator legitymuje się prawnie uzasadnionym interesem.

[15] ICO, *Legitimate interests*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/.

R. Zmiana celu przetwarzania danych

Zgodnie z art. 6 ust. 4 RODO, jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani prawa Unii lub prawa państwa członkowskiego stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1 RODO, administrator – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – bierze pod uwagę m.in.:

1) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania;
2) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem;
3) charakter danych osobowych, w szczególności to, czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 lub dane osobowe dotyczące wyroków skazujących i czynów zabronionych zgodnie z art. 10;
4) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą;
5) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.

Komentarz:

Artykuł 6 ust. 4 RODO dotyczy testu zgodności celów, czyli mechanizmu zmiany pierwotnego celu zebrania danych i dalszego przetwarzania danych w innym celu (zgodnym). Analiza opinii GR29 (obecnie EROD) dotyczącej *reuse* danych w sektorze publicznym nr 6/2013 (w tym także problemu zmiany celu przetwarzania danych), wskazuje, że kluczowym wymogiem w kontekście zmiany celu przetwarzania danych jest ocena ryzyka naruszenia praw lub wolności. GR29 wskazuje (w pkt 4.2), że: „Uwzględniając potencjalne czynniki ryzyka przy ponownym wykorzystywaniu ISP, w szczególności fakt, że po publicznym udostępnieniu danych osobowych w celu ponownego wykorzystania sprawowanie skutecznej kontroli nad tymi danymi będzie znacznie utrudnione, Grupa Robocza Art. 29 podkreśla konieczność przestrzegania zasad dotyczących «ochrony danych już w fazie projektowania oraz ochrony danych jako opcji domyślnej», a także konieczność odniesienia się do problemów związanych z ochroną danych na wczesnym etapie. W szczególności Grupa Robocza Art. 29 zdecydowanie zaleca, aby organ sektora publicznego przeprowadził dogłębną ocenę skutków w zakresie ochrony danych, zanim udostępni określone dane osobowe do ponownego wykorzystania. Państwa członkowskie powinny również rozważyć wprowadzenie obowiązku przeprowadzania tego rodzaju oceny skutków w ramach przepisów krajowych lub promowanie tej oceny jako najlepszej praktyki. W każdym razie, nawet jeżeli nie zostało to wyraźnie przewidziane w przepisach krajowych, przed ujawnieniem informacji i podjęciem decyzji o udostępnieniu ich

w celu ponownego wykorzystania organy sektora publicznego powinny przeprowadzić dogłębną ocenę w celu ustalenia, czy określone dane osobowe mogą zostać udostępnione do ponownego wykorzystania, a jeżeli mogą, należy ustalić, na jakich warunkach ponowne wykorzystanie jest dozwolone oraz jakie są wymagane konkretne zabezpieczenia służące ochronie danych".

2. Ramy regulacyjne oceny ryzyka – wstępne wnioski

Można sformułować następujące wnioski dotyczące ram regulacyjnych oceny ryzyka:

1) każdy z przepisów RODO dotyczący oceny ryzyka posługuje się tym samym zwrotem w kontekście tej oceny (ryzyko naruszenia praw lub wolności osób fizycznych);
2) ryzyko naruszenia praw lub wolności oceniane jest w różnych kontekstach normatywnych, np. w fazie projektowania, w przypadku naruszenia ochrony danych itp., w każdym jednak przypadku jest częścią procesu zarządzania zgodnością z RODO poprzez ocenę ryzyka;
3) pojęcie ryzyka naruszenia praw lub wolności używane jest w relacji do praw osób, których dane dotyczą (a nie np. ryzyka dla organizacji);
4) żaden z przepisów RODO nie definiuje, czym jest ryzyko naruszenia praw lub wolności osób fizycznych;
5) zgodnie z motywem 76 RODO ryzyko identyfikowane jest w ramach poszczególnych operacji na danych (np. pozyskiwanie danych, usuwanie itp.);
6) ryzyko identyfikowane i szacowane jest przy uwzględnieniu „tła" tej oceny (zgodnie z motywem 76 RODO prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić przez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych);
7) co do zasady adresatem wymogów w zakresie oceny ryzyka naruszenia praw lub wolności jest administrator danych, a niektórych (wyjątkowo) – podmiot przetwarzający (art. 32 i 30 RODO);
8) ryzyko szacowane jest przez pryzmat jego wagi i prawdopodobieństwa;
9) RODO nie definiuje, czym jest waga i prawdopodobieństwo ryzyka naruszenia praw lub wolności;
10) żaden z przepisów RODO nie określa, w jakiej relacji mają pozostawać względem siebie waga i prawdopodobieństwo, aby wynikiem oceny ryzyka była identyfikacja ryzyka lub wysokiego ryzyka naruszenia praw lub wolności;
11) przepisy RODO nie wskazują, jakie negatywne konsekwencje dla praw lub wolności osób fizycznych należy uwzględnić przy ocenie ryzyka – w tym zakresie kluczowe znaczenie mają motywy 75 i 85 RODO;
12) RODO nie przesądza, jakie środki należy wdrożyć na określonym poziomie ryzyka; wskazuje jedynie – w poszczególnych przepisach – że muszą być odpowiednie. W przypadku oceny ryzyka w zakresie bezpieczeństwa (art. 32 RODO) wskazuje tylko przykładowe środki techniczne i organizacyjne (np. szyfrowanie);

13) niektóre przepisy RODO łączą konsekwencje prawne (np. obowiązek poinformowania organu nadzorczego) z wystąpieniem ogólnie ryzyka, a niektóre z wystąpieniem określonego poziomu ryzyka, np. wysokiego ryzyka (np. art. 34 RODO);
14) ocena skutków (art. 35 RODO) jest tylko szczególnym przypadkiem analizy ryzyka, o czym świadczy treść art. 35 ust. 7 RODO;
15) nie ma przepisu RODO, który wyjaśniałby, w jaki sposób ocenę ryzyka powinni przeprowadzać współadministratorzy, kwestię tę należy oceniać przy uwzględnieniu art. 26 RODO[16];
16) niektóre przepisy RODO odwołują się pośrednio do oceny ryzyka, wskazując np. obowiązek weryfikacji adekwatności wdrożonych zabezpieczeń – ocena ryzyka, zgodnie z art. 24, 25 i 32 RODO, jest właśnie „probierzem" weryfikacji adekwatności wdrożonych zabezpieczeń (środków technicznych lub organizacyjnych);
17) RODO nie daje podstaw, aby przyjąć, że administrator może „poświęcić" prawa lub wolności osób, których dane przetwarza, akceptując np. wysokie ryzyko dla praw lub wolności osób, których dane są przetwarzane ze względu na potrzebę ochrony innych wartości/dóbr, np. związanych z bezpieczeństwem narodowym. Takie działanie (w kontrolowalnym przez RODO zakresie) może zostać podjęte wyłącznie na poziomie ustawodawcy (krajowego lub unijnego) – wynika to z treści art. 23 RODO, który daje podstawę do tego, aby aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22, 34, a także w art. 5 RODO – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym m.in.:
    a) bezpieczeństwu narodowemu,
    b) obronie,
    c) bezpieczeństwu publicznemu,
    d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom;
    e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu.

[16] EROD wskazuje, że współadministratorzy muszą uzgodnić m.in. zakres odpowiedzialności, który dotyczy m.in. wdrażania środków odpowiednich do poziomu ryzyka (EROD powołuje w tym kontekście m.in. art. 32, 35 RODO) – EROD, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, s. 41, nb 163.

Tabela 1. Podsumowanie wymogów dotyczących oceny ryzyka w ramach przepisów kluczowych dla systemu ochrony danych i oceny ryzyka

nr	Umiejscowienie przepisu	Podmioty zobowiązane do oceny ryzyka	Cechy charakterystyczne danego typu ryzyka i jego funkcje w ochronie osób fizycznych w związku z przetwarzaniem danych osobowych	Czy przepis odwołuje się do określonego poziomu ryzyka?	Czy przepis odwołuje się do określonego poziomu wagi lub prawdopodobieństwa?	Czy ocena ryzyka dotyczy określonych aspektów, np. bezpieczeństwa?	Do jakich elementów tła oceny ryzyka odwołuje się przepis?
A	art. 24 ust. 1	administrator	• ryzyko rozumiane bardzo szeroko i ogólnie dotyczące całości przetwarzania danych osobowych przez administratora danych; • funkcja: wdrażanie środków (technicznych lub organizacyjnych), aby zapewnić, że administrator będzie przestrzegał przepisów RODO oraz będzie skutecznie realizował prawa przysługujących podmiotom danych	nie	nie	nie	charakter, zakres, kontekst, cele
B	art. 25 ust. 1 i 2	administrator	• ryzyko dotyczy przyszłych procesów przetwarzania, które są projektowane przez administratora; • funkcja: wdrażane środki mają zapewnić, że administrator będzie skutecznie realizował: – zasady ochrony danych określonych m.in. w art. 5 RODO – wymogi RODO – prawa podmiotów danych	nie	nie	nie	charakter, zakres, kontekst, cele + stan wiedzy, koszt wdrożenia
D	art. 32 ust. 1	administrator, podmiot przetwarzający	• ryzyko rozumiane jako kombinacja wagi i prawdopodobieństwa zrealizowania się zagrożeń bezpieczeństwa danych, które dotyczą poufności, dostępności i integralności danych osobowych; • funkcja: wdrażane środki mają zapewnić, że administrator lub podmiot przetwarzający wdrożą środki bezpieczeństwa na odpowiednim poziomie	nie	nie	tak (bezpieczeństwo)	charakter, zakres, kontekst, cele + stan wiedzy, koszt wdrożenia