Paweł Litwiński

Rozdział II. Dokumentowanie procesów przetwarzania danych osobowych

1. Uwagi ogólne

Ustawa o ochronie danych osobowych z 1997 r. przyzwyczaiła administratorów danych osobowych do stosowania systemu środków zabezpieczenia danych opartego na katalogu wymaganych przez prawo, konkretnych rozwiązań. Katalog ten wynikał z DokPrzetwR, a zwłaszcza z załącznika do niego, w którym wskazane zostały szczegółowe wymagania techniczne i organizacyjne, jakie powinny zostać spełnione przy przetwarzaniu danych osobowych. W odbiorze wielu administratorów danych takie rozwiązanie zastosowane przez ustawodawcę spowodowało, że zupełnie bez znaczenia pozostawała ogólna reguła z art. 36 OchrDanychU97, która nakazywała dobór środków zabezpieczenia danych osobowych odpowiednio do zagrożeń oraz kategorii danych objętych ochroną – stosowano się wyłącznie do katalogu obowiązków określonego w rozporządzeniu, traktując go jak swoistą listę kontrolną.

Nie budzi chyba wątpliwości, że takie praktyki administratorów danych powinny zostać ocenione wysoce negatywnie. Sprowadzanie obowiązku zabezpieczenia danych osobowych wyłącznie do wykazu konkretnych rozwiązań, które trzeba zastosować i zastosowanie których wyczerpuje obowiązek zabezpieczenia danych, powodowało, że obowiązek ten stawał się czysto fasadowym, formalnym obowiązkiem podjęcia określonych działań. Bez znaczenia pozostawało przy tym wielokrotnie to, czy te działania doprowadziły do skutecznego zabezpieczenia danych osobowych odpowiednio do zagrożeń oraz kategorii danych objętych ochroną. Tym większym szokiem dla podmiotów przetwarzających dane osobowe w realiach polskich stało się rozpoczęcie stosowania RODO, który to akt prawny opiera się na zupełnie innym podejściu do obowiązku zabezpieczenia danych osobowych. Jest to podejście oparte na ryzyku (ang. *risk based approach*). Podkreślić przy tym należy, że zmiana podejścia do kwestii zabezpieczenia danych osobowych opiera się

w mniejszym stopniu na zmianie treści przepisów, które regulują tę kwestię, a w większym stopniu na wyeliminowaniu z obrotu prawnego DokPrzetwR. To rozporządzenie bowiem, z jego katalogiem środków zabezpieczenia danych, doprowadziło w wielu przypadkach do utraty praktycznego znaczenia przez ogólną regułę zabezpieczenia danych wyrażoną w art. 36 OchrDanychU97.

Podejście oparte na ryzyku zakłada, że dobór środków zabezpieczenia danych osobowych powinien się opierać na:
1) stanie wiedzy technicznej,
2) koszcie wdrażania konkretnych rozwiązań,
3) charakterze, zakresie, kontekście i celach przetwarzania danych osobowych,
4) ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze.

W każdym przypadku to administrator danych powinien więc dokonać wyboru, jakie konkretne rozwiązania w zakresie zabezpieczenia danych zastosuje[1]. Na poziomie samego RODO nie istnieje przy tym żaden, nawet przykładowy, katalog tych środków – z jednym wyjątkiem. Mianowicie zgodnie z art. 24 ust. 2 RODO, jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki techniczne i organizacyjne mające zapewnić, aby przetwarzanie danych odbywało się zgodnie z RODO i aby móc to wykazać, powinny obejmować wdrożenie odpowiednich polityk ochrony danych. Podkreślić jednak należy, że decyzja o wdrożeniu dokumentacji zależy zawsze od woli i decyzji administratora danych[2].

Decyzja o tym, czy wdrożyć dokumentację ochrony danych osobowych, powinna być oparta na regule proporcjonalności – jak wskazuje się w literaturze, zabezpieczenia powinny być odpowiednie, nie chodzi tu jednak o zabezpieczenia najlepsze z możliwych (najnowsze, najdroższe, najbardziej zaawansowane technologicznie), a o takie środki techniczne i organizacyjne, które są proporcjonalne[3] ze względu na:
1) charakter, zakres, kontekst i cele przetwarzania oraz
2) ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze.

Artykuł 36 ust. 2 OchrDanychU97 nakazywał prowadzenie dokumentacji opisującej sposób przetwarzania danych oraz stosowane środki zabezpieczenia danych osobowych, a DokPrzetwR szczegółowo opisywało zawartość tej dokumentacji. **Na gruncie RODO samo wdrożenie dokumentacji zależy już od decyzji administratora danych, a żaden akt prawny nie reguluje zawartości takiej dokumentacji**. Jak więc należy w tej chwili, stosując RODO, podejść do kwestii dokumentacji ochrony danych osobowych?

---

1 Zob. *D. Lubasz*, (w:) RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. *E. Bielak-Jomaa*, *D. Lubasz*, Warszawa 2017, s. 693.

2 Tak *P. Barta*, *M. Kawecki*, *P. Litwiński*, Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, Warszawa 2018, s. 452.

3 Zob. *P. Fajgielski*, Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018, s. 316.

2. Zasada rozliczalności danych osobowych a dokumentacja ochrony danych

Zasada rozliczalności to całkowicie nowe rozwiązanie wprowadzone do systemu prawa przez przepisy RODO. Zasada ta, wyrażona w art. 5 ust. 2 RODO, nakłada na administratorów i podmioty przetwarzające dane osobowe odpowiedzialność za przestrzeganie przepisów dotyczących przetwarzania danych oraz wymaga, aby podmioty te były w stanie to wykazać[4].

Zgodnie z opinią Grupy Roboczej Art. 29 w sprawie zasady rozliczalności (WP 173), obowiązek zapewnienia rozliczalności oznacza:

1) wdrożenie środków (w tym wewnętrznych procedur) gwarantujących przestrzeganie przepisów o ochronie danych w związku z operacjami ich przetwarzania oraz
2) sporządzenie dokumentacji, która wskazuje osobom, których dane dotyczą, oraz organom nadzorczym, jakie środki podjęto, aby zapewnić przestrzeganie przepisów o ochronie danych osobowych[5].

Również w literaturze przedmiotu podkreśla się, że konsekwencją zasady rozliczalności jest, iż w razie sporu z osobą, której dane dotyczą, albo z organem nadzorczym, administrator danych powinien być w stanie przedstawić dowody na to, że przestrzega przepisów o ochronie danych osobowych. Dowodami takimi mogą być przede wszystkim dokumenty opisujące zasady przetwarzania i ochrony danych osobowych. Dlatego też, pomimo braku wyraźnego wymogu wynikającego z przepisów RODO, zasadne i rekomendowane jest prowadzenie dokumentacji przetwarzania danych osobowych[6]. Pozostaje to w zgodzie z motywem 78 RODO, w którym podkreśla się, że celem przyjęcia i wdrożenia przez administratora wewnętrznych polityk oraz wdrożenia odpowiednich środków jest ułatwienie realizacji zasady rozliczalności, a zatem umożliwienia wykazania zgodności z RODO.

Dokumentacja ochrony danych osobowych wdrażana na podstawie RODO, po pierwsze, będzie stanowiła dowód na wdrożenie rozwiązań zapewniających praktyczną realizację zasady rozliczalności. Po drugie, dokumentacja będzie stanowiła środek dowodowy w razie sporu na okoliczność przyjęcia i wdrożenia konkretnych rozwiązań opisanych w dokumentacji. Po trzecie wreszcie, dokumentacja stanowić może doskonały instrument umożliwiający podejmowanie działań edukacyjnych wśród pracowników administratora danych.

Ważne

Mimo braku wprost sformułowanego prawnego obowiązku posługiwania się dokumentacją ochrony danych osobowych, względy czysto praktyczne wskazują na to, że posługiwanie się nią jest bardzo użyteczne, a często wręcz zalecane, jako praktyczny sposób realizacji zasady rozliczalności danych osobowych. Nie jest więc zalecane, by wraz z rozpoczęciem stosowania RODO kończyć

4 Zob. *A. Nerka*, (w:) Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, red. *M. Sakowska-Baryła*, Warszawa 2018, s. 149.
5 Opinia 3/2010 w sprawie zasady rozliczalności (WP 173), s. 9.
6 Zob. *P. Fajgielski*, Ogólne rozporządzenie o ochronie danych..., s. 157.

posługiwanie się dokumentacją ochrony danych osobowych opracowaną i wdrożoną pod rządami OchrDanychU97 – wręcz przeciwnie, rekomendowanym rozwiązaniem jest dostosowanie treści dokumentacji do wymagań RODO i zapewnienie ciągłości jej stosowania w organizacji.

3. Dokumentacja ochrony danych osobowych a przepisy RODO

Ponieważ w przepisach RODO brak jest obowiązku posługiwania się dokumentacją ochrony danych osobowych w znaczeniu, jakie temu pojęciu nadawała OchrDanychU97, a jednocześnie zasada rozliczalności wskazuje, że wdrożenie takiej dokumentacji jest bardzo pożądane, podstawowe pytanie, na jakie należy znaleźć odpowiedź, to pytanie o zawartość dokumentacji ochrony danych osobowych funkcjonującej zgodnie z przepisami RODO.

W celu udzielenia odpowiedzi na to pytanie należy podkreślić, że RODO – choć nie nakazuje wdrożenia dokumentacji ochrony danych osobowych w znaczeniu znanym z OchrDanychU16 – nakazuje wykonać wiele czynności, które zgodnie z zasadą rozliczalności powinny zostać odpowiednio udokumentowane. Są to:

1) rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania, o których mowa w art. 30 RODO,
2) raport z przeprowadzonej ogólnej analizy ryzyka – art. 32 RODO,
3) raport z oceny skutków dla ochrony danych – art. 35 ust. 7 RODO, jeżeli została przeprowadzona.

Co najmniej więc w tym zakresie każdy administrator danych lub podmiot przetwarzający powinni sporządzić odpowiednią dokumentację. Ale to nie wszystko – uwzględniając kolejne obowiązki wynikające z przepisów RODO, w praktyce zaleca się sporządzenie i wdrożenie dokumentacji obejmującej:

1) wytyczne dotyczące klasyfikacji naruszeń i procedurę zgłaszania naruszenia ochrony danych do organu nadzorczego – art. 33 ust. 3 RODO,
2) procedurę na wypadek wystąpienia naruszeń mogących powodować wysokie ryzyko naruszenia praw i wolności osób, w zakresie ich informowania o działaniach, jakie powinni wykonać, aby ryzyko to ograniczyć – art. 34 RODO,
3) procedurę prowadzenia wewnętrznej dokumentacji stanowiącej rejestr naruszeń ochrony danych, o którym mowa w art. 33 ust. 5 RODO,
4) procedury związane z pseudonimizacją i szyfrowaniem, jeżeli zostały wdrożone takie rozwiązania,
5) plan ciągłości działania – art. 32 ust. 1 lit. b RODO,
6) procedury odtwarzania systemu po awarii oraz ich testowania – art. 32 ust. 1 lit. c i d RODO[7].

[7] Dokumentacja przetwarzania danych osobowych zgodnie z RODO, materiał udostępniony na stronie UODO: https://uodo.gov.pl/pl/138/273 (dostęp: 8.11.2018 r.).

Dodatkowo, jak wskazała Grupa Robocza Art. 29 w wytycznych WP 248[8], polityka wewnętrzna administratora danych, może rozszerzyć zakres dokumentacji poza zakres wynikający z przepisów RODO.

4. Dokumentowanie czynności wymaganych przez przepisy RODO

W art. 30 RODO wprowadzono obowiązek prowadzenia przez podmioty przetwarzające dane dwóch rodzajów rejestrów czynności przetwarzania:

1) rejestr czynności przetwarzania administratora (art. 30 ust. 1 RODO),
2) rejestr kategorii czynności przetwarzania podmiotu przetwarzającego (art. 30 ust. 2 RODO).

Zgodnie z art. 30 ust. 1 RODO w rejestrze czynności przetwarzania prowadzonym przez administratora danych osobowych należy zamieścić następujące informacje:

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

Rejestr czynności przetwarzania podmiotu przetwarzającego składa się, co do zasady, z analogicznych elementów, do tych, z których składa się rejestr czynności administratora danych. Podstawową jednak różnicą jest to, że nie odnosi się on do czynności przetwarzania danych, ale kategorii takich czynności przetwarzania, dokonywanych w imieniu administratora. Kategorie czynności przetwarzania to powiązane ze sobą procesy, które administrator decyduje się przekazać podmiotowi przetwarzającemu. Takimi typowymi kategoriami przetwarzań mogą być np. hosting danych (w jego różnych odmianach), serwis z usługą helpdesk, odbiór i niszczenie nośników danych, obsługa rachunkowo-księgowa[9]. Analogicznie wypowiada się również Prezes UODO, wskazując, że „w przypadku rejestru kategorii czynności przetwarzania, poszczególne wpisy (rekordy) tego rejestru

8 Wytyczne WP 248 dotyczące oceny skutków dla ochrony danych (WP 248), s. 21.

9 Zob. *K. Wygoda*, (w:) Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, red. *M. Sakowska-Baryła*, Warszawa 2018, s. 340–341.

powinny być uporządkowane według kategorii przetwarzania, tj. rodzaju usług świadczonych na rzecz administratorów”[10]. W praktyce oznacza to więc, że rejestr kategorii czynności przetwarzania danych może się charakteryzować w tym zakresie mniejszą szczegółowością niż rejestr administratora[11].

Rejestr prowadzony przez podmiot przetwarzający w porównaniu do rejestru prowadzonego przez administratora danych nie zawiera informacji o:
1) celach przetwarzania danych,
2) kategoriach osób, których dane dotyczą, oraz kategoriach danych osobowych,
3) kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione,
4) planowanych terminach usunięcia poszczególnych kategorii danych.

Podmiot przetwarzający powinien jednak umieścić w rejestrze informację o kategoriach przetwarzań (rodzajach czynności przetwarzania) dokonywanych w imieniu każdego z administratorów (art. 30 ust. 2 lit. b RODO).

Określenie poziomu ryzyka naruszenia praw i wolności osób, których dane dotyczą, ma podstawowe znaczenie dla doboru odpowiednich środków technicznych i organizacyjnych mających zapewnić zabezpieczenie danych osobowych, zgodnie z art. 32 RODO.

Ważne

Jako że RODO nie zawiera żadnych przepisów regulujących sposób postępowania w celu dokonania oceny poziomu ryzyka, szczególnego znaczenia w tym zakresie nabierają praktyczne wskazówki opublikowane przez Prezesa UODO, w tym m.in. dokument „Jak rozumieć podejście oparte na ryzyku według RODO? Poradnik RODO. Podejście oparte na ryzyku. Część 1” oraz dokument „Jak stosować podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku. Część 2”[12]. Decyzja o wyborze konkretnej metodologii szacowania poziomu ryzyka została jednak pozostawiona administratorowi danych, który może w tym zakresie skorzystać z innych opracowań niż przygotowane przez organ nadzorczy.

Ocena skutków dla ochrony danych osobowych to proces mający opisać przetwarzanie danych, ocenić niezbędność i proporcjonalność przetwarzania oraz pomóc w zarządzaniu ryzykiem naruszenia praw lub wolności osób fizycznych wynikającym z przetwarzania danych osobowych (oceniając ryzyko i ustalając środki mające mu zaradzić) [13]. Ocena skutków dla ochrony danych to narzędzie istotne dla celów rozliczalności, ponieważ pomagają administratorom nie tylko w przestrzeganiu wymogów RODO, ale również w wykazaniu, że podjęto odpowiednie środki w celu zapewnienia zgodności z RODO (zob. także art. 24 RODO). Innymi słowy, DPIA to proces służący do zapewnienia i wykazania zgodności[14].

10 Wskazówki i wyjaśnienia dotyczące obowiązku rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO, materiał udostępniony na stronie UODO (dostęp: 4.11.2018 r.), s. 13.
11 Tak *P. Barta*, *M. Kawecki*, *P. Litwiński*, Rozporządzenie..., s. 495.
12 Dokumenty dostępne na stronie internetowej https://uodo.gov.pl/pl/123/208.
13 Wytyczne WP 248 dotyczące oceny skutków dla ochrony danych (WP 248), s. 4.
14 Tak *P. Barta*, *M. Kawecki*, *P. Litwiński*, Rozporządzenie..., s. 531.

Ocena skutków dla ochrony danych osobowych powinna zostać wykonana co najmniej w sytuacjach wskazanych w art. 35 ust. 1 i 3 RODO[15]. Jeżeli administrator danych osobowych jest zobowiązany do dokonania oceny skutków, wówczas zgodnie z art. 35 ust. 7 RODO powinien udokumentować przeprowadzenie następujących czynności:

1) sporządzenia systematycznego opisu planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
2) dokonania oceny, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
3) dokonania oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
4) wskazania środków planowanych w celu zaradzenia ryzyku, w tym zabezpieczeń oraz środków i mechanizmów bezpieczeństwa mających zapewnić ochronę danych osobowych i wykazania przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

Podobnie jak w przypadku oceny poziomu ryzyka naruszenia praw i wolność osób, których dane dotyczą, również w przypadku oceny skutków dla ochrony danych osobowych przepisy RODO nie określają metodologii dokonywania takiej oceny. Ocena może więc być przeprowadzana według dowolnej metodologii przyjętej przez administratora, przy czym sam wybór metodologii powinien również stanowić element dokumentacji ochrony danych osobowych tak, by stała się ona częścią strategii zarządzania danymi[16].

5. Dokumentowanie czynności związanych z wykonywaniem obowiązków wynikających z RODO

Jednym z obowiązków wynikających z przepisów RODO, w zakresie którego pożądane jest przygotowanie odpowiedniej dokumentacji, jest obowiązek zgłaszania naruszenia ochrony danych do organu nadzorczego, o którym mowa w art. 33 RODO. Zgodnie z tym przepisem **w przypadku naruszenia ochrony danych osobowych, administrator danych bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza to naruszenie organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych**. Samo zgłoszenie powinno przy tym:

1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

[15] Wykaz operacji przetwarzania, które wymagają dokonania oceny, może zostać także przygotowany przez organ nadzorczy. Taki wykaz w warunkach polskich został przygotowany przez Prezesa UODO i zawarty w komunikacie z 17.8.2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M.P. z 2018 r. poz. 827).

[16] *A. Bensoussan* (red.), *J.F. Henrotte*, *M. Gallardo*, *S. Fanti*, General Data Protection Regulation: texts, commentaries and practical guidelines, Mechelen 2017, s. 201.

2) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
4) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Obowiązek ten sam w sobie wydaje się prosty do spełnienia – w terminie określonym w RODO należy przekazać organowi nadzorczemu wymagane informacje, jeżeli dojdzie do naruszenia ochrony danych osobowych. W praktyce jednak obowiązek zgłaszania naruszeń o tyle tylko ma szansę zadziałać w organizacji, o ile będzie istniała jasna i stosowana przez wszystkich procedura identyfikacji naruszeń i dokonywania samego zgłoszenia. Stąd ze wszech miar celowe jest opracowanie zasad:
1) uznawania określonego zdarzenia za naruszenie ochrony danych osobowych, na podstawie definicji zawartej w art. 4 pkt 12 RODO;
2) dokonywania zgłoszenia zdarzeń uznanych za naruszenie do organu nadzorczego w terminie określonym w RODO, w tym wzoru samego zgłoszenia.

W ramach tych procedur kluczowe jest także zapewnienie współdziałania w ramach organizacji wszystkich zainteresowanych podmiotów, w szczególności IOD.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator danych bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu (art. 34 ust. 1 RODO). W ramach zawiadomienia należy przekazać informacje przekazywane do organu nadzorczego, z wyjątkiem opisu charakteru naruszenia. Zawiadomienie nie jest jednak wymagane, jeżeli zaistniała choćby jedna z następujących okoliczności:
1) administrator danych wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
2) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
3) zawiadomienie wymagałoby niewspółmiernie dużego wysiłku.

Co do dodatkowo istotne, **zawiadomienie powinno być sporządzone jasnym i prostym językiem**.

W literaturze przedmiotu wskazuje się wprost, że takie sformułowanie obowiązku zawiadamiania o naruszeniach może budzić wątpliwości interpretacyjne, zarówno w odniesieniu do tego, kiedy informować, jak i w zakresie kryterium, od spełnienia którego zależy w ogóle powstanie tego obowiązku[17]. Stąd znów wydaje się celowe i zasadne, aby doprecyzować – na potrzeby konkretnej organizacji – zasady wykonywania obowiązku informowania o incydentach osoby, których dane dotyczą. W szczególności należy opracować

[17] Zob. *M. Sakowska-Baryła*, (w:) Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, red. *M. Sakowska-Baryła*, Warszawa 2018, s. 375.

wzór samego zawiadomienia tak, żeby w razie wystąpienia konieczności jego przekazania ograniczyć się wyłącznie do kwestii technicznych.

Niezależnie od tego, czy naruszenie ochrony danych wiązało się z obowiązkiem zawiadomienia organu nadzorczego lub osób, których dane dotyczą, administrator danych osobowych ma prawny obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, ich skutków oraz podjętych działań zaradczych. Jak wprost wskazuje RODO w art. 33 ust. 5, dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania obowiązków związanych ze zgłaszaniem naruszeń. W wykonaniu tego obowiązku administrator danych powinien więc prowadzić wewnętrzny rejestr naruszeń, który powinien zawierać informacje pozwalające na wykazanie w razie kontroli, dlaczego w przypadku konkretnego zaistniałego naruszenia podjęto takie, a nie inne działania. Zasadne więc pozostaje przygotowanie wzoru takiego rejestru i uzupełnianie go w razie występowania naruszeń.

Podejście oparte na ryzyku w zakresie zabezpieczenia danych osobowych wychodzi z założenia, że dobór konkretnych rozwiązań w tym zakresie pozostaje w wyłącznej gestii administratora danych osobowych. Artykuł 32 ust. 1 RODO wskazuje przy tym wyłącznie przykładowe środki techniczne i organizacyjne, które mogą służyć osiągnięciu celu w postaci zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku. Są nimi w szczególności:

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

Stosowna dokumentacja powinna więc – w duchu zasady rozliczalności – opisywać stosowane rozwiązania w tym zakresie, a także procedurę ich wdrożenia w konkretnych przypadkach. Nie można także zapominać o konieczności wykazania w razie konieczności, dlaczego podjęto decyzję o zastosowaniu konkretnych środków technicznych i organizacyjnych, a innych nie zastosowano – również w tym zakresie środkiem umożliwiającym wykazywanie zgodności powinna być odpowiednia dokumentacja.

Podkreślenia wreszcie wymaga, że **chociaż realizacja obowiązków związanych z zabezpieczeniem danych osobowych na gruncie RODO nie jest związana ze sformułowanym wprost w RODO obowiązkiem prowadzenia szczególnej, związanej z tym dokumentacji, to na zasadzie art. 24 ust. 2 RODO w związku z realizacją zasady rozliczalności (art. 5 ust. 2 RODO), administrator danych powinien rozważyć zastosowanie środka w postaci wprowadzenia dokumentacji ochrony danych jako autonomicznego dokumentu lub polityki**[18]. Oczywiście oceny zasadności zastosowania takiego rozwiązania dokonuje administrator danych, ale reguła wynikająca z art. 24 ust. 2 RODO jest w tym zakresie jasna – środki techniczne i organizacyjne mające zapewnić, aby przetwarzanie danych odbywało się zgodnie z RODO i aby móc to wykazać, powinny

[18] Zob. *D. Lubasz*, (w:) RODO..., s. 705.

obejmować wdrożenie odpowiednich polityk ochrony danych, jeżeli jest to „proporcjonalne w stosunku do czynności przetwarzania".

6. Dokumentacja przetwarzania danych a *privacy by design*

Uwzględnianie ochrony danych w fazie projektowania to zupełnie nowy obowiązek związany z przetwarzaniem danych osobowych, wprowadzone przez RODO. Zasada *privacy by design* sprowadza się do konieczności spełnienia przez administratora danych dwóch obowiązków. Pierwszy wymaga uwzględniania ochrony danych w fazie projektowania, czyli „podjęcia działań 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 (...)". Drugi wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania (domyślna ochrona danych)[19]. Rezultatem realizacji tego obowiązku powinno być spełnienie wymogów RODO oraz ochrona praw osób, których dane dotyczą. Podkreślić przy tym należy, że obowiązek ten aktualizuje się już na etapie projektowania sposobów przetwarzania danych (czyli podejmowania działań na przyszłość – gdy dane nie są jeszcze przetwarzane) i trwa przez cały okres ich przetwarzania. Oznacza to, że będzie miał on charakter dynamiczny[20].

W praktyce zasadę *privacy by design* można rozumieć w ten sposób, w jaki to zostało zaproponowane w rezolucji w sprawie prywatności w fazie projektowania, dokumencie 32 Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności[21]. Wyjaśniono w nim, że określenie „Prywatność w Fazie Projektowania" odnosi się do pewnej filozofii i podejścia opartego na włączaniu prywatności w projektowanie, działanie i zarządzanie technologiami informacyjnymi i systemami przez cały cykl życia informacji. W rezolucji wskazano również zasady podstawowe w odniesieniu do prywatności w fazie projektowania. Są nimi:

1) podejście proaktywne, niereaktywne i zaradcze, nienaprawcze,
2) prywatność jako ustawienie domyślne,
3) prywatność włączona w projekt,
4) pełna funkcjonalność: suma dodatnia, nie suma zerowa,
5) ochrona od początku do końca cyklu życia informacji,
6) widoczność i przejrzystość,
7) poszanowanie dla prywatności użytkowników[22].

19 Zob. *K. Wygoda*, (w:) Ogólne rozporządzenie o ochronie danych..., s. 292–293.
20 Zob. *P. Barta*, *M. Kawecki*, *P. Litwiński*, Rozporządzenie..., s. 455.
21 Jerozolima, 27–29.10.2010 r., http://www.giodo.gov.pl/pl/1520084/3830 (dostęp: 8.11.2018 r.).
22 Szerzej na ten temat zob. *P. Barta*, *M. Kawecki*, *P. Litwiński*, Rozporządzenie..., s. 454 i n.; *D. Lubasz*, *K. Witkowska-Nowakowska*, (w:) RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. *E. Bielak-Jomaa*, *D. Lubasz*, Warszawa 2017, s. 600 i n.

Oczywiście zgodnie z zasadą rozliczalności, administrator danych powinien przestrzegać zasady *privacy by design* i mieć możliwość wykazania tego w razie konieczności. Odpowiednia dokumentacja projektowania procesów przetwarzania danych osobowych jest w tym zakresie właściwym narzędziem. Dokumentacja taka powinna w szczególności wykazywać spełnienie postulatu prywatności włączonej w projekt, np. przez udział IOD w projekcie.

7. Dokumentacja wynikająca z RODO

Z powyższych rozważań wyłania się obraz dokumentacji ochrony danych osobowych zgodnej z RODO, na którą składają się następujące elementy:

1) polityka ochrony danych jako samodzielny środek mający zapewnić, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać;
2) dokumenty wymagane przez RODO, tj.:
   a) rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania,
   b) raport z przeprowadzonej ogólnej analizy ryzyka,
   c) raport z ocen skutków dla ochrony danych, jeżeli została przeprowadzona;
3) dokumenty związane z wykonywaniem obowiązków wynikających z RODO, tj.:
   a) procedura wykonywania obowiązków związanych ze zgłaszaniem naruszeń ochrony danych i ewidencjonowaniem naruszeń,
   b) procedury związane z doborem i stosowaniem konkretnych środków zabezpieczenia danych osobowych.

Ponieważ w przepisach RODO nie wskazano, jaka powinna być treść polityki ochrony danych, część – albo nawet wszystkie – wymagane i sugerowane dokumenty można połączyć w całość, jako elementy polityki. Załącznikami do takiego dokumentu powinny być natomiast wzory i formularze, np. w zakresie zgłaszania naruszenia ochrony danych czy prowadzenia rejestru czynności przetwarzania.

8. Wzory dokumentów

8.1. Wzór rejestru czynności przetwarzania

REJESTR CZYNNOŚCI PRZETWARZANIA

Imię i nazwisko lub nazwa oraz dane kontaktowe Administratora Danych		
Imię i nazwisko lub nazwa oraz dane kontaktowe Inspektora Ochrony Danych Osobowych		
Opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych		
Cele przetwarzania danych osobowych		

Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych		
Informacja o przekazywaniu danych osobowych do państwa trzeciego		
Planowane terminy usunięcia poszczególnych kategorii danych		
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa		

8.2. Wzór rejestru naruszeń ochrony danych

REJESTR NARUSZEŃ OCHRONY DANYCH

1.	**Miejsce i dzień naruszenia**		
	Rodzaj naruszenia	**Naruszenie ochrony danych osobowych, które nie podlega zgłoszeniu organowi nadzorczemu** (naruszenie ochrony danych osobowych nie spowodowało ryzyka naruszenia praw i wolności osób fizycznych)	□
		Naruszenie, o którym trzeba zawiadomić zarówno organ nadzorczy, jak i osobę, której dane dotyczą (naruszenie ochrony danych osobowych spowodowało wysokie ryzyko naruszenia praw lub wolności osób fizycznych)	□
		Naruszenie podlegające zgłoszeniu jedynie organowi nadzorczemu (jest mało prawdopodobne, aby naruszenie skutkowało wysokim ryzykiem naruszenia praw lub wolności osób fizycznych)	□
		Naruszenie podlegające zgłoszeniu jedynie organowi nadzorczemu (naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, jednak zawiadomienie osoby, której dane dotyczą, nie jest konieczne ze względu na wypełnienie przesłanek: 1) Administrator Danych Osobowych wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych; 2) Administrator Danych Osobowych zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;	□

		3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku ADO wydaje publiczny komunikat lub stosuje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób).	
	Kategoria i przybliżona liczba osób, których dane dotyczą		
	Kategorie i przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie		
	Okoliczności naruszenia ochrony danych osobowych		
	Skutki naruszenia ochrony danych osobowych		
	Podjęte działania zaradcze		
	Dzień zgłoszenia incydentu naruszenia ochrony danych osobowych organowi nadzorczemu (*jeżeli dotyczy*)		
	Dzień zawiadomienia osób, których dane dotyczą (*jeżeli dotyczy*)		

8.3. Wzór zgłoszenia naruszenia ochrony danych

Prezes Urzędu Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa

ZGŁOSZENIE INCYDENTU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Działając na podstawie art. 33 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 2016 Nr 119, s. 1), dalej: RODO, niniejszym zgłaszam zajście incydentu naruszenia ochrony danych osobowych.

Dane Administratora Danych Osobowych	
Imię i nazwisko Inspektora Ochrony Danych Osobowych oraz dane kontaktowe	

Miejsce i dzień naruszenia	
Kategoria i przybliżona liczba osób, których dane dotyczą	
Kategorie i przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie	
Opis charakteru naruszenia ochrony danych	
Możliwe konsekwencje naruszenia ochrony danych	
Środki zastosowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych	

.....

(*podpis osoby uprawnionej*
do reprezentowania Administratora Danych)

Podstawa prawna:

- motyw 78, art. 4 pkt 12, art. 5 ust. 2, art. 24, 30, 32–35 RODO.