



# Dokumentacja przetwarzania danych osobowych zgodnie z RODO

# SPIS TREŚCI

Co musi obejmować dokumentacja.....	2
Kiedy dokumentacja będzie spełniała wymagania RODO.....	3
Co z dotychczasową dokumentacją .....	3
Czy dokumentacja przetwarzania zgodnie z RODO powinna zawierać instrukcję zarządzania systemami informatycznymi .....	5
Uzupełnienie dotychczasowej dokumentacji .....	6

## **Od 25 maja 2018 r. – jak informuje Urząd Ochrony Danych Osobowych – z uwagi rozpoczęcie stosowania RODO oraz wejście w życie nowej ustawy o ochronie danych osobowych tracą moc wcześniej obowiązujące wymagania dotyczące dokumentacji przetwarzania danych osobowych. W jaki sposób prowadzić dokumentację według nowych zasad?**

Obecnie prowadzona dokumentacja ochrony danych osobowych powinna być zgodna z wymogami rozporządzenia Parlamentu Europejskiego i Rady (UE) z 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, RODO) i ustawy z 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000). W dokumentacji trzeba również uwzględnić wymogi przepisów branżowych, m.in.:

- rozporządzenia ministra zdrowia z 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania,
- rozporządzenia ministra nauki i szkolnictwa wyższego z 16 września 2016 r. w sprawie dokumentacji przebiegu studiów,
- rozporządzenia ministra edukacji narodowej w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji,
- rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 536/2014 z 16 kwietnia 2014 r. w sprawie badań klinicznych produktów leczniczych stosowanych u ludzi oraz uchylenia dyrektywy 2001/20/WE.

Ani przepisy krajowe, ani RODO nie zawierają praktycznie żadnych wytycznych odnoszących się do sposobu prowadzenia dokumentacji przetwarzania danych osobowych, jak również jej zawartości. Nie oznacza to jednak, że po 25 maja 2018 r. administrator danych nie musi prowadzić żadnej

dokumentacji w tym zakresie – informuje Urząd Ochrony Danych Osobowych (UODO). RODO nie określa formalnych wymagań dotyczących dokumentacji przetwarzania danych osobowych, jednak daje dużą swobodę w tym zakresie.

Zdaniem UODO po 25 maja 2018 r. administrator danych wciąż powinien prowadzić dokumentację, w której będą określone zasady i procedury dotyczące przetwarzania danych osobowych zgodnie z przyjętymi rozwiązaniami prawnymi, organizacyjnymi i technicznymi.

## CO MUSI OBEJMOWAĆ DOKUMENTACJA

RODO wskazuje, jakie kwestie należy uregulować w dokumentacji, są to:

- prowadzenie rejestru czynności przetwarzania i zakres rejestru kategorii czynności przetwarzania, o których mowa w art. 30 RODO;
- zgłaszanie naruszeń ochrony danych do organu nadzorczego (UODO) – art. 33 ust. 3 RODO;
- prowadzenie wewnętrznej dokumentacji stanowiącej rejestr naruszeń ochrony danych, o którym mowa w art. 33 ust. 5 RODO;
- zawartość raportu dokumentującego wyniki przeprowadzonych ocen skutków dla ochrony danych – art. 35 ust. 7.

RODO nie wymaga jednak, aby dokument zawierający te obligatoryjne elementy dokumentacji miał określoną nazwę czy strukturę. Ważne jest tylko, aby administrator danych wykazał, że ma te rejestry czy raporty i aby ich zawartość była zgodna z wymaganiami art. 30, art. 33 ust. 3 i 5 oraz art. 35 ust. 7 RODO. Nie są to jednak jedyne wymagania, które należy uwzględnić w dokumentacji. Administrator danych powinien wziąć też pod uwagę art. 24 RODO, zgodnie z którym, „uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądowi i uaktualniane”. Takimi środkami może być opracowanie polityk ochrony danych, stosowanie zatwierdzonych kodeksów postępowania lub uzyskanie certyfikatu.

Zdaniem UODO administrator powinien uregulować w dokumentacji sposób przetwarzania danych, związane z nim procedury i zastosowane zabezpieczenia techniczne i organizacyjne, aby wykazać, że przestrzega wymagań RODO.

# KIEDY DOKUMENTACJA BĘDZIE SPEŁNIAŁA WYMAGANIA RODO

Dzięki dokumentacji administrator powinien być w stanie wykazać, że:

- a) stosuje się do ogólnych zasad przetwarzania określonych w art. 5 RODO,
- b) zapewnia, aby dane przetwarzane były zgodnie z prawem – art. 6–11 RODO,
- c) zapewnia, aby przestrzegane były prawa osób, których dane są przetwarzane – art. 12–23 RODO,
- d) zapewnia wypełnianie ogólnych obowiązków w zakresie przetwarzania danych ciążących na administratorze i podmiocie przetwarzającym – art. 24–31 RODO,
- e) zapewnia bezpieczeństwo przetwarzania danych, uwzględniając charakter zakres, kontekst i cele przetwarzania danych – art. 32–36 RODO,
- f) zapewnia kontrolę nad przetwarzaniem danych poprzez monitorowanie przestrzegania przepisów i przyjętych procedur przetwarzania przez inspektora ochrony danych lub podmioty certyfikujące czy monitorujące przestrzeganie przyjętych kodeksów postępowania – art. 27–43,
- g) stosuje się do wymagań w zakresie przekazywania danych do państw trzecich i instytucji międzynarodowych – art. 44–49 RODO.

Zgodnie z art. 24 oraz art. 32 RODO przy wykonywaniu tych obowiązków w zakresie zapewniania zgodności należy uwzględniać stan wiedzy technicznej, koszty, charakter, zakres, kontekst, cele przetwarzania, a także ryzyka, na jakie są narażone przetwarzane dane.

## CO Z DOTYCHCZASOWĄ DOKUMENTACJĄ

Obecnie prowadzona dokumentacja, na którą składają się polityka bezpieczeństwa i instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, z powodzeniem może być wykorzystana w celu stworzenia dokumentacji, której celem będzie wykazanie zgodności realizowanych procesów przetwarzania z wymaganiami RODO. Obowiązek wykazania przestrzegania stosowania przepisów RODO wynikający z art. 24 RODO nie określa bowiem, w jaki sposób, poprzez jakie dokumenty czy inne instrumenty zarządzania powinien być zrealizowany. Przepis art. 24 RODO stanowi jedynie, że administrator ma wykazać, że wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO.

Jeśli zatem prowadzona według dotychczas obowiązujących wymagań dokumentacja zawierała wymagane elementy, takie jak inwentaryzacja zasobów informacyjnych, opis przepływu danych między systemami czy specyfikacje środków organizacyjnych i technicznych zastosowanych do ochrony przetwarzanych danych, czego wymagała polityka bezpieczeństwa, to w pełni można je przenieść do nowej dokumentacji.

Nie ma również przeszkód, aby uzupełnić dotychczas stosowaną dokumentację o nowe elementy wymienione w rozdziale 1, takie jak:

- rejestr czynności przetwarzania i zakres rejestru kategorii czynności przetwarzania, o których mowa w art. 30 RODO;
- procedury dotyczące zgłaszania naruszeń ochrony danych do organu nadzorczego (UODO) – art. 33 ust. 3 RODO;
- procedury dotyczące prowadzenia wewnętrznego rejestru naruszeń ochrony danych, o którym mowa w art. 33 ust. 5 RODO;
- raporty dokumentujące wyniki przeprowadzonych ocen skutków dla ochrony danych – art. 35 ust. 7

– jeśli zgodnie z przepisami RODO są wymagane.

Dokumentując przyjęte procedury i wymagania dotyczące przetwarzania danych osobowych, zgodnie z art. 32 ust. 1 RODO, powinniśmy mieć na uwadze, aby przyjęte rozwiązania były adekwatne do obecnego stanu wiedzy technicznej. Dotyczy to nie tylko wiedzy technicznej w zakresie dostępnych środków bezpieczeństwa, ale również wiedzy w zakresie systemów zarządzania bezpieczeństwem, do którego należą takie elementy jak standardy w zakresie zarządzania, dokumentowania zmian, konfiguracji i innych elementów, które powinny być zawarte w dokumentacji przetwarzania.

Należy pamiętać również o innych obowiązujących wymaganiach prawnych określonych w takich przepisach jak:

- ustawa z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jedn.: Dz.U. z 2014 r. poz. 1114) oraz wydane do niej
- rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tekst jedn.: Dz.U. z 2016 r. poz. 113).

# CZY DOKUMENTACJA PRZETWARZANIA ZGODNIE Z RODO POWINNA ZAWIERAĆ INSTRUKCJĘ ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

RODO nie określa wprost, jak należy udokumentować organizację przetwarzania i zarządzanie bezpieczeństwem przetwarzanych danych, w tym nie nakazuje prowadzenia instrukcji zarządzania systemami informatycznymi. Wymaga jednak, aby zastosowane środki bezpieczeństwa i wszystkie podejmowane w tym zakresie działania można było wykazać.

Ponadto obowiązek prowadzenia dokumentacji przetwarzania danych wynika pośrednio również z art. 32 RODO dotyczącego bezpieczeństwa przetwarzania, który stanowi, że uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

UODO wskazuje, że jednym z najważniejszych, powszechnie akceptowanych dokumentów prezentujących aktualny stan wiedzy technicznej w zakresie stosowania środków bezpieczeństwa i zarządzania bezpieczeństwem są m.in. normy ISO/IEC z serii 27000, w tym: norma PN-EN ISO/IEC 27001:2017 Technologia informacyjna – Techniki zabezpieczeń, oraz norma PN-EN ISO/IEC 27002:2017 Technika informatyczna – Technika bezpieczeństwa – Praktyczne zasady zabezpieczania informacji. Wyraźnie podkreśla się w nich, że polityka bezpieczeństwa informacji powinna być dostępna w formie udokumentowanej informacji, ogłoszona wewnątrz organizacji oraz dostępna dla zainteresowanych stron, jeśli jest to właściwe.

Zgodnie z art. 24 i 32 RODO opracowana polityka bezpieczeństwa powinna uwzględniać zakres, kontekst i cele przetwarzania oraz ryzyka naruszenia praw i wolności, w tym prawdopodobieństwo ich wystąpienia. Można się tu posłużyć normą PN-EN ISO/IEC 27002:2017, która zaleca w tym zakresie uwzględnić takie elementy, jak:

- zarządzanie aktywami (przetwarzanymi zbiorami danych),
- kontrole dostępu (rejestrwanie i wyrejestrowywanie użytkowników, zarządzanie hasłami, użycie uprzywilejowanych programów narzędziowych),
- środki ochrony kryptograficznej (polityka stosowania zabezpieczeń, zarządzanie kluczami),

- bezpieczeństwo fizyczne i środowiskowe oraz bezpieczeństwo eksploatacji (zarządzanie zmianami, zarządzanie pojemnością, zapewnienie ciągłości działania, rejestrowanie zdarzeń i monitorowanie),
- bezpieczeństwo komunikacji (zabezpieczenie, rozdzielanie sieci),
- pozyskiwanie, rozwój i utrzymywanie systemów,
- relacje z dostawcami (umowy, w tym umowy powierzenia przetwarzania),
- zarządzanie incydentami związanymi z bezpieczeństwem informacji,
- zarządzanie ciągłością działania,
- zgodność z wymaganiami prawnymi i umownymi.

Część z tych elementów, zgodnie z obowiązującymi dotychczas wymaganiami, powinna być zawarta w instrukcji zarządzania systemami informatycznymi. Elementy te również można wykorzystać w nowej dokumentacji, aby wykazać zgodność z RODO.

## UZUPEŁNIENIE DOTYCHCZASOWEJ DOKUMENTACJI

Nowa, zgodna z RODO dokumentacja powinna uwzględniać takie elementy, jak:

- rejestr czynności przetwarzania i zakres rejestru kategorii czynności przetwarzania,
- wytyczne dotyczące klasyfikacji naruszeń i procedurę zgłaszanie naruszenie ochrony danych do organu nadzorczego (UODO);
- procedurę na wypadek wystąpienia naruszeń mogących powodować wysokie ryzyko naruszenia praw i wolności osób,
- procedurę prowadzenia wewnętrznej dokumentacji stanowiącej rejestr naruszeń ochrony danych,
- raport z przeprowadzonej ogólnej analizy ryzyka,
- raport z ocen skutków dla ochrony danych,
- procedury związane z pseudonimizacją i szyfrowaniem,
- plan ciągłości działania,
- procedury odtwarzania systemu po awarii oraz ich testowania.

Źródło:

- Urząd Ochrony Danych Osobowych, „Dokumentacja przetwarzania danych osobowych zgodnie z RODO”, dostęp: 1 czerwca 2018 r.

**Autor:**

**Wioleta Szczygielska**

specjalista z zakresu ochrony danych osobowych



# STOPKA REDAKCYJNA

Redaktor: Joanna Banasiak-Lach

ISBN: 978-83-269-7785-5

E-book nr: 2HH0802

Firma: Wiedza i Praktyka sp. z o.o.

Adres: 03-918 Warszawa, ul. Łotewska 9a

Kontakt: Telefon 22 518 29 29, faks 22 617 60 10, e-mail: *cok@wip.pl*

NIP: 526-19-92-256

Numer KRS: 0000098264 – Sąd Rejonowy dla m.st. Warszawy, Sąd Gospodarczy  
XIII Wydział Gospodarczy Rejestrowy. Wysokość kapitału zakładowego:  
200.000 zł, Nr rejestrowy BDO: 000008579

Copyright by: Wiedza i Praktyka sp. z o.o. Warszawa 2018