Ocena skutków dla ochrony prywatności

METODYKA

Privacy Impact Assessment (PIA)

METHODOLOGY

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

February 2018 edition

Nieoficjalne tłumaczenie na język polski, wersja 0.2 (robocza)

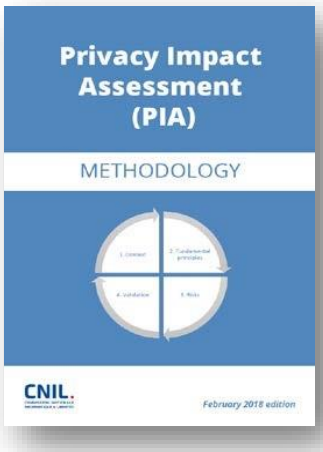
Spis treści

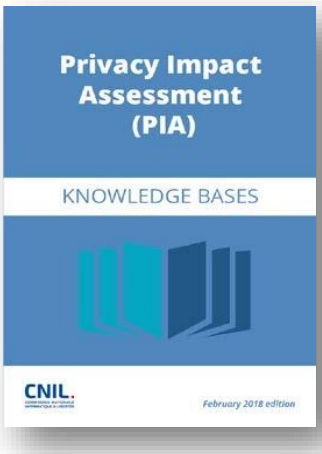
Przedmowa

Metodyka francuskiego krajowego organu ds. ochrony danych (CNIL) obejmuje trzy wytyczne: pierwszą określającą podejście *(przyp. tłum.: metodyka, ang. methodology)*, drugą zawierającą szablony *(przyp. tłum.: ang. templates)*, które mogą być wykorzystane do sformalizowania analizy oraz trzecią dostarczającą bazę wiedzy *(przyp. tłum.: ang. knowledge bases)* (katalog środków/mechanizmów kontrolnych przeznaczonych do zapewnienia zgodności z przepisami prawa, postępowania z ryzykiem oraz przykłady).

Wytyczne mogą być pobrane ze strony CNIL:

https://www.cnil.fr/en/privacy-impact-assessments-cnil-publishes-its-pia-manual





Konwencja pisania przywoływanych dokumentów:

- pojęcie „prywatność” używane jest jako skrót określający wszystkie podstawowe prawa i wolności (w szczególności wymienione w [RODO], w Artykułach 7 i 8 [Karty UE] i Artykule 1 [DP-Act]: „prywatność, tożsamość, prawa człowieka oraz wolności osobiste lub obywatelskie") *(przyp. red.: przywoływany fragment pochodzi z [DP-Act], w Polsce odpowiednikiem jest [Ustawa z 10 maja 2018 r. o ochronie danych osobowych], nie zawiera ona jednak adekwatnych zapisów)*;
- akronim „PIA” jest stosowany zamiennie *(przyp. red.: równoważnie)* zarówno do oceny skutków dla ochrony prywatności (ang. *Privacy Impact Assessment*) jak i do oceny skutków dla ochrony danych (ang. *Data Protection Impact Assessment*, DPIA);
- sformułowania w nawiasach kwadratowych ([tytuł]) korespondują z materiałami źródłowymi.

Wprowadzenie

Niniejsze wytyczne wyjaśniają sposób zrealizowania oceny skutków dla ochrony danych (ang.: *Data Protection Impact Assessment, DPIA*) (patrz art. 35 [RODO]), która często określana jest jako ocena skutków dla ochrony prywatności (ang. *Privacy Impact Assessment, PIA*).

Niniejsze wytyczne opisują sposób użycia metodyki [EBIOS][1] w kontekście specyficznym dla „Ochrony danych osobowych". Podejście to jest zgodne z kryteriami [Wytyczne WP29] (patrz mapowanie spełnienia kryteriów w załączeniu) oraz jest zgodne z międzynarodowymi standardami zarządzania ryzykiem (takimi jak [ISO 31000]).

Przedstawiona metodyka jest iteracyjna, powinna zapewnić uzasadnione i wiarygodne wykorzystanie danych osobowych w trakcie przetwarzania.

Metodyka nie wskazuje warunków determinujących potrzebę przeprowadzenia lub nieprzeprowadzenia PIA (patrz art. 35 ust. 1 [RODO]) lub warunków determinujących konieczność przeprowadzenia konsultacji z organem nadzorczym (patrz art. 36 ust. 1 [RODO]).

PIA zasadniczo wykonywana przez Administratora Danych Osobowych, przeznaczona jest do opracowania i wykazania realizacji zasad ochrony prywatności w taki sposób, by osoby których dane dotyczą *(przyp. red.: podmioty danych)* zachowały kontrolę nad swoimi danymi.

Metodyka przeznaczona jest dla Administratorów Danych Osobowych, którzy chcą wykazać podejście do zapewnienia zgodności i wybrane przez nich środki *(przyp. red: mechanizmów kontrolnych, ang. controls)* (koncepcja odpowiedzialności, patrz art. 25 [RODO]), a także dostawców produktów chcących wykazać, że ich rozwiązanie nie narusza prywatności dzięki uwzględnieniu wymagań zapewniania prywatności na etapie projektowania (koncepcja uwzględnienia ochrony danych w fazie projektowania, patrz art. 25 [RODO])[2]. Metodyka przydatna jest dla wszystkich osób zaangażowanych w tworzenie lub doskonalenie metod przetwarzania danych osobowych lub produktów *(przyp. red.: służących przetwarzaniu danych)*:

- organów decyzyjnych, które zlecają lub zatwierdzają tworzenie nowych metod przetwarzania danych osobowych lub produktów;
- właścicieli projektów, którzy muszą przeprowadzić szacowanie ryzyka dla swoich systemów oraz zdefiniować cele bezpieczeństwa;
- głównych wykonawców, którzy muszą zaproponować rozwiązania adresujące ryzyka zgodnie z celami zidentyfikowanymi przez właścicieli projektów;
- Inspektorów Ochrony Danych (IOD), którzy muszą wspierać właścicieli projektów oraz organy decyzyjne w obszarze ochrony danych osobowych;
- Dyrektorów ds. bezpieczeństwa informacji *(ang. Chief Information Security Officers, CISO)*, którzy muszą wspierać właścicieli projektów w zakresie bezpieczeństwa informacji (BI).

[1] EBIOS – (fr. *Expression des Besoins et Identification des Objectifs de Sécurité*, ang. *Expression of Needs and Identification of Security Objectives*) Wyrażanie potrzeb i identyfikacja celów bezpieczeństwa – nazwa metodyki zarządzania ryzykiem opublikowanej przez francuską Krajową Agencję ds. Cyberbezpieczeństwa (ANSSI, fr. *Agence Nationale de la Sécurité des Systèmes d'Information*, ang. *French National Cybersecurity Agency*).

[2] W pozostałej części dokumentu termin „przetwarzanie danych osobowych" jest stosowany zamiennie (tożsamo) z terminem „produkt".

Jak przeprowadzać PIA?

Zapewnienia zgodności wdrażane poprzez przeprowadzenie PIA, bazuje na dwóch filarach:

1. **podstawowych prawach i zasadach**[3], które są „nienegocjowalne", ustanowione przez prawo, które muszą być przestrzegane niezależnie od rodzaju, wagi i prawdopodobieństwa ryzyka;
2. **zarządzaniu ryzykiem dla prywatności osób, których dane dotyczą**[4], determinującym środki (mechanizmy kontrolne) techniczne i organizacyjne dla ochrony danych osobowych[5].

Rysunek 1 Zapewnienie zgodności z wykorzystaniem PIA

Podsumowując, dla przeprowadzenia PIA niezbędnie należy:

1. zdefiniować i opisać **kontekst** rozważanego przetwarzania danych osobowych;
2. przeanalizować środki gwarantujące zgodność z **podstawowymi zasadami**: zasadą proporcjonalności i niezbędności przetwarzania oraz ochrony praw osób, których dane dotyczą;
3. oszacować **ryzyka** prywatności związane z bezpieczeństwem danych i zapewnić właściwe postępowanie z ryzykiem;
4. formalnie udokumentować **zatwierdzenie** PIA mając na uwadze wcześniej zebrane informacje lub podjąć decyzję o korekcie poprzednich kroków.

Rysunek 2 Ogólne podejście do przeprowadzenia PIA

Działania realizowane są w procesie ciągłego/ustawicznego doskonalenia. W związku z tym, czasem wymagane jest przeprowadzenie kilku iteracji zanim zostanie osiągnięty akceptowalny system ochrony prywatności. Wymagane jest również

[3] Konkretne, wyraźne i prawnie uzasadnione cele; adekwatne, stosowne i nienadmierne dane; jasna i pełna informacja dla osób, których dane dotyczą; ograniczony okres przechowywania; prawo do dostępu, sprzeciwu, sprostowania i usunięcia danych, itd.

[4] Związanym z bezpieczeństwem danych osobowych oraz wpływającym na prywatność osób, których dane dotyczą.

[5] W celu "podjęcia wszelkich użytecznych środków ostrożności, w odniesieniu do charakteru danych i ryzyka związanego z przetwarzaniem, dla zachowania bezpieczeństwa danych, w szczególności zapobiegania ich zmianie i zniszczeniu lub dostępowi przez nieupoważnione osoby trzecie" (Artykuł 34 [DP-Act]) *(przyp. red: przywoływany fragment pochodzi z [DP-Act], w Polsce odpowiednikiem jest Ustawa z 10 maja 2018 r. o ochronie danych osobowych, niemniej zapisy ustaw nie pokrywają się)*.

monitorowanie zmian pojawiających się wraz z upływem czasu (w zakresie kontekstu, zastosowanych środków, ryzyk, itp.), np. corocznie oraz zawsze w przypadku znaczących zmian.

PIA powinno być zrealizowane zawsze w przypadku projektowania nowych metod przetwarzania danych osobowych. Wdrożenie adekwatnego podejścia na samym początku, pozwala określić niezbędne i wystarczające środki, a tym samym optymalizować koszty. Działając przeciwnie, wdrażając środki ochrony po wytworzeniu systemu i wdrożeniu mechanizmów kontrolnych, może doprowadzić do zakwestionowania dokonanych wyborów.

1 Badanie kontekstu

Zazwyczaj przeprowadzane przez właściciela projektu[6], z pomocą osoby odpowiedzialnej za aspekty „ochrony danych”[7].

Cel: uzyskać jasny opis rozważanych operacji przetwarzania danych osobowych.

1.1 Przegląd

- Przedstaw zarys rozpatrywanego **przetwarzania danych**, jego **charakter**, **zakres**, **kontekst**, **cele** i **interes**[8].
- Zidentyfikuj **Administratora Danych Osobowych** i wszystkich **procesorów** (podmioty przetwarzające).
- Wymień **odniesienia** *(przyp. red.: np. przepisy prawa)* dotyczące przetwarzania, których przestrzeganie jest konieczne lub musi być dla nich zachowana zgodność[9], w szczególności zatwierdzone kodeksy postępowania (patrz art. 40 [RODO]) i certyfikaty dotyczące ochrony danych (patrz art. 42 [RODO])[10].

1.2 Dane, procesy i aktywa wspierające

- Zdefiniuj i opisz szczegóły zakresu:
  1. **dane osobowe**, które mają być objęte przetwarzaniem, ich **odbiorców** i **okresy przechowywania**;
  2. opis **przetwarzania** oraz **aktywa** wspierające przetwarzanie w całym cyklu życia danych osobowych (od ich zebrania do ich usunięcia).

[6] W sensie biznesowym. Może to być delegowane, przekazane reprezentantowi lub zrealizowane przez innego interesariusza.
[7] Takim jak np. Inspektor Ochrony Danych.
[8] Odpowiedz na pytanie „Jakie są oczekiwane korzyści (dla organizacji, osób, których dane dotyczą, ogólnie dla społeczeństwa, itd.)?”.
[9] Zależnie od przypadku, będą one szczególnie przydatne do wykazania zgodności z podstawowymi zasadami, uzasadnienia środków lub udowodnienia, że są one zgodne z aktualnym stanem techniki.
[10] Inne przykłady: polityka bezpieczeństwa, sektorowe standardy prawne, itp..

2 Badanie podstawowych zasad

Zazwyczaj realizowane przez właściciela projektu, a następnie oceniane przez osobę odpowiedzialną za aspekty „ochrony danych".

Cel: budowa systemu zapewniającego zgodność z zasadami ochrony prywatności.

2.1 Oszacowanie środków gwarantujących zachowanie zasady proporcjonalności i konieczności przetwarzania

- Wyjaśnij i uzasadnij **wybory dokonywane celem spełnienia następujących wymagań**:
  1. **cel (cele)**: konkretne, wyraźne i prawnie uzasadnione (patrz art. 5 ust. 1 lit. b) [RODO]);
  2. **podstawy prawne**: zgodność przetwarzania z prawem, zakaz nadużyć (patrz art. 6 [RODO])[11];
  3. **minimalizacja danych**: dane są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (patrz art. 5 lit. c) [RODO])[12];
  4. **jakość danych**: dane są prawidłowe i aktualne (patrz art. 5 lit. d) [RODO]);
  5. **okres przechowywania**: ograniczony (patrz art. 5 lit. e) [RODO]).
- Sprawdź czy dla poruszanych zagadnień, jest konieczne lub jest możliwe doskonalenie sposobu planowania, wyjaśniania i uzasadniania na zgodność z [RODO].
- W stosownych przypadkach przejrzyj ich opis lub zaproponuj dodatkowe środki.

2.2 Oszacowanie środków służących ochronie praw osób, których dane dotyczą

- Zidentyfikuj lub określ, oraz opisz **środki** (istniejące lub planowane) **wybrane do zapewnienia zgodności z poniższymi wymaganiami prawnymi** (wymagane jest wyjaśnienie sposobu w jaki mają być realizowane):
  1. **informacje** dla osób, których dane dotyczą (rzetelne i przejrzyste przetwarzanie, patrz art. 12, 13 i 14 [RODO]);
  2. **uzyskanie zgody** w stosownych przypadkach[13]: wyraźnej, którą można wykazać i wycofać (patrz art. 7 i 8 [RODO]);
  3. wyegzekwowanie **prawa dostępu do danych i prawa do przenoszenia danych** (patrz art. 15 i 20 [RODO]);
  4. wyegzekwowanie **prawa do sprostowania i prawa do usunięcia danych** (patrz art. 16 i 17 [RODO]);
  5. wyegzekwowanie **prawa do ograniczenia przetwarzania i prawa do sprzeciwu** (patrz art. 18 i 21 [RODO]);
  6. **podmioty przetwarzające**: wskazane i objęte umową (patrz art. 28 [RODO]);
  7. **przekazywanie danych**: zgodność z zobowiązaniami dotyczącymi przekazywania danych poza Unię Europejską (patrz art. 44 do 49 [RODO]).
- Sprawdź czy dla każdego środka i jego opisu, jest konieczne lub jest możliwe doskonalenie odnośnie zgodności z [RODO].
- W stosownych przypadkach przejrzyj ich opis lub zaproponuj dodatkowe środki.

[11] Należy wykazać również, że odbiorcy są uprawnieni.
[12] Należy wykazać również, że odbiorcy faktycznie potrzebują dostępu do danych.
[13] Należy uzasadnić przypadki, w których zgoda nie była uzyskiwana.

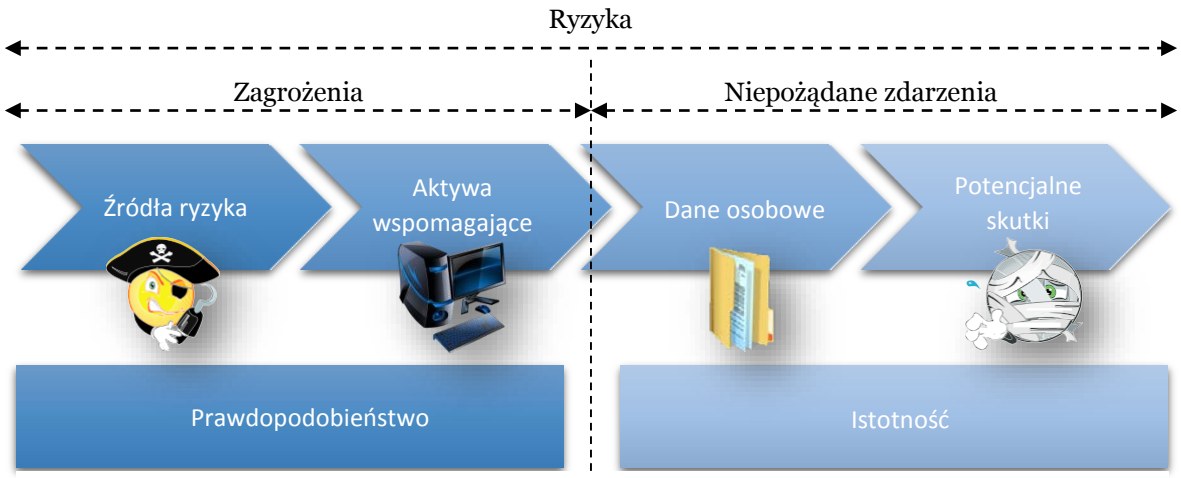
3 Badanie ryzyka związanego z bezpieczeństwem danych[14]

Co to jest ryzyko prywatności?

Ryzyko jest hipotetycznym scenariuszem opisującym niepożądane zdarzenie oraz wszystkie zagrożenia umożliwiające jego wystąpienie. Bardziej konkretnie, opisuje ono:

- jak źródła ryzyka (np. pracownik przekupiony przez konkurenta)
- mogą wykorzystać podatności aktywów wspierających (np.: system zarządzania plikami, który umożliwia manipulowanie danymi)
- w kontekście zagrożeń (np. nadużycie poprzez wysłanie wiadomości e-mail)
- i umożliwią wystąpienie niepożądanego zdarzenie (np.: nieuprawniony dostęp do danych osobowych)
- wobec danych osobowych (np.: kartoteka klienta)
- w ten sposób wywołując skutki dla prywatności osób (np.: niepożądane oferty, poczucie naruszenia prywatności, problemy osobiste lub zawodowe).

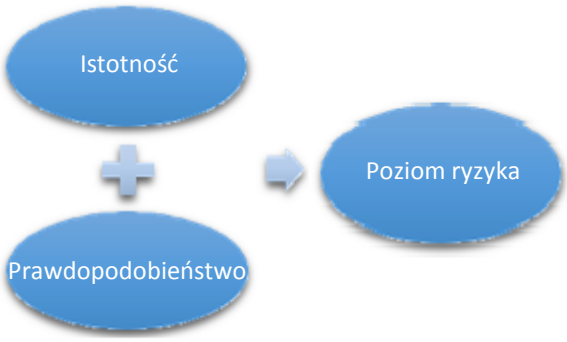
Poniższy diagram podsumowuje wszystkie powyższe pojęcia:



Rysunek 4 Elementy ryzyka

Poziom ryzyka szacujemy pod względem istotności i prawdopodobieństwa:

- **istotność** oznacza wielkość ryzyka. Przede wszystkim zależy od szkodliwego charakteru potencjalnych skutków[15];
- **prawdopodobieństwo** oznacza możliwość ziszczenia się ryzyka. Przede wszystkim zależy od podatności aktywów wspierających na zagrożenia oraz zdolności źródeł ryzyka do ich wykorzystania.



Rysunek 3 Czynniki szacowania ryzyka

[14] patrz art. 32 [RODO].

[15] W świetle kontekstu przetwarzania danych osobowych (charakter danych, osoby, których dane dotyczą, cel przetwarzania, itp.).

3.1 Ocena istniejących i planowanych środków

Zazwyczaj przeprowadzana przez głównego wykonawcę kontraktu[16], a następnie oceniana przez osobę odpowiedzialną za aspekty „bezpieczeństwa danych”[17].

Cel: poznanie środków kontroli, które przyczyniają się do bezpieczeństwa.

- Zidentyfikuj lub określ **istniejące lub planowane środki** (już wprowadzone), które mogą przybierać trzy formy:
  1. **środki dotyczące konkretnie przetwarzanych danych**: szyfrowanie, anonimizacja, partycjonowanie danych, kontrola dostępu, dzienniki systemowe, itp.;
  2. **ogólne środki bezpieczeństwa dotyczące systemu, w którym przeprowadzane jest przetwarzanie**: zabezpieczenia eksploatacji, kopie zapasowe, bezpieczeństwo sprzętu, itp.;
  3. **środki organizacyjne (zarządzanie)**: polityka, zarządzanie projektem, zarządzanie personelem, zarządzanie incydentami i naruszeniami, relacje ze stronami trzecimi, itp..
- Sprawdź czy dla każdego środka i jego opisu, jest konieczne lub jest możliwe doskonalenie zgodnie z najlepszymi praktykami bezpieczeństwa.
- W stosownych przypadkach przejrzyj ich opis lub zaproponuj dodatkowe środki.

3.2 Szacowanie ryzyka: potencjalne naruszenia prywatności

Zazwyczaj realizowane przez właściciela projektu, a następnie oceniane przez osobę odpowiedzialną za aspekty „ochrony danych”.

Cel: poznanie przyczyn i konsekwencji ryzyka.

- Dla każdego niepożądanego zdarzenia (nieupoważniony dostęp do danych osobowych[18], niepożądana modyfikacja danych osobowych[19] oraz zniknięcie danych osobowych[20]):
  1. określ potencjalne **skutki** dla prywatności osób, jeżeli wystąpiły[21];
  2. oszacuj **istotność**, w szczególności w zależności od szkodliwego charakteru potencjalnych skutków oraz w stosownych przypadkach środki, które mogłyby je modyfikować;
  3. zidentyfikuj **zagrożenia** dla aktywów wspierających przetwarzanie danych, mogące prowadzić do wystąpienia niepożądanego zdarzenia[22] oraz **źródła ryzyka**, które mogą spowodować to zagrożenie;
  4. oszacuj **prawdopodobieństwo**, w szczególności w zależności od poziomu podatności aktywów wspomagających przetwarzanie danych osobowych,

[16] To może być osoba delegowana, przedstawiciel lub podmiot przetwarzający.
[17] Kierownik ds. bezpieczeństwa informacji lub inna osoba.
[18] Dane ujawnione nieupoważnionym osobom (naruszenie poufności danych osobowych).
[19] Dane podmienione lub zmienione (naruszenie integralności danych osobowych).
[20] Dane niedostępne lub nie będą dostępne (naruszenie dostępności danych osobowych).
[21] Odpowiedz na pytanie "Czego obawiamy się wobec osób, których dane dotyczą?".
[22] Odpowiedz na pytanie "Jak to się może wydarzyć?".

poziomu zdolności źródeł ryzyka do ich wykorzystania oraz środki, które mogłyby je modyfikować.

- Określ, czy ryzyka zidentyfikowane w ten sposób[23] mogą być uznane za akceptowalne w świetle istniejących lub planowanych środków.
- Jeżeli nie, zaproponuj dodatkowe środki i ponownie przeprowadź szacowanie poziomu ryzyka z ich uwzględnieniem, by określić ryzyko rezydualne.

[23] Ryzyko opiera się na niepożądanym zdarzeniu i zagrożeniach, które je umożliwiają.

4 Zatwierdzenie PIA

Zazwyczaj realizowane przez Administratora Danych Osobowych, z pomocą osoby odpowiedzialnej za aspekty „ochrony danych”.

Cel: decyzja, czy zaakceptować PIA w świetle ustaleń przeprowadzonego badania.

4.1 Przygotowanie materiałów wymaganych do zatwierdzenia

- Skonsoliduj i przedstaw wyniki badań:
  1. przygotuj wizualną prezentację **środków wybranych w celu zapewnienia zgodności z zasadami podstawowymi**, zależnie od ich zgodności z [RODO] (np. wymagających doskonalenia lub uznanych za zgodne);
  2. przygotuj wizualną prezentację **środków wybranych w celu poprawy bezpieczeństwa danych**, zależnie od zgodności z najlepszymi praktykami w zakresie bezpieczeństwa (np.: wymagających doskonalenia lub uznanych za zgodne);
  3. przedstaw wizualną mapę **ryzyka** (początkowe i w stosownych przypadkach rezydualne[24]), zależnie od istotności i prawdopodobieństwa;
  4. sporządź **plan działania** w oparciu o dodatkowe środki określone podczas poprzednich kroków. W odniesieniu do każdego środka należy określić co najmniej: osobę odpowiedzialną za wdrożenie, koszt (finansowy lub w zakresie pracochłonności) oraz przewidywany harmonogram.
- Formalnie udokumentuj uwzględnienie opinii interesariuszy:
  1. konsultację z **osobą odpowiedzialną za aspekty „ochrony danych"** (patrz art. 35 ust. 2 [RODO]) *(przyp. red.: Inspektora Ochrony Danych)*;
  2. opinię **osób, których dane dotyczą lub ich przedstawicieli** (patrz. art. 35 ust. 9 [RODO]).

4.2 Formalne zatwierdzenie

- Podejmij decyzję, czy wybrane środki, ryzyko rezydualne i plan działania są akceptowalne wraz z uzasadnieniami, w świetle wcześniej określonych interesów i opinii interesariuszy. W taki sposób PIA może być:
  1. Zatwierdzona;
  2. Zatwierdzona warunkowo z uwagami (wyjaśnić sposób poprawienia);
  3. Odrzucona (wraz z rozpatrywanym przetwarzaniem).
- W razie potrzeby powtórz poprzednie kroki by PIA mogła być zatwierdzona.

[24] Ryzyko pozostające po wdrożeniu środków.

Załączniki

Definicje

Uwaga: wyrazy w nawiasach odpowiadają krótszym terminom użytym w niniejszym dokumencie.

Środek (ang. *Control*)	Działanie, które należy podjąć. *Uwaga: może to być techniczny lub organizacyjny środek oraz może obejmować wprowadzenie zasad podstawowych w życie lub prowadzić do unikania, zmniejszania, przeniesienia lub transferu całości lub części ryzyka.*
Administrator Danych Osobowych	Osoba fizyczna lub prawna, organ administracji publicznej, agencja lub inny organ, który samodzielnie lub wspólnie z innymi osobami określa cele i środki przetwarzania danych osobowych; w przypadku gdy cele i sposoby takiego przetwarzania są określone przez prawo Unii lub prawo państwa członkowskiego, administrator lub szczególne kryteria jego ustanowienia mogą być ujęte w prawie Unii lub w prawie państwa członkowskiego. [RODO] *Uwaga: o ile nie zostało to wyraźnie określone w przepisach ustawowych lub wykonawczych dotyczących tego przetwarzania. (przyp. red: przywoływany fragment pochodzi z [DP-Act], w Polsce odpowiednikiem jest Ustawa z 10 maja 2018 r. o ochronie danych osobowych, niemniej zapisy ustaw nie pokrywają się).*
Podmioty danych	Osoby, których dotyczą dane objęte przetwarzaniem. *(przyp. red.: przywoływany fragment pochodzi z [DP-Act], w Polsce odpowiednikiem jest Ustawa z 10 maja 2018 r. o ochronie danych osobowych, niemniej zapisy ustaw nie pokrywają się)*
Niepożądane zdarzenie	Potencjalne naruszenie danych, które może mieć skutki dla prywatności osób, których dane dotyczą.
Prawdopodobieństwo	Oszacowanie możliwości wystąpienia ryzyka. *Uwaga: zależy przede wszystkim od poziomu podatności, które można wykorzystać oraz od poziomu zdolności ich wykorzystania przez źródła ryzyka.*
Dane osobowe (dane)	Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (dalej zwanej "podmiotem danych"); "możliwa do zidentyfikowania osoba fizyczna" to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, w szczególności przez odniesienie do identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników charakterystycznych dla fizycznej, fizjologicznej, genetycznej, umysłowej, ekonomicznej, kulturowej lub społecznej tożsamości tej osoby fizycznej. [RODO] *Uwaga: Aby ustalić, czy dana osoba jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszystkie środki, z których administrator danych lub jakakolwiek inna osoba*

	może korzystać lub do których może mieć dostęp. (przyp. red: przywoływany fragment pochodzi z [DP-Act], w Polsce odpowiednikiem jest Ustawa z 10 maja 2018 r. o ochronie danych osobowych, niemniej zapisy ustaw nie pokrywają się).
Przetwarzanie danych osobowych (przetwarzanie)	Wszelka operacja lub zbiór operacji dokonywanych na danych osobowych lub w zbiorach danych osobowych, niezależnie od tego, czy są to środki zautomatyzowane czy też nie, takie jak zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptowanie lub zmiana, wyszukiwanie, konsultowanie, wykorzystywanie, ujawnianie przez przekazywanie, rozpowszechnianie lub udostępnianie w inny sposób, wyrównywanie struktur lub łączenie, ograniczanie, wymazywanie lub niszczenie. [RODO]
Ryzyko	Scenariusz opisujący niepożądane zdarzenie oraz wszystkie zagrożenia umożliwiające jego wystąpienie. *Uwaga: szacuje się je pod względem istotności i prawdopodobieństwa.*
Źródło ryzyka	Źródło osobowe lub nieosobowe, które może powodować ryzyko. *Uwaga: źródło ryzyka może działać przypadkowo lub umyślnie.*
Istotność	Oszacowanie wielkości potencjalnych skutków dla prywatności osób, których dane dotyczą *(przyp. red.: podmiotów danych).* *Uwaga: Zależy przede wszystkim od szkodliwego charakteru potencjalnych skutków.*
Aktywa wspomagające	Aktywa od których zależne są dane osobowe. *Uwaga: może to być sprzęt, oprogramowanie, sieci, ludzie, dokumenty papierowe lub papierowe kanały komunikacji.*
Zagrożenie	Działanie obejmujące jedno lub więcej pojedynczych akcji na aktywach wspomagających. *Uwaga: jest wykorzystywane celowo lub w inny sposób przez źródła ryzyka i może powodować niepożądane zdarzenie.*

Bibliografia

[Karta UE]	Karta praw podstawowych Unii Europejskiej, 2010/C83/02
[RODO]	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
[DP-Act]	Francuska ustawa o ochronie danych nr. 78-17 z dnia 6 stycznia 1978 r., z późn. zmianami[25] *(przyp. red.: w Polsce odpowiednikiem jest Ustawa z 10 maja 2018 r. o ochronie danych osobowych, niemniej zapisy ustaw nie pokrywają się).*

[25] Zmieniona francuską ustawą nr 2004-801 z dnia 6 sierpnia 2004 r. o ochronie osób fizycznych w zakresie przetwarzania danych osobowych oraz francuską ustawą nr 2009-526 z dnia 12 maja 2009 r. w sprawie uproszczenia i zwiększenia przejrzystości francuskiego prawa i ułatwienia procedur.

[Wytyczne WP29]	Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) określające, czy przetwarzanie "może prowadzić do wysokiego ryzyka" dla celów rozporządzenia 2016/679, wp248rev.01, Grupa robocza art. 29.
[ISO 31000]	ISO 31000: 2009, Zarządzanie ryzykiem – Zasady i wytyczne, ISO.

Mapa pokrycia kryteriów [Wytyczne WP29]

Kryteria [Wytyczne WP29]	**Spełnienie**	**Rozdział w niniejszych wytycznych**
Zapewniono systematyczny opis operacji przetwarzania (art. 35 ust. 7 lit. a): - uwzględniono charakter, zakres, kontekst i cele przetwarzania (motyw 90); - w rejestrze zamieszczono dane osobowe, informacje o odbiorcach i okresie przechowywania danych osobowych; - przedstawiono funkcjonalny opis operacji przetwarzania; - zidentyfikowano zasoby, z którymi styczność mają dane osobowe (sprzęt komputerowy, oprogramowanie, sieci, osoby, opracowania lub kanały transmisji opracowań); - uwzględniono przestrzeganie zatwierdzonych kodeksów postępowania (art. 35 ust. 8);	☑	1. Badanie kontekstu

Oceniono niezbędność oraz proporcjonalność (art. 35 ust. 7 lit. b)):
- wskazano środki, których podjęcie jest planowane w celu zapewnienia przestrzegania rozporządzenia (art. 35 ust. 7 lit. d) i motyw 90), uwzględniając:
  - środki przyczyniające się do proporcjonalności i niezbędności przetwarzania, z uwzględnieniem następujących aspektów:
  - konkretne, wyraźne i prawnie uzasadnione cele (art. 5 ust. 1 lit. b));
  - zgodność przetwarzania z prawem (art. 6);
  - dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (art. 5 ust. 1 lit. c));
  - ograniczony czas przechowywania (art. 5 ust. 1 lit. e));
  - środki przyczyniające się do zachowania praw osób, których dane dotyczą:
  - poinformowanie osoby, której dane dotyczą (art. 12, 13 i 14);
  - prawo dostępu i prawo do przenoszenia danych (art. 15 i 20);
  - prawo do sprostowania i do usunięcia danych (art. 16, 17 i 19);
  - prawo do sprzeciwu i prawo do ograniczenia przetwarzania (art. 18, 19 i 21);
  - relacje z podmiotem przetwarzającym (art. 28);
  - zabezpieczenia przy międzynarodowym przekazywaniu danych (rozdział V);
  - uprzednie konsultacje (art. 36);
	☑	2. Badanie podstawowych zasad

Przeprowadzono działania w zakresie zarządzania ryzykiem naruszenia praw i wolności osób, których dane dotyczą (art. 35 ust. 7 lit. c)): - uwzględniono źródło, charakter, specyfikę i powagę ryzyka (por. motyw 84), czy konkretniej, w przypadku każdego rodzaju ryzyka (bezprawnego dostępu, niepożądanej zmiany i zniknięcia danych), z punktu widzenia osób, których dane dotyczą: - uwzględniono źródła ryzyka (motyw 90); - zidentyfikowano możliwe skutki dla praw i wolności osób, których dane dotyczą, w przypadku zdarzeń takich jak bezprawny dostęp, niepożądane zmiany i zniknięcie danych; - zidentyfikowano zagrożenia, które mogłyby doprowadzić do bezprawnego dostępu, niepożądanych zmian i zniknięcia danych; - oszacowano prawdopodobieństwo i powagę (motyw 90); - określono środki, których podjęcie jest planowane w celu zaradzenia ryzyku (art. 35 ust. 7 lit. d) i motyw 90);	☑	3 Badanie ryzyka związanego z bezpieczeństwem danych
Zaangażowano zainteresowane strony: - skonsultowano się z inspektorem ochrony danych w celu uzyskania zalecenia (art. 35 ust. 2); - w stosownych przypadkach zasięgnięto opinii osób, których dane dotyczą, lub ich przedstawicieli (art. 35 ust. 9).	☑	4. Zatwierdzenie PIA

Informacje o tłumaczeniu

Niniejsza publikacja została przetłumaczona na język polski z anglojęzycznej wersji dokumentu dostępnej na stronie https://www.cnil.fr/en/PIA-privacy-impact-assessment-en.

Tłumaczenie na język polski zostało zrealizowane w ramach funkcjonowania blogu ryzykoIT.pl.

Autorami przekładu są:

- Małgorzata Pikur, malgorzata@ryzykoit.pl
- Sebastian Pikur, sebastian@ryzykoit.pl