Szablon raportu z procesu oceny skutków dla ochrony danych w Unii Europejskiej: propozycja

d.pia.lab Policy Brief nr 1/2020

Dariusz KLOZA, Alessandra CALVI, Simone CASIRAGHI,
Sergi VAZQUEZ MAYMIR, Nikolaos IOANNIDIS, Alessia TANAS i Niels VAN DIJK

Brukselskie Laboratorium ds. Oceny Skutków dla Prywatności i Ochrony Danych (d.pia.lab)
Grupa Badawcza ds. Prawa, Nauki, Technologii i Społeczeństwa (LSTS) | Vrije Universiteit Brussel (VUB)

W niniejszym dokumencie zaproponowano szablon raportu z procesu oceny skutków dla ochrony danych (OSOD) w Unii Europejskiej (UE). Oparty na opracowanej wcześniej strukturze (por. Policy Brief nr 1/2017) i metodzie oceny skutków (por. Policy Brief nr 1/2019), niniejszy szablon jest zgodny z wymogami art. 35–36 ogólnego rozporządzenia o ochronie danych (RODO) i odzwierciedla najlepsze praktyki w zakresie oceny skutków, jednocześnie proponując pięć nowatorskich założeń. Pierwszym założeniem jest jego kompleksowość, tak aby umożliwić podejmowanie jak najsolidniejszych decyzji w zakresie ochrony danych osobowych. Drugim założeniem jego jest jego efektywność, czyli uzyskanie rezultatów przy jak najmniejszym wykorzystaniu zasobów. Trzecim założeniem jest zbadanie i uwzględnienie perspektyw różnych interesariuszy, przy czym dominuje perspektywa jednostki. Niniejszy szablon jednocześnie sprzyja myśleniu w kategoriach praw podstawowych, na przykład poprzez wymóg uzasadnienia każdego wyboru, tym samym wykraczając poza mechaniczne „odhaczanie" punktów z listy wymogów. Czwartym założeniem jest dążenie do realizacji podejścia *legal design,* prowadząc osoby oceniające w praktyczny, łatwy i intuicyjny sposób przez cały 11-stopniowy proces oceny, oferując jednocześnie niezbędne instrukcje i wyjaśnienia dla każdego kroku oraz posiadając strukturę rozszerzalnych i modyfikowalnych tabel i pól do wypełnienia. Zgodnie z piątym założeniem, kształt szablonu nie jest ostateczny, gdyż w miarę wzrostu doświadczenia z jego użycia musi on być rewidowany. Szablon ten jest skierowany głównie do osób, którym administratorzy danych powierzyli zadanie przeprowadzenia procesu oceny skutków dla ochrony danych. Niemniej, może on również pomóc organom nadzorczym w UE w opracowaniu szablonów raportu z procesu OSOD z możliwością dostosowania do ich własnych jurysdykcji.

1 WPROWADZENIE

1.1 KONTEKST

Ogólne rozporządzenie o ochronie danych (RODO) Unii Europejskiej (UE) nakłada na administratorów danych m.in. obowiązek przeprowadzenia, w przypadku dużego prawdopodobieństwa wystąpienia wysokiego ryzyka naruszenia praw i wolności osób fizycznych, procesu oceny skutków dla ochrony danych (OSOD; ang. *data protection impact assessment*) (art. 35 ust. 1). Ten nowy wymóg wywołał szereg pytań, w tym dotyczących praktycznych kwestii związanych z procesem oceny. W odpowiedzi d.pia.lab proponuje *szablon* raportu z procesu oceny skutków dla ochrony danych, który odzwierciedla najlepsze praktyki oceny i jest zgodny z wymogami RODO.

Szablon procesu oceny stanowi praktyczną pomoc dla oceniających. Zawiera formularz, który – wypełniony zgodnie z określoną metodą – ustrukturyzuje proces oceny, poprowadzi przezeń oceniających, a po jego zakończeniu posłuży jako raport końcowy. Jednocześnie szablon daje możliwość udokumentowania wszystkich działań podejmowanych w ramach danego procesu oceny. Pozwala to administratorom wykazać m.in. zgodność z prawem oraz udowodnić jakość procesu oceny (por. zasada rozliczalności; art. 5 ust. 2). Szablon procesu oceny może być postrzegany jako praktyczna implementacja *metody* oceny skutków (tj. procedury składającej się z następujących po sobie lub powtarzających się kroków), która sama w sobie odzwierciedla jego *strukturę* (tj. warunki i zasady określające jego teorię i praktykę). Pomimo wielu korzyści, szablony procesu oceny skutków mają swoje nieodłączne ograniczenia i nie można ich używać bez krytycznej refleksji.

 ISSN 2565-9936

1.2 AKTUALNY STAN WIEDZY I INNOWACYJNOŚĆ

Nie ma zgody co do tego, jak *dokładnie* przeprowadza się proces oceny skutków. Opracowano wiele szablonów procesu OSOD, które mają różne kształty i różne zastosowania (jurysdykcja, sektor publiczny, sektor prywatny itp.). Jakość tych szablonów znacznie się różni. Najczęstsze problemy wydają się dotyczyć ich przydatności do danego celu, niezrozumiałości, niskiego poziomu przejrzystości i szczegółowości, co ostatecznie czyni je mało przydatnymi dla oceniających.

Proponowany szablon bazuje na krytycznej i porównawczej analizie istniejących szablonów, dopracowanych przez d.pia.lab na podstawie własnych doświadczeń. Jest on zgodny z zasadami i warunkami określonymi w strukturze dla oceny skutków opracowanej przez d.pia.lab (por. Policy Brief nr 1/2017, rozdz. 2). Opiera się na ogólnej metodzie oceny skutków (por. Policy Brief nr 1/2019, rozdz. 2), nieznacznie poprawionej i zaktualizowanej, oraz dostosowanej do wymogów prawnych UE (por. Policy Brief nr 1/2019, rozdz. 3). Innymi słowy, szablon łączy ogólną metodę oceny skutków z konkretną metodą procesu OSOD, zgodnie z interpretacją zawartą w art. 35–36, zasadniczo poprzez nałożenie tej drugiej na tę pierwszą. W szablonie rozróżnia się obowiązkowe i dobrowolne elementy procesu oceny, w związku z czym każdy element, który nie jest wymagany *expressis verbis* przez RODO, jest wyraźnie oznaczony jako taki.

Niniejszy szablon oferuje co najmniej pięć nowych założeń. Po pierwsze, założeniem szablonu jest jego kompleksowość, tak aby umożliwić podejmowanie jak najsolidniejszych decyzji w zakresie ochrony danych osobowych. Realizując niniejsze, ma on nie pomijać m.in istotnych problemów społecznych, interesariuszy i kroków do podjęcia w procesie oceny.

Po drugie, dąży on do efektywności, czyli uzyskania rezultatów (takich jak wsparcie przy podejmowaniu decyzji) przy jak najmniejszym wykorzystaniu zasobów. Przykładowo, pozwala na wybór konkretnych technik oceny lub na integrację wielu procesów oceny. Mając na uwadze przedmiotową optymalizację wykorzystania zasobów, oddzielny krok jest dedykowany na zaplanowanie i przygotowanie danego procesu oceny.

Po trzecie, założeniem szablonu jest zbadanie i uwzględnienie perspektyw różnych interesariuszy (np. osób fizycznych, osób prawnych z sektora publicznego i prywatnego) przy szczególnym nacisku na perspektywę jednostki. Zakłada się, że dane osobowe – i związane z nimi podstawowe prawa i wolności – zasługują na ochronę o określonej jakości. W związku z tym założeniem szablonu jest dążenie do ochrony jednostek, nie tylko poprzez pomoc administratorom w przestrzeganiu prawa, ale także dzięki wyjściu poza czysty formalizm. Wymagając szczegółowego uzasadnienia każdego dokonanego wyboru, sprzyja on myśleniu w kategoriach praw podstawowych oraz kieruje proces oceny w stronę bardziej kompleksowego działania zamiast zwykłej kontroli zgodności i „odhaczania" punktów z listy wymogów.

Po czwarte, szablon ma być przyjazny dla użytkownika. Realizując podejście *legal design*, które ma na celu uczynienie systemów i usług prawnych bardziej skoncentrowanymi na człowieku, użytecznymi i satysfakcjonującymi – szablon ten nie tylko prowadzi osoby oceniające krok po kroku przez proces oceny w praktyczny, łatwy i intuicyjny sposób, ale zawiera również minimalne, lecz niezbędne, instrukcje i wyjaśnienia.

Wreszcie, po piąte, kształt szablonu z założenia nie jest ostateczny. Podobnie bowiem jak struktury i metody, a także same procesy oceny, szablon jest „żywym instrumentem" który stale ewoluuje wraz ze wzrostem doświadczenia z jego użycia i dlatego wymaga odpowiedniej rewizji.

Proponowany szablon podlega pewnym niezbędnym ograniczeniom. Po pierwsze, opierając się na procesie oceny skutków dla ochrony danych zgodnie z wymogami RODO, *nie* uwzględnia specyfiki procesu OSOD na innych płaszczyznach prawa UE, np. na mocy dyrektywy 2016/680 lub rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii (2018/1725). Po drugie, proponowany szablon rzadko będzie stosowany bezpośrednio. Będzie on musiał zostać dostosowany do kontekstu jego użycia, takiego jak dana jurysdykcja, sektor prywatny lub sektor publiczny.

1.3 ADRESACI SZABLONU

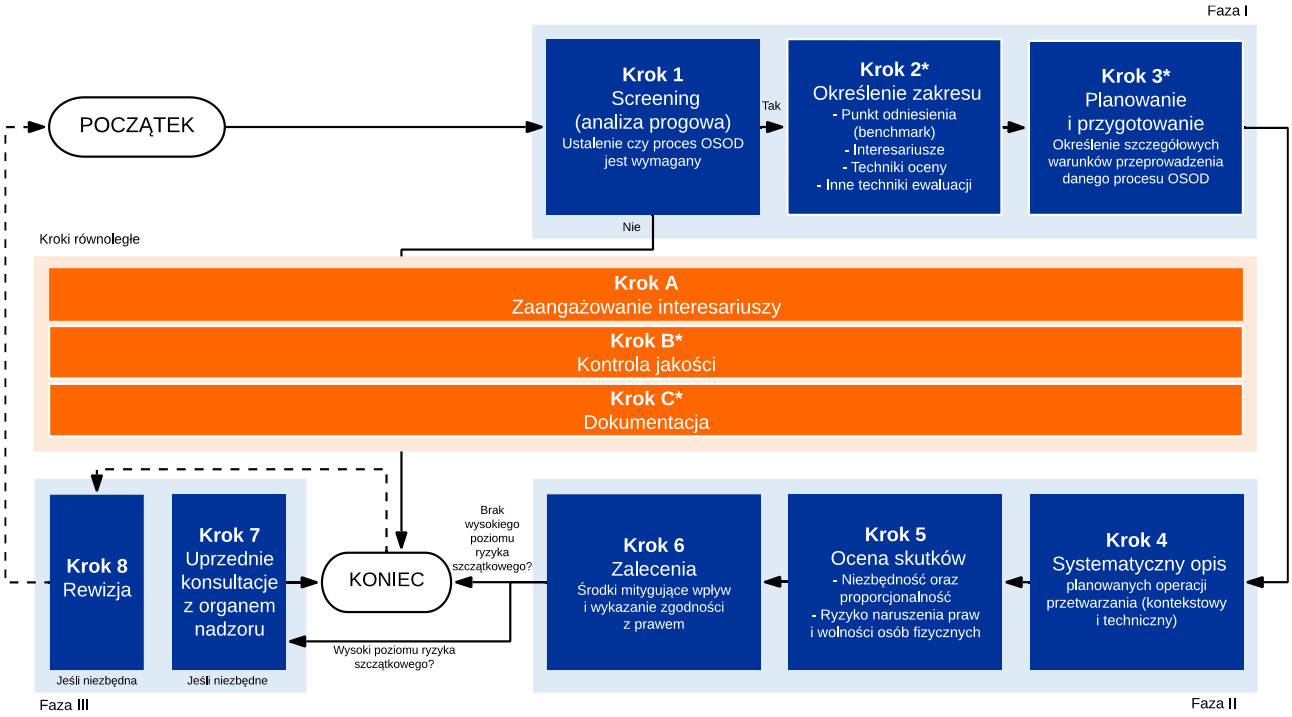
Proponowany szablon jest przeznaczony przede wszystkim do wykorzystania przez osoby oceniające, którym administrator danych powierzył wykonanie danego procesu OSOD. Oceniający to osoby fizyczne lub prawne, które w praktyce przeprowadzają proces oceny. Proces ten rzadko jest zadaniem jednej osoby; zamiast tego, w celu realizacji procesu oceny najczęściej współpracuje ze sobą zespół osób oceniających o zróżnicowanej wiedzy i *know-how*. Osoby oceniające mogą działać wewnątrz organizacji lub na zasadzie odpłatnego outsourcingu (np. doradztwa). Ostatecznie jednak to na administratorze spoczywa odpowiedzialność za przestrzeganie zasady rozliczalności (art. 5 ust. 2 i art. 24) i to on pozostaje prawnie odpowiedzialny za proces oceny (art. 83 ust. 4 lit. a). Jeśli administratorzy sami przeprowadzają proces oceny, stają się wówczas osobami oceniającymi.

Ponadto, proponowany szablon może wpłynąć na rozwój szablonów dla (dostosowanego) procesu OSOD, które krajowe lub regionalne organy nadzorcze w UE i innych jurysdykcjach Europejskiego Obszaru Gospodarczego (EOG) mogłyby opracować w ramach własnych jurysdykcji. Może on ponadto służyć jako wzór szablonów (dostosowanych) dla procesu

OSOD w innych jurysdykcjach i – potencjalnie – dla szablonów przeznaczonych dla innych rodzajów procesów oceny w innych dziedzinach.

1.4 PRZEGLĄD METODY OCENY

Proponowany szablon odzwierciedla metodę składającą się z jedenastu kroków, z których pierwszych sześć to następujące po sobie kroki (kroki 1–6; kroki 1–3 można w dużej mierze wykonywać równolegle), dwa kroki *ex post* (kroki 7–8, znajdujące zastosowanie tylko w określonych warunkach) i trzy równoległe kroki (kroki A – C, które należy wykonać w całym procesie oceny równolegle z krokami 1–8) zgrupowane w czterech fazach (fazy I – III; faza równoległa nie jest numerowana). Kolejność tych kroków jest motywowana sposobem, w jaki każdy krok odnosi się do kolejnego.



1.5 JAK OCENIAJĄCY SKORZYSTA Z SZABLONU?

Aby zdać raport z procesu oceny, oceniający wypełniają, w przystępnym języku, tabele lub inne pola przypisane do każdego kroku. W miarę możliwości, każda odpowiedź jest wyczerpująca i dostatecznie umotywowana (opisana, wyjaśniona, uzasadniona itp.), zarówno w odniesieniu do kryteriów spełnionych, jak i niespełnionych. W każdej tabeli można dodać kolejne wiersze, jeśli zajdzie taka potrzeba. Jeśli ilość miejsca okaże się niewystarczająca, każdy element można przenieść do załącznika. Ewentualnie, dowolna z tabel lub dowolne z pól może zostać usunięte, a te same informacje przedstawione w innym formacie, jeśli oceniający uznają to za stosowne. Objaśnienia na początku każdego kroku mogą zostać usunięte po uzupełnieniu raportu. (Równolegle z niniejszym Policy Brief, d.pia.lab oferuje edytowalny formularz do wypełnienia).

Zgodnie z ujętą w tym szablonie w 11 krokach metodą, następujące po sobie kroki są zaznaczane na niebiesko, a równoległe kroki na pomarańczowo. Oceniający wypełniają tylko pola zaznaczone odpowiednio na jasnoniebiesko lub jasnopomarańczowo. Na koniec każdego kroku znajduje się pole przeznaczone, w razie konieczności, na dalsze uwagi lub komentarze. Po otrzymaniu wypełnionego raportu, administrator wypełnia z kolei jedynie jasnozielone pola.

Szablon zakłada, że zespół osób oceniających zna ramy prawne ochrony danych osobowych określone w RODO. (Odniesienia do przepisów prawnych bez dalszego doprecyzowania dotyczą RODO.) Zakłada również minimalną znajomość procesu oceny ryzyka oraz kryteriów ograniczających korzystanie z praw człowieka, w szczególności zasad niezbędności[1] i proporcjonalności. Niemniej jednak proponowany szablon należy czytać w połączeniu z poprzednimi

[1] W polskiej wersji językowej Karty Praw Podstwowych UE zwrot *„limitations may be made only if they are necessary”* przetłumaczono jako *„ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne”*, natomiast w RODO zwrot *„an assessment of the necessity and proportionality of the processing operations in relation to the purposes”* przetłumaczono jako *„ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów”*. W dalszej części tekstu termin „niezbędność” używany jest w odniesieniu do obu tych pojęć (konieczności i niezbędności) w rozumieniu przywołanych aktów prawnych (przyp. tłum.).

dokumentami Policy Briefs autorstwa d.pia.lab, w których wyjaśniono kluczowe pojęcia. Dalsze odniesienia są sugerowane na końcu niniejszego Policy Brief.

Proces OSOD jest zwykle inicjowany przez (kierownictwo) administratora, na którym spoczywa obowiązek przeprowadzenia tego procesu (art. 35 ust. 1). Podmiot przetwarzający, jeśli został wyznaczony, ma obowiązek pomagać administratorowi (art. 28 ust. 3 lit. f); jednakże podmiot przetwarzający może przeprowadzić proces oceny do własnych celów z własnej woli. Zakłada się, że wszystkie podmioty – od administratora i oceniających poprzez inspektora ochrony danych (ang. *DPO*) po interesariuszy – są zaangażowane w cały proces oceny. Ponieważ proces oceny dotyczy operacji przetwarzania danych, które zwykle nie są jeszcze wykonywane, lecz zostaną przeprowadzone w przyszłości, oceniający mogą polegać na szacunkach, a czasami również na niekompletnych informacjach.

Dołożono wszelkich starań, aby zapewnić dokładność przedstawionych informacji. Niemniej, całość informacji zawartych w tym dokumencie nie jest objęta żadną gwarancją. Ani d.pia.lab, ani poszczególni autorzy nie ponoszą żadnej odpowiedzialności za jakiekolwiek negatywne konsekwencje poniesione w wyniku zastosowania, niewłaściwego użycia niniejszego dokumentu lub polegania na nim.

WZÓR RAPORTU Z PROCESU OCENY SKUTKÓW DLA OCHRONY DANYCH

IDENTYFIKACJA DANYCH

Nazwa przedsięwzięcia i numer – jeśli ma zastosowanie	
Imię i nazwisko, dane kontaktowe i inne dane identyfikacyjne:	
▪ administrator(zy)	
▪ podmiot(y) przetwarzający(-e) – jeśli dotyczy	
▪ osoba(-y) odpowiedzialna(-e) za przedsięwzięcie (właściciel procesowy)	
▪ osoba(-y) oceniająca(-e)	
▪ inspektor ochrony danych – jeśli wyznaczono	
▪ administrator bezpieczeństwa informacji – jeśli wyznaczono	
▪ właściwy organ kontrolny nadzorujący jakość procesu oceny – jeśli wyznaczono	
▪ właściwy(-e) organ(-y) nadzoru	
▪ inni zaangażowani – jeśli praktykowane	
Wersja raportu	
Poziom poufności raportu	☐ Publiczny ☐ Poufny ☐ Szczególne warunki *[Wyjaśnić]*
Data i miejsce sporządzenia raportu	
[Wszelkie inne informacje – jeśli praktykowane]	

STRESZCZENIE

[Podsumować najważniejsze informacje dotyczące wyniku każdego przeprowadzonego etapu procesu oceny skutków dla ochrony danych (OSOD).]

FAZA I: PRZYGOTOWANIE DO PROCESU OCENY

KROK 1 SCREENING (ANALIZA PROGOWA)

Cel

Celem tego kroku jest, w pierwszej kolejności, ustalenie, czy proces OSOD jest w ogóle wymagany, na co może wskazywać spełnienie jednego lub więcej kryteriów określonych w prawie lub innych odpowiednich wymogach regulacyjnych; alternatywnie dokonuje się ustalenia, czy proces oceny nie jest wymagany z uwagi na odpowiednie przesłanki zwalniające.

EXTRA Administrator może z własnej woli zdecydować o przeprowadzeniu procesu OSOD niezależnie od wymogów prawnych, również pomocniczo w celu przestrzegania zasady rozliczalności (art. 5 ust. 2, art. 24), zasady uwzględniania ochrony danych w fazie projektowania i zasady domyślnej ochrony danych (art. 25) oraz bezpieczeństwa przetwarzania (art. 32).

Realizacja

Na tym etapie, na podstawie podstawowych kontekstowych i technicznych opisów planowanych operacji przetwarzania danych, które stanowią przedmiot oceny (por. *krok 1a*), oceniający analizują, czy wspomniane operacje spełniają którekolwiek z kryteriów progowych (por. *krok 1b*). Jako warunek wstępny, oceniający określają, czy dane osobowe będą przetwarzane; jeśli nie, RODO nie ma zastosowania, a zatem proces OSOD nie jest obowiązkowy.

Kryteria są ustalone przede wszystkim przez RODO i mogą być uzupełniane poprzez inny instrument prawny lub regulacyjny, któremu podlega administrator, np. kodeks postępowania (art. 40) (por. *krok 2a*); orzecznictwo może także zapewnić dalsze wyjaśnienie tych kryteriów.

Chociaż na wczesnych etapach zwykle dostępnych jest niewiele informacji, opis wstępny jest krótki (ok. jednej strony) ale wystarczająco szczegółowy, aby oceniający mogli określić, czy kryteria progowe są spełnione. Taki opis może opierać się na rejestrach czynności przetwarzania, jeśli są dostępne (art. 30). Unika się w nim ogólnych stwierdzeń. Jeśli okaże się, że proces oceny jest wymagany, wstępny opis zostanie rozszerzony w *kroku 4*.

Kryteria progowe opierają się na pojęciu ryzyka (wyjaśnionym w *kroku 5*) i są pozytywne albo negatywne. (Kryteria negatywne mają pierwszeństwo przed pozytywnymi). Jeśli którekolwiek z kryteriów pozytywnych zostanie spełnione, prawo wówczas wymaga przeprowadzenia procesu oceny. Natomiast w przypadku spełnienia któregokolwiek z kryteriów negatywnych, administrator jest zwolniony z przeprowadzania procesu oceny. W pierwszej sytuacji oceniający przechodzą do *kroku 2*.

EXTRA W tej drugiej sytuacji oceniający przygotowują oświadczenie o braku znaczącego wpływu, uzasadniające powody niewykonania procesu OSOD i nie procedują dalej, chyba że istnieje potrzeba rewizji procesu oceny (por. *krok 8*). W przypadku wątpliwości zaleca się przeprowadzenie procesu oceny.

KROK 1A: WSTĘPNY OPIS PRZEWIDYWANYCH CZYNNOŚCI PRZETWARZANIA

			Uzasadnienie
	Czy planowane jest kiedykolwiek przetwarzanie danych osobowych?		☐ Tak ☐ Nie
Opis kontekstowy	**Charakter** (*jaki rodzaj operacji przetwarzania?*)		
	Zakres	Skala (*jak wiele? O jakim zasięgu?*)	
		Czas (*kiedy? Jak długo?*)	
	Kontekst (*w jakich okolicznościach*?)	Wewnętrzny (*dotyczący administratora*)	
		Zewnętrzny (*dotyczący poszczególnych osób, grup, społeczeństwa itp.*)	
	Cel operacji przetwarzania (*dlaczego?*)		
Opis techniczny	Kategorie przetwarzanych danych osobowych (*jakie?*)		
	Środki przetwarzania (infrastruktura) (*za pomocą jakich środków? np. analogowych, cyfrowych*)		
	Planowane przepływy danych (*skąd dokąd? od kogo do kogo?*)		
	Bezpieczeństwo danych (*w jaki sposób jest zapewnione?*)		
	Jurysdykcja/rynek (*gdzie?*)		
	Podmioty w „łańcuchu dostaw” (*kto?*)		
	[Inne, doprecyzować]		

KROK 1B: SCREENING (ANALIZA PROGOWA)

Kryteria pozytywne

Kryterium	*Podstawa prawna*	*Spełnione?*	Uzasadnienie
KRYTERIUM 1: PRAWDOPODOBIEŃSTWO WYSOKIEGO RYZYKA (OGÓLNE) *Czy planowane operacje przetwarzania mogą powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych?* Do ustalenia na podstawie: ▪ wskaźników ryzyka (charakter, zakres, kontekst i cele przetwarzania) ▪ podstawowej oceny ryzyka (*na ile prawdopodobne? jak poważne?)* ▪ istniejącego rejestru zagrożeń dla ochrony danych (jeśli istnieje) ▪ *[inne; doprecyzować]*	art. 35 ust. 1	☐	
KRYTERIUM 2: PRAWDOPODOBIEŃSTWO WYSOKIEGO RYZYKA (SZCZEGÓŁOWE) *Czy planowane operacje przetwarzania obejmują którąkolwiek z następujących sytuacji, powodujących – według prawa – duże prawdopodobieństwo wystąpienia wysokiego ryzyka*:			
▪ systematyczna, kompleksowa ocena czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną	art. 35 ust. 3 lit. a)	☐	
▪ przetwarzanie na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych	art. 35 ust. 3 lit. b)	☐	
▪ systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie	art. 35 ust. 3 lit. c)	☐	
KRYTERIUM 3: PRAWDOPODOBIEŃSTWO WYSOKIEGO RYZYKA (WYLICZENIE POZYTYWNE) *Czy planowane operacje przetwarzania znajdują się w sporządzonym przez organy nadzoru publicznym wykazie operacji przetwarzania wymagających procesu OSOD?*	art. 35 ust. 4	☐	
KRYTERIUM 3 BIS: ZATWIERDZONE KODEKSY POSTĘPOWANIA *Czy zatwierdzony kodeks postępowania wymaga przeprowadzenia procedury OSOD dla planowanych operacji przetwarzania?*	art. 40	☐	
[Inne, por. krok 2a; doprecyzować]		☐	
Czy proces OSOD jest wymagany?		☐	**Tak** *[przejść do kroku 2]*
		☐	**Nie** *[przejść do kroku 1c]*

Kryteria negatywne

Kryterium	*Podstawa prawna*	*Spełnione?*	*Uzasadnienie*
KRYTERIUM 4: PRAWDOPODOBIEŃSTWO WYSOKIEGO RYZYKA (WYLICZENIE NEGATYWNE) *Czy planowane operacje przetwarzania znajdują się w sporządzonym przez organy nadzoru publicznym wykazie operacji przetwarzania, które są zwolnione z procesu OSOD?*	art. 35 ust. 5	☐	
KRYTERIUM 5: UPRZEDNIA (REGULACYJNA) OCENA SKUTKÓW *Czy planowane operacje przetwarzania zostały już poddane wcześniejszemu procesowi oceny?*	art. 35 ust. 10	☐	
KRYTERIUM 6: ZWOLNIENIE DLA OKREŚLONYCH ZAWODÓW *Czy planowane operacje dotyczą przetwarzania danych osobowych klientów lub pacjentów przez pojedynczych lekarzy, pracowników służby zdrowia lub prawników, a w konsekwencji dane nie są przetwarzane na dużą skalę?*	motyw 91	☐	
KRYTERIUM 6 BIS: ZATWIERDZONE KODEKSY POSTĘPOWANIA *Czy zatwierdzony kodeks postępowania wyłącza planowane operacje przetwarzania z procesu oceny skutków dla ochrony danych?*	art. 40	☐	
[Inne, por. krok 2a; doprecyzować]		☐	
Czy administrator danych jest zwolniony z procesu OSOD?		☐	**Zwolniony** *[przejść do kroku 1c]*
		☐	**Nie zwolniony** *[przejść do kroku 2]*
W przypadku zwolnienia, czy proces OSOD zostanie przeprowadzony dobrowolnie?		☐	**Tak** *[przejść do kroku 2]*
		☐	**Nie** *[przejść do kroku 1c]*

KROK 1C: OŚWIADCZENIE O BRAKU ISTOTNEGO WPŁYWU EXTRA

[Jeżeli kryteria od 1 do 3bis włącznie NIE są spełnione, to dlaczego planowane operacje przetwarzania są nieobjęte procesem OSOD?]

KOMENTARZE

[Wypełnić]

KROK 2* OKREŚLENIE ZAKRESU

Cel

Celem tego kroku jest identyfikacja, z możliwie dostępną precyzją:

a) punktu odniesienia (benchmarku), czyli określonego standardu podstawowego prawa do ochrony danych osobowych oraz powiązanych podstawowych praw i wolności odzwierciedlonych w obowiązujących ramach prawnych;

b) kategorii interesariuszy, tj. tych, którzy mają być zaangażowani w proces oceny i określenie ich zaangażowania na każdym etapie (techniki angażowania interesariuszy);

c) technik oceny, innych niż ocena niezbędności i proporcjonalności oraz ocena ryzyka, które mają być stosowane w procesie oceny, jeśli takie istnieją;

d) innych technik ewaluacji, które mogą być uzasadnione lub niezbędne.

Realizacja

PUNKT ODNIESIENIA (BENCHMARK). W procesie oceny skutków dla ochrony danych (OSOD) punkt odniesienia obejmuje określony standard: (a) podstawowego prawa do ochrony danych osobowych oraz (b) innych podstawowych praw i wolności, na które wpływ mają planowane operacje przetwarzania (por. art. 1 ust. 2; motyw 4). Na tym etapie oceniający mapują te elementy dotyczące praw i wolności, których planowane operacje przetwarzania danych będą dotyczyć. (Nie wszystkie operacje przetwarzania powodują automatyczne uruchomienie całości odpowiednich przepisów, w tym RODO). Ponieważ prawa i wolności osób fizycznych są usankcjonowane przez wiele aktów prawnych oraz innych instrumentów regulacyjnych, równocześnie odbywa się zmapowanie ram prawnych obowiązujących w danej jurysdykcji.

INTERESARIUSZE. W tym kroku oceniający następnie identyfikują kategorie interesariuszy, z którymi należy się skonsultować. Przede wszystkim są to osoby, których dane dotyczą (np. pracownicy, klienci, pacjenci, studenci, uczniowie lub emeryci) lub ich przedstawiciele (np. organizacje pozarządowe, stowarzyszenia lub grupy interesów). Konsultacje powinny obejmować również inne osoby zainteresowane, osoby wpływające na planowane operacje przetwarzania, osoby których przetwarzanie dotyczy, osoby zainteresowane przetwarzaniem lub ich przedstawicieli, a także ekspertów. Interesariusze są rozumiani szeroko, a ich zasięg i liczba jest współmierna do operacji przetwarzania. Interesariusze mogą także zasugerować innych interesariuszy. (Konkretne osoby, grupy lub organizacje, z którymi należy się skonsultować, są określane w *kroku 3*). Interesariusze nie są oceniającymi; dostarczają danych wejściowych, które oceniający następnie uwzględniają lub odrzucają.

W porównaniu z typowym spektrum zaangażowania interesariuszy (począwszy od zakomunikowania, aż do współdecydowania), RODO umieszcza ich zaangażowanie pośrodku, na poziomie konsultacji. Ich opinie są zbierane i brane pod uwagę. Niemniej, administrator może z własnej woli zdecydować o wyższym poziomie zaangażowania interesariuszy w dany proces OSOD.

Możliwe techniki zaangażowania interesariuszy obejmują różnorodne wydarzenia (warsztaty, grupy fokusowe, sądy obywatelskie), badania (wywiady, ankiety, ustrukturyzowane lub częściowo ustrukturyzowane kwestionariusze) aż po oświadczenia pisemne.

TECHNIKI OCENY. W procesie oceny skutków dla ochrony danych RODO przewiduje zastosowanie dwóch rodzajów technik oceny: (a) ocena niezbędności i proporcjonalności (art. 35 ust. 7 lit. b) oraz (b) ocena ryzyka (art. 35 ust. 7 lit. c). Jeśli te dwa elementy okażą się niewystarczające do podjęcia decyzji, można zastosować inne techniki oceny, np. analizę (planowanie) scenariuszy, prognozowanie technologii lub analizę kosztów i korzyści (ang. *CBA*). RODO nie określa dokładnie, jaką technikę oceny należy zastosować, pozostawiając wybór administratorowi. Techniki oceny są naukowo uzasadnione, zgodne z prawem i powtarzalne (tj. audytor lub sędzia mógłby zweryfikować wyniki przy użyciu tej samej metody).

INNE TECHNIKI EWALUACJI. Osoby oceniające mogą skorzystać z innych technik oceny, gdy jest to uzasadnione lub wymagane przez prawo, np. aby zapewnić kompletność informacji wykorzystywanych w procesie decyzyjnym. Przykładowo, jeśli planowane operacje przetwarzania wpływają *również* na środowisko naturalne lub środowisko człowieka, wraz z procesem OSOD uzasadnione lub wymagane przez prawo może być przeprowadzenie samodzielnego

procesu oceny oddziaływania na środowisko. Analizę kosztów i korzyści można natomiast zastosować jako samodzielną technikę oceny w celu określenia, czy korzyści z planowanych operacji przetwarzania przewyższają ich koszty.

Ponadto, ze względu na kompleksowość i skuteczność, można zintegrować różne rodzaje oceny skutków i inne techniki oceny, pod warunkiem, że punkty odniesienia lub techniki oceny są wzajemnie spójne, nie są sobie podporządkowane ani wewnętrznie sprzeczne. Następnie oceniający dokonują syntezy wyników zintegrowanego procesu oceny.

KROK 2A: PUNKT ODNIESIENIA (BENCHMARK)

Punkt odniesienia (1): Obowiązujące przepisy prawne i regulacje

	Obowiązujące przepisy prawne i regulacje	*Podstawa prawna*	*Stosowalne?*	*Uzasadnienie*
lex generalis	Ogólne rozporządzenie o ochronie danych (RODO)		☒	
	Przepisy krajowe uzupełniające RODO		☒	
	Dyrektywa 2016/680 [transpozycja krajowa]		☐	
	[Inne, doprecyzować]		☐	
lex specialis	Dyrektywa o prywatności i łączności elektronicznej [transpozycja krajowa]		☐	
	Wykaz krajowych wyłączeń/włączeń	art. 35 ust. 4 i 5	☐	
	Zatwierdzony kodeks postępowania	art. 40	☐	
	Certyfikaty	art. 42	☐	
	Decyzje w sprawie adekwatności	art. 45	☐	
	Wiążące reguły korporacyjne	art. 47	☐	
	Standardowe klauzule umowne	art. 46 ust. 2 lit. c), d); art. 46 ust. 3 lit. a);	☐	
	[Inne, doprecyzować]		☐	

inne	Rozporządzenie 2018/1725		☐	
	Standardy techniczne		☐	
	Polityka ochrony danych		☐	
	Kodeks etyki zawodowej *(np. etyka, ład korporacyjny, itp.)*		☐	
	Umowy o wymianie danych		☐	
	[Inne, doprecyzować]		☐	

Punkt odniesienia (2): Zakres procesu oceny

	Zakres procesu oceny		*Podstawa prawna*	*Stosowalne?*	*Uzasadnienie*
Prawo do ochrony danych osobowych	Zasady ochrony danych osobowych		art. 5	☒	
	Podstawa prawna dla przetwarzania		art. 6–8	☒	
	Przetwarzanie szczególnych kategorii danych osobowych		art. 9–10	☐	
	Prawa osoby, której dane dotyczą	Przejrzystość i informacja	art. 12–14	☒	
		Prawo dostępu	art. 15	☒	
		Prawo do sprostowania	art. 16	☒	
		Prawo do usunięcia danych („prawo do bycia zapomnianym”)	art. 17	☐	
		Prawo do ograniczenia przetwarzania	art. 18	☒	
		Prawo do przenoszenia danych	art. 20	☐	
		Prawo do sprzeciwu	art. 21	☐	
		Prawo do niepodlegania procesowi zautomatyzowanego podejmowania decyzji	art. 22	☐	
	Obowiązki administratora oraz podmiotu przetwarzającego		art. 24–39	☒	
	Transfer danych poza UE/EOG		art. 46–49	☐	
	Ograniczenie obowiązków i praw		art. 23	☐	
	Szczególne sytuacje związane z przetwarzaniem		art. 85–91	☐	
	[Inne, doprecyzować]			☐	

Inne prawa podstawowe	Prawo do poszanowania życia prywatnego i rodzinnego, domu oraz komunikowania się	motyw 4	☐	
	Wolności myśli, sumienia i religii		☐	
	Wolność wypowiedzi i informacji		☐	
	Wolność prowadzenia działalności gospodarczej		☐	
	Prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu		☐	
	Prawo do różnorodności kulturowej, religijnej i językowej		☐	
	[Inne podstawowe prawa, doprecyzować]	Karta Praw Podstawowych UE	☐	
[Inne aspekty ochrony danych osobowych, doprecyzować]			☐	

KROK 2B: INTERESARIUSZE, POZIOM I TECHNIKI ZAANGAŻOWANIA

Interesariusze wewnętrzni

Kategoria interesariusza	*Zaangażowany?*	*Poziom zaangażowania*	*Techniki zaangażowania interesariusza*	*Uzasadnienie*
Podmiot(y) przetwarzający(-e) dane	☐			
Inspektor(zy) ochrony danych	☐			
Odbiorcy (art. 4 ust. 9)	☐			
Przedstawiciel(e) (art. 27)	☐			
Specjalista(-ci) ds. bezpieczeństwa informacji	☐			
Obsługa prawna	☐			
Pracownicy, związki zawodowe, kontrahenci itp.	☐			
[Inne, doprecyzować]	☐			

Interesariusze zewnętrzni

Kategoria interesariusza	*Zaangażowany?*	*Poziom zaangażowania*	*Techniki zaangażowania interesariuszy*	*Uzasadnienie*
Osoby, których dane dotyczą, uwzględniając: ▪ małoletnich ▪ osoby wymagające szczególnej opieki ▪ *[inne, doprecyzować]*	☐			
Przedstawiciel(e) osób, których dane dotyczą	☐			
Osoby, których dane nie dotyczą	☐			
Przedstawiciel(e) osób, których dane nie dotyczą	☐			
Strony trzecie (art. 4 ust. 10) – sektor publiczny	☐			
Strony trzecie (art. 4 ust. 10) – sektor prywatny	☐			
Eksperci	☐			
Organ(y) nadzoru	☐			
[Inni, których dotyczy itp.; doprecyzować]	☐			

Brak zaangażowania interesariuszy

[Jeżeli interesariusze nie mają być zaangażowani w obecny proces OSOD, wyjaśnić dlaczego.]

KROK 2C: TECHNIKI OCENY

	Rodzaje technik oceny	*Podstawa prawna*	*Stosowalne?*	*Konkretne techniki*	*Uzasadnienie*
Obowiązkowe	Ocena niezbędności i proporcjonalności	art. 35 ust. 7 lit. b)	☒		
	Ocena ryzyka (prawa i wolności osób fizycznych)	art. 35 ust. 7 lit. c)	☒		
	[Inne, por. krok 2a*; doprecyzować]*		☐		
Uzupełniające	Ocena ryzyka (bezpieczeństwo danych)		☐		
	Planowanie scenariusza		☐		
	Analiza kosztów i korzyści		☐		
	Mocne i słabe strony, szanse, zagrożenia (tzw. analiza SWOT)		☐		
	[Inne, doprecyzować]		☐		

KROK 2D: INNE TECHNIKI OCENY

Rodzaje technik oceny	*Stosowalne?*	*Szczególne techniki*	*Uzasadnienie*
Ocena oddziaływania na środowisko (ang. *EIA*)	☐		
Ocena wpływu na prywatność (ang. *PIA*)	☐		
Ocena wpływu na aspekty etyczne	☐		
Ocena wpływu społecznego	☐		
Ocena wpływu na zdrowie	☐		
Ocena ryzyka	☐		
Analiza kosztów i korzyści (ang. *CBA*)	☐		
Mocne i słabe strony, szanse, zagrożenia (analiza SWOT)	☐		
[Inne, doprecyzować]	☐		

ZINTEGROWANA OCENA SKUTKÓW

	Uzasadnienie
Elementy punktu odniesienia (benchmarku)	
Techniki oceny	
[Inne, doprecyzować]	

KOMENTARZE

[Wypełnić]

KROK 3* PLANOWANIE I PRZYGOTOWANIE

Cel

Celem tego kroku jest określenie szczegółowych warunków przeprowadzenia danego procesu OSOD. Krok ten odpowiada na pytanie jak przeprowadzić dany proces, stanowiąc jego pisemną instrukcję podlegającą ewentualnej aktualizacji w trakcie procesu oceny. Warto zaznaczyć, że nie wszystkie jego elementy mają identyczne znaczenie i równy poziom stosowalności.

Realizacja

SZCZEGÓŁOWE CELE DANEGO PROCESU OSOD. Na poziomie ogólnym, merytorycznym celem procesu OSOD jest zapewnienie możliwie najwyższego poziomu ochrony jednostek, których dane osobowe będą przetwarzane w ramach planowanych operacji. *Formalnym* celem jest zapewnienie zgodności z prawem (por. Art. 35 ust. 7 lit. d). Proces OSOD dąży do realizacji obu celów poprzez wspomaganie procesu decyzyjnego dot. uruchomienia i kształtu planowanych operacji przetwarzania. Ponadto, administrator precyzyjnie wyjaśnia szczegółowe cele danego procesu oceny.

KRYTERIA AKCEPTACJI NEGATYWNYCH SKUTKÓW (DLA OCHRONY DANYCH). Administrator ustala i uzasadnia kryteria progu akceptacji negatywnych skutków, poniżej którego operacja przetwarzania zostanie uznana za zbędną lub nieproporcjonalną. Bierze przy tym pod uwagę kontekst prawny lub kulturowy. Próg jest ustalony i uzasadniony dla każdej zastosowanej techniki oceny (por. *krok 2c*).

Administrator ustala również próg, powyżej którego ryzyko naruszenia prawa nie byłoby akceptowalne, biorąc pod uwagę kontekst prawny czy kulturowy oraz nastawienie do ryzyka (np. skłonność lub niechęć do ryzyka). Innymi słowy, administrator określa poziom akceptowalnego ryzyka. Ponadto, administrator określa z góry zarówno skalę prawdopodobieństwa[2] ryzyka jak i wagi ryzyka.

DEDYKOWANE ZASOBY. Administrator wylicza i zapewnia zasoby niezbędne do przeprowadzenia procesu OSOD, które obejmują między innymi: czas (godziny, dni lub miesiące, które należy poświęcić na wykonanie całego procesu OSOD); pieniądze (koszt pracy, wyposażenia, zaangażowania interesariuszy itp.); siłę roboczą (liczba osób zatrudnionych w niepełnym lub pełnym wymiarze godzin, które mają być zaangażowane w proces); wiedzę (doświadczenie osób oceniających, np. prawne, etyczne, informatyczne, umiejętność korzystania z danych, zarządzanie projektami, public relations itp.); know-how (doświadczenie wymagane od osób zaangażowanych w proces OSOD); pomieszczenia (miejsca) w których zostanie przeprowadzony proces i infrastruktura (zasoby wymagane do przeprowadzenia procesu, np. sprzęt i oprogramowanie). Osoby oceniające mogą skorzystać z oprogramowania, które ułatwia proces poprzez jego częściową automatyzację.

PROCEDURY I RAMY CZASOWE. Administrator ustala ramy czasowe dla procesu OSOD, określając np. najważniejsze etapy, terminy, a także przypisując obowiązki osobom oceniającym i określając, kto jest przed kim odpowiedzialny w ramach struktury organizacyjnej administratora.

(ZESPÓŁ) OCENIAJĄCY, ROLA I ODPOWIEDZIALNOŚĆ. Proces oceny wymaga wielu rodzajów specjalistycznej wiedzy. Administrator, na podstawie przejrzystych kryteriów, wybiera oceniających z wewnątrz lub spoza organizacji (outsourcing). Zespół oceniający może być zmieniany lub powiększany w miarę postępów procesu oceny. Jeśli proces podlega outsourcingowi, w całości lub w części, administrator powinien zawrzeć umowę o świadczenie usług z zewnętrznymi oceniającymi. Administrator określa przy tym ich role i obowiązki (np. do kogo osoby oceniające raportują) i zapewnia ich niezależność zawodową (np. oceniający nie zwracają się o instrukcje ani ich nie otrzymują; ich stronniczość jest natomiast wyraźnie oznaczona jako taka).

INTERESARIUSZE. Opierając się na kategoriach uprzednio zdefiniowanych w *kroku 2b*, oceniający identyfikują interesariuszy, mając na uwadze ich różnorodność (np. równowagę płci, różnorodność geograficzną, różnorodność wiekową lub wielodyscyplinarność) oraz – jeśli mają być zastosowane jakiekolwiek techniki bezpośredniego zaangażowania interesariuszy – również ich dane kontaktowe. W zależności od długości, lista interesariuszy może być

[2] Polskie słowo „prawdopodobieństwo" znajduje w języku angielskim dwa odpowiedniki: „*likelihood*" oraz „*probability*". Pierwsze z nich ma zazwyczaj szersze znaczenie, obejmuje jakościowe, eksperckie metody analizy oraz metody matematyczne związane z rachunkiem prawdopodobieństwa. Częsta interpretacja drugiego słowa odnosi się wyłącznie do matematycznych metod szacowania prawdopodobieństwa. Rozróżnienie to jest podkreślone np. w normie ISO 31000:2018 w pkt. 3.7. Zważywszy, że prawodawca zastosował w angielskiej wersji językowej RODO słowo „*likelihood*" w odniesieniu do prawdopodobieństwa, jest ono stosowane w tym szerokim znaczeniu również w ochronie danych osobowych (przyp. tłum.).

wypełniona w tym szablonie lub dołączona do niego. W przypadku konsultacji prowadzonych na dużą skalę, konieczne może być opracowanie planu konsultacji. Dane osobowe zidentyfikowanych interesariuszy muszą być odpowiednio chronione.

CIĄGŁOŚĆ. Administrator zapewnia ciągłość procesu oceny w przypadku np. zmian w podmiotach zaangażowanych w proces (np. administrator, podmioty przetwarzające, oceniający itp.), zakłóceń, klęsk żywiołowych lub awarii mediów.

REWIZJA. Administrator określa kryteria powodujące rewizję procesu oceny. RODO przewiduje w tym zakresie minimalne kryterium w postaci zmiany poziomu ryzyka (por. art. 35 ust. 11) (por. *krok 8*).

KROK 3A: CELE PROCESU OCENY

Cel	*Stosowalne?*	*Uzasadnienie*
Ochrona osób fizycznych	☒	
Zgodność z prawem	☒	
[Inne, doprecyzować]	☐	

KROK 3B: KRYTERIUM AKCEPTACJI NEGATYWNYCH SKUTKÓW

Metoda oceny		*Uzasadnienie*
Niezbędność oraz proporcjonalność (art. 35 ust. 7 lit. b)		
EXTRA Kryteria ograniczenia praw człowieka (art. 52 ust. 1 Karty Praw Podstawowych UE)		
Ocena ryzyka (jakościowa, ilościowa) *(kryteria ryzyka)*	Skala prawdopodobieństwa	
	Skala wagi	
	Próg akceptacji	
[Inne, doprecyzować]		

KROK 3C: DEDYKOWANE ZASOBY

	Wartość	*Uzasadnienie*
Czas (*jak długo?)*		
Pieniądze (*ile?*)		
Zasoby ludzkie (*ile osób?*)		
Wiedza (*jakie kompetencje/jaka ekspertyza?)*		
Know-how (*jakie doświadczenia?*)		
Lokal (*gdzie?*)		
Infrastruktura (*za pomocą jakich środków?*)		
[Inne, doprecyzować]		

KROK 3D: PROCEDURY I RAMY CZASOWE PROCESU OCENY

	Cel pośredni	*Termin*	*Odpowiedzialność*	*Nadzór*
1	*[Doprecyzować]*			
2				

KROK 3E: OSOBY OCENIAJĄCE, ROLA I ODPOWIEDZIALNOŚĆ

	Imię i nazwisko	*Organizacja (jeśli zewnętrzna)*	*Dane kontaktowe*	*Kompetencje*	*Rola oraz odpowiedzialność*	*Inne informacje*
1	*[Uzupełnić]*				*[Lider]*	
2						

KROK 3F: INTERESARIUSZE

[Podać dane kontaktowe wszystkich interesariuszy zaangażowanych w obecny proces OSOD oraz plan konsultacji, jeśli to konieczne.]

KROK 3G: CIĄGŁOŚĆ PROCESU OCENY

[W jaki sposób obecny proces oceny byłby kontynuowany w przypadku zakłóceń, reorganizacji administratora itp.?]

KROK 3H: KRYTERIA WYWOŁUJĄCE REWIZJĘ PROCESU OSOD

Kryterium	*Stosowalne?*	*Uzasadnienie*
Zmiana prawdopodobieństwa lub waga ryzyka	☒	
[Inne, doprecyzować]	☐	

KOMENTARZE

[Wypełnić]

POWTARZALNE KROKI W FAZIE I

KROK A ZAANGAŻOWANIE INTERESARIUSZY

Cel

Celem tego kroku jest prowadzenie konsultacji oraz zasięganie opinii na temat planowanych operacji przetwarzania od osób, których dane dotyczą lub ich przedstawicieli (art. 35 ust. 9), o ile jest to możliwe.

EXTRA Dodatkowo, oceniający mogą zdecydować o zaangażowaniu większej liczby interesariuszy na szerszą skalę.

Realizacja

Interesariusze są identyfikowani, informowani oraz angażowani, a ich opinie są brane pod uwagę.

Interesariusze, których kategorie zostały określone w *kroku 2b,* są następnie identyfikowani w *kroku 3f*. Ich zaangażowanie ma charakter ciągły, oznaczający konsultacje kwestii ujętych w ramach każdego z kroków. (Zaangażowanie interesariuszy jest usystematyzowane według kolejnych faz procesu oceny).

Podawane informacje powinny charakteryzować się solidnością i dokładnością, jednocześnie będąc wyczerpującymi i istotnymi. Informacje są przekazywane interesariuszom prostym językiem, co może wiązać się z koniecznością przygotowania określonej dokumentacji, np. briefingów o charakterze technicznym. Zaangażowanie interesariuszy następuje z należytym poszanowaniem poufności, m.in. tajemnic państwowych, handlowych, danych osobowych lub innych zastrzeżonych informacji.

Po zebraniu opinii interesariuszy, oceniający rozważają je i zajmują stanowisko w sprawie ich ewentualnej akceptacji; oceniający przedstawiają przy tym wyczerpujące uzasadnienie, szczególnie w przypadku braku akceptacji.

Zarówno zaangażowanie interesariuszy jak i kontrola jakości (por. *krok B*) podlegają raportowaniu po zakończeniu każdej fazy procesu oceny. Po pierwszej fazie oceniający oraz organy kontroli jakości są zainteresowani tym, czy decyzja o przeprowadzeniu OSOD była właściwa, a jeśli tak, to czy zakres procesu oceny i zakres podjętych działań były prawidłowe. Po drugiej fazie przedmiotem ich zainteresowania jest przede wszystkim dokonanie prawidłowej oceny skutków. Po trzeciej fazie, jeśli została uruchomiona, rozważeniu podlegają pozostałe ryzyka i ich prawidłowa ocena, a także pytanie, czy proces oceny wymaga ponownego przeprowadzenia.

	Zidentyfikowani interesariusze	*Jakie informacje zostały przekazane interesariuszom?*	*Jaki wkład wnieśli interesariusze (np. opinię)?*	*W jaki sposób uwzględniono ich wkład?* *Dlaczego został odrzucony?*
Wewnętrzni	Podmiot(y) przetwarzający(-e) dane			
	Inspektor(zy) ochrony danych			
	Odbiorcy (art. 4 ust. 9)			
	Przedstawiciel(e) (art. 27)			
	Specjalista(-ci) ds. bezpieczeństwa informacji			
	Obsługa prawna			

	Pracownicy, związki zawodowe, kontrahenci itp.				
	[Inni, doprecyzować]				
Zewnętrzni	Osoby, których dane dotyczą				
	Przedstawiciele osób, których dane dotyczą				
	Osoby, których dane nie dotyczą				
	Przedstawiciele osób, których dane nie dotyczą				
	Strony trzecie (art. 4 ust. 10)	sektor publiczny			
		sektor prywatny			
	Eksperci				
	Organ(y) nadzoru				
	[Inni, doprecyzować]				

Brak zaangażowania interesariuszy w obecnej fazie

[Jeżeli interesariusze nie są zaangażowani w obecnej fazie procesu OSOD, wyjaśnić dlaczego.]

KROK B* KONTROLA JAKOŚCI

Cel

Celem tego równoległego kroku jest prowadzenie na przestrzeni całego procesu OSOD wewnętrznej lub zewnętrznej weryfikacji jego zgodności z określonym standardem wykonania oraz usunięcie, w razie konieczności, wszelkich nieprawidłowości.

Realizacja

Kontrola jakości może mieć charakter wewnętrzny lub zewnętrzny i przybierać formę monitorowania, przeglądu, audytu itp. Administrator może wymagać od zespołu oceniającego sprawozdań (regularnych lub *ad hoc*) o postępach procesu oceny. Może on także wdrożyć narzędzie monitorujące postępy lub powołać wewnętrzną radę doradczą. (Niezależność zawodowa osób oceniających powinna zostać zagwarantowana.) Równocześnie inspektor ochrony danych ma za zadanie monitorowanie procesu OSOD i doradztwo w jego zakresie. Zewnętrzna kontrola jakości może być przeprowadzona przez organizację audytową zatrudnioną przez administratora lub alternatywnie przez organ nadzoru – na żądanie administratora lub z własnej inicjatywy tego organu (np. gdy wymaga tego prawo).

Kontrola jakości może być ustrukturyzowana, ciągła (powtarzalna na wszystkich etapach procesu) lub wykonywana doraźnie; może być formalna (np. dotycząca zgodności z procedurami procesu OSOD) lub merytoryczna (np. weryfikacja, czy ryzyko zostało odpowiednio ocenione); może wystąpić w trakcie procesu lub po jego zakończeniu. W przypadku roszczeń sądowych, sądy dokonają oceny procesu OSOD pod względem formy lub treści.

Organ kontroli jakości	*Jaką informację zwrotną otrzymano?*	*W jaki sposób informacja zwrotna została uwzględniona? Dlaczego została odrzucona?*
Inspektor(zy) ochrony danych		
Organ nadzoru		
[Inne, doprecyzować]		

Brak kontroli jakości w obecnej fazie

[Jeżeli jakość nie była kontrolowana na obecnym etapie procesu OSOD, wyjaśnić dlaczego.]

KOMENTARZE

[Wypełnić]

FAZA II: OCENA

KROK 4 SYSTEMATYCZNY OPIS

Cele

Celem tego kroku jest, poprzez rozszerzenie wstępnego opisu (por. *krok 1a*), systematyczne opisywanie planowanych operacji przetwarzania, zarówno pod względem kontekstowym jak i technicznym.

Realizacja

Systematyczny opis odnosi się zarówno do kontekstowych jak i technicznych aspektów planowanych operacji przetwarzania, a także wszelkich innych istotnych informacji w tym zakresie. Aspekty kontekstowe dotyczą charakteru (tj. nieodłączne cechy), zakresu (rozmiaru oraz skali, np. czasu trwania, budżetu, złożoności itp.), kontekstu wewnętrznego i zewnętrznego (tj. okoliczności) oraz celów planowanych operacji przetwarzania, a także, w stosownych przypadkach, prawnie uzasadnionego interesu administratora. Diagram przepływu danych lub inne wizualizacje mogą zostać załączone. Niniejszy opis może być oparty na rejestrach czynności przetwarzania (art. 30). Unika się stwierdzeń o charakterze ogólnym. Opis może ulegać zmianom w miarę postępu prac w ramach procesu oceny.

Systematyczny opis rozszerza opis wstępny (por. *krok 1a*), w związku z czym jest obszerniejszy. Musi być przy tym wystarczająco kompletny, dokładny i wiarygodny, ponieważ stanowi podstawę do analizy skutków w *kroku 5*.

ZWIĘZŁY OPIS PLANOWANEGO PRZEDSIĘWZIĘCIA

[Opis]

SZCZEGÓŁOWY OPIS PLANOWANEGO PRZEDSIĘWZIĘCIA

			Opis	
Opis kontekstowy	**Charakter** (*jaki rodzaj operacji przetwarzania? np. zbieranie, przechowywanie, usuwanie, itp.*)		1	
			2	
			…	
	Zakres	Skala (*jak wiele? O jakim zasięgu*)		
		Czas (*kiedy? Jak długo?*)		
	Kontekst (*w jakich okolicznościach*?)	Wewnętrzny (*dotyczący administratora*)		
		Zewnętrzny (*dotyczący poszczególnych osób, grup, społeczeństwa itp.*)		
	Cel operacji przetwarzania, w tym, w stosownych przypadkach, uzasadniony interes (*dlaczego?*)			
	EXTRA **Korzyści** z operacji przetwarzania	Dla osób, w tym dla tych, których dane dotyczą		
		Dla administratora		
		Dla całego społeczeństwa		
	EXTRA **Wady** operacji przetwarzania	Dla osób, w tym dla tych, których dane dotyczą		
		Dla administratora		
		Dla całego społeczeństwa		
Opis techniczny	Kategorie danych osobowych (*jakie?*) ▪ *Szczególne kategorie danych osobowych* ▪ *Dane osób wymagających szczególnej opieki (np. dzieci)* ▪ *Dane o wysoce osobistym charakterze*			

Środki przetwarzania (infrastruktura) (*za pomocą jakich środków?*)	
Planowane przepływy danych (*skąd dokąd? Od kogo do kogo?*)	
Bezpieczeństwo danych (*w jaki sposób jest zapewnione?*)	
Jurysdykcja/rynek (*gdzie?*)	
Podmioty w „łańcuchu dostaw” (*kto?*)	
[Inne, doprecyzować]	

SCHEMAT PRZEPŁYWU DANYCH (OSOBOWYCH) LUB INNE WIZUALIZACJE

[Wstawić schemat]

KOMENTARZE

[Wypełnić]

KROK 5 OCENA SKUTKÓW

Cele

Uwzględniając cele planowanych operacji przetwarzania, w niniejszym kroku ocenie podlega niezbędność oraz proporcjonalność planowanych operacji, a także ewentualne ryzyko naruszenia praw i wolności osób fizycznych wynikające z tych operacji.

Realizacja

Osoby oceniające stosują określone techniki oceny, zdefiniowane uprzednio w *kroku 2c,* opierając swoją analizę na wynikach *kroku 4*. Oceniający mogą zastosować odpowiednią spośród dostępnych metod lub skorzystać z metody zaproponowanej w niniejszym szablonie. W przeciwieństwie do metod oceny ryzyka (np. standardów międzynarodowych, takich jak ISO 31000:2018 lub ISO 27005:2018), metody oceny proporcjonalności i niezbędności w kontekście ochrony danych osobowych są stosunkowo nieliczne.

OCENA NIEZBĘDNOŚCI I PROPORCJONALNOŚCI. Ocena niezbędności i proporcjonalności może odbywać się na dwóch poziomach. Po pierwsze, każda operacja przetwarzania danych jest oceniana pod kątem zasad ochrony danych osobowych (por. *poziom 1*). Są to: zgodność z prawem, rzetelność i przejrzystość, ograniczenie celu, minimalizacja danych, prawidłowość, ograniczenie przechowywania, integralność i poufność (art. 5 ust. 1), w tym bezpieczeństwo przetwarzania (art. 32) a także uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych (art. 25). Każda operacja przetwarzania danych jest oceniana w tabeli, która następnie musi zostać skopiowana dla kolejnych operacji.

EXTRA Biorąc pod uwagę fakt, że w grę wchodzi prawo podstawowe, oraz że proces oceny planowanych operacji przetwarzania, postrzegany wyłącznie pod kątem zasad ochrony danych osobowych (poziom 1) może nie zawsze być wystarczająco kompletny, ze szkodą dla poziomu ochrony i jakości w procesie decyzyjnym, któremu ma służyć, oceniający mogą rozszerzyć przedmiot oceny na całość kryteriów dotyczących ograniczenia praw człowieka. Innymi słowy, przy założeniu, że całość przepisów RODO, a zwłaszcza zasady ochrony danych osobowych, została stworzona z poszanowaniem kryteriów dot. ograniczenia praw człowieka (art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej; KPP UE) (poziom 1), nadal mogą istnieć przypadki, które podważałyby takie założenie. W takiej sytuacji przetwarzanie będące przedmiotem oceny musi zostać zbadane pod kątem całości kryteriów dotyczących ograniczenia (poziom 2). Na przykład, pomimo domniemania zgodności z prawami podstawowymi, przepis RODO może być w całości lub w części z nimi sprzeczny; podobnie może się stać z krajowym wyłączeniem lub odstępstwem od RODO (np. przetwarzanie do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej; art. 85). Szersza ocena może jednak mieć zastosowanie tylko do określonych administratorów danych lub do określonych operacji przetwarzania danych (np. zadania wykonywanego w interesie publicznym).

Ponieważ prawa do ochrony danych osobowych i (większość) pokrewnych praw podstawowych nie są prawami bezwzględnymi, lecz względnymi (tj. ingerencja w takie prawo może być uzasadniona tylko pod pewnymi warunkami), pięć kryteriów dot. ograniczenia zgodnie z art. 52 KPP UE można czytać następująco:

- *legalność* (tj., jeżeli podstawa operacji przetwarzania danych jest „przewidziana ustawą" o wystarczającej jakości, np. przejrzystość, dostępność, precyzja, przewidywalność, zgodność z zasadą praworządności);
- poszanowanie *istoty prawa* (tj. jeżeli ingerencja w prawo podstawowe nie uniemożliwia wykonania prawa);
- *zasadność* (jeśli operacja przetwarzania służy określonemu „interesowi ogólnemu" (por. np. art. 3 Traktatu o Unii Europejskiej; TUE) lub „ochronie praw i wolności innych osób");
- *niezbędność* (tj. jeśli operacja przetwarzania jest „konieczna i [jeśli] rzeczywiście odpowiada" uzasadnionym celom);
- *proporcjonalność sensu stricto (ważenie*) (np. wyważenie, czy wybrano najmniej inwazyjne rozwiązanie).

Ponadto argumentuje się, zgodnie z doktryną, że należy także ocenić *adekwatność* operacji przetwarzania, tj. czy operacja przetwarzania jest odpowiednia, aby osiągnąć dany prawnie uzasadniony cel (czy kiedykolwiek jest w stanie doprowadzić do osiągnięcia zamierzonego celu).

Na mocy art. 52 ust. 3 KPP UE, „znaczenie i zakres" praw, w tym kryteria dot. ich ograniczenia, „są takie same jak praw przyznanych przez tę konwencję" (Europejska Konwencja Praw Człowieka; EKPCz).

OCENA RYZYKA. Na gruncie RODO ryzyko rozumiane jest jako negatywne konsekwencje wynikające z operacji przetwarzania, które mogą, ale nie muszą mieć miejsca w przyszłości. W przypadku zaistnienia spowodowałoby uszczerbek fizyczny, majątkową lub niemajątkową szkodę osobom fizycznym (w dużej mierze osobom, których dane dotyczą), a *nie* tylko administratorom lub przetwarzającym. Ocena ryzyka ma być jak najbardziej obiektywna (motywy 75–76). Nie zawsze jest to jednak osiągalne w praktyce ze względu na niejasności co do możliwego do przypisania prawdopodobieństwa i rodzajów szkód oraz biorąc pod uwagę „subiektywne" postrzeganie ryzyka przez zainteresowane strony (np. osoby, których dane dotyczą).

Ryzyko jest zwykle oceniane poprzez połączenie dwóch pomiarów, mianowicie prawdopodobieństwa (tj. szansy wystąpienia) oraz jego wagi (tj. skali konsekwencji) (motyw 76). Ryzyko można ocenić jakościowo, ilościowo lub za pomocą kombinacji obu. Istnieją aspekty ochrony danych osobowych, które mieszczą się w pierwszej kategorii (tj. ryzyko naruszenia praw i wolności) i drugiej (np. bezpieczeństwo danych). Ilościowa ocena ryzyka mierzy prawdopodobieństwo wystąpienia ryzyka i łączy je z jego wagą. Prawdopodobieństwo jest wyrażane w skali od 0 do 1. Z kolei jakościowa ocena ryzyka wykorzystuje poziomy prawdopodobieństwa (np. 4-częściową opisową skalę: nieistotne, niskie, średnie i wysokie) do połączenia z jego wagą. Ostatecznie waga ryzyka wskazuje na wielkość szkody w przypadku jego zmaterializowania. Można ją także wyrazić na czterostopniowej skali opisowej. Obie skale – prawdopodobieństwa i wagi – są wstępnie zdefiniowane i uzasadnione w *kroku 3b*.

Typowa metoda oceny ryzyka wymaga przede wszystkim identyfikacji ryzyka, tj. jego znalezienia, rozpoznania i opisania. (Przydatne mogą być tutaj „bazy wiedzy".) W drugim kroku analizuje się ryzyko, w tym jego charakter, w celu określenia poziomu ryzyka, np. poprzez pomnożenie prawdopodobieństwa wystąpienia przez stopień wagi konsekwencji. W trzecim kroku dokonuje się oceny ryzyka, tj. wyniki analizy ryzyka porównuje się z kryteriami akceptacji ryzyka (por. *krok 3b*) w celu ustalenia, czy ryzyko i jego poziom są akceptowalne, czy zalecany jest środek mitygujący i czy jakiekolwiek ryzyko powinno być traktowane priorytetowo. (Postępowanie z ryzykiem wykracza poza proces oceny ryzyka, a zatem stanowi część oddzielnego procesu).

KROK 6 ZALECENIA

Cel

Celem tego kroku jest zaproponowanie środków zaradczych mitygujących ryzyka oraz wyeliminowanie zbędnych i nieproporcjonalnych operacji przetwarzania, zidentyfikowanych w poprzednim kroku. Założeniem jest ochrona osób fizycznych oraz wykazanie zgodności z prawem „z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy" (art. 35 ust. 7 lit. d).

EXTRA Oceniający mogą zasugerować środki maksymalizujące pozytywne skutki.

Realizacja

Oceniający zalecają i opisują środki mitygujące dla wszelkich rodzajów negatywnego wpływu (w tym ryzyk oraz nieproporcjonalnych i niepotrzebnych ingerencji w prawa człowieka) zidentyfikowanych w *kroku 5*. Zalecenia stanowią zobowiązanie starannego działania a nie zobowiązanie rezultatu.

Dla każdej zasady ochrony danych osobowych (poziom 1) lub kryterium dla ograniczenia praw człowieka (poziom 2), które *nie* zostały zrealizowane na poprzednim etapie, oceniający zalecają środki zapewniające realizację tych zasad lub wypełnienie kryteriów.

Każde ryzyko jest ograniczane poprzez manewrowanie jego prawdopodobieństwem – np. poprzez ograniczenie narażenia na ryzyko, lub jego nasileniem – np. poprzez przygotowanie planu postępowania z ryzykiem na wypadek zmaterializowania się ryzyka, albo jedno i drugie. Ryzyka można uniknąć, zredukować je, przenieść (na inny podmiot, np. outsourcing, ubezpieczenie albo przeniesienie w czasie) lub zaakceptować. Ryzyko szczątkowe (ryzyko rezydualne) to takie, które pozostaje po zastosowaniu środków mitygujących wynikających z zaleceń. Jeżeli pomimo zastosowanych środków ryzyko szczątkowe pozostaje wysokie, powoduje to konieczność przeprowadzenia uprzednich konsultacji z organem nadzoru (por. *krok 7*).

Zarówno w przypadku ryzyka, jak i zbędności i nieproporcjonalności, środki mitygujące mogą mieć charakter regulacyjny (prawny), techniczny, organizacyjny lub behawioralny. (Przydatne mogą być tutaj bazy wiedzy). Oceniający mogą najpierw podsumować działania uprzednio zaplanowane lub wdrożone. Krok ten kończy się wraz z implementacją przez

oceniających planu wdrożeniowego, w którym wyznacza się osobę odpowiedzialną za realizację każdego działania i jego termin.

Po otrzymaniu raportu, kierownictwo administratora podejmuje decyzję o realizacji planowanego przedsięwzięcia i warunkach, na jakich może ono być realizowane, jeśli zdecydowano się kontynuować przedsięwzięcie. Tym samym, wraz z otrzymaniem raportu, kierownictwo administratora zajmuje stanowisko w sprawie każdego z zaleceń wystosowanych przez oceniających. Jeśli zdecyduje się odrzucić lub zmienić którekolwiek z nich – przedstawia wyczerpujące uzasadnienie. Co więcej, po uzgodnieniu z administratorem, niektóre zalecenia mogą zostać wdrożone już w trakcie procesu oceny.

NIEZBĘDNOŚĆ I PROPORCJONALNOŚĆ OPERACJI PRZETWARZANIA

Poziom 1: Zasady ochrony danych osobowych

Identyfikator operacji przetwarzania	
Rodzaj operacji przetwarzania	

KROK 5 OCENA SKUTKÓW						**KROK 6 ZALECENIA**				
						Plan reagowania, jeśli zasada nie jest zrealizowana				
Zasada		*Podstawa prawna*	*Stosowalne?*	*Spełnione?*	*Uzasadnienie*	*Wprowadzone środki*	*Środki do wprowadzenia*	*Osoba odpowiedzialna*	*Priorytet*	*Termin*
Zgodność z prawem	Zgoda	art. 6 ust. 1 lit. a)	☐	☐						
	Umowa	art. 6 ust.1 lit. b)	☐	☐						
	Wypełnienie obowiązku prawnego	art. 6 ust. 1 lit. c)	☐	☐						

	Ochrona życiowych interesów	art. 6 ust. 1 lit. d)	☐	☐						
	Interes publiczny	art. 6 ust. 1 lit. e)	☐	☐						
	Prawnie uzasadnione interesy	art. 6 ust. 1 lit. f)	☐	☐						
Rzetelność		art. 5 ust. 1 lit. a)		☐						
Przejrzystość				☐						
Ograniczenie celu	Konkretny	art. 5 ust. 1 lit. b)		☐						
	Wyraźny			☐						
	Prawnie uzasadniony			☐						
	Bez dalszego przetwarzania			☐						
	(Wyjątki)	art. 89 ust. 1		☐						

Minimalizacja danych	Adekwatne	art. 5 ust. 1 lit. c)	☐						
	Stosowne		☐						
	Ograniczone		☐						
Prawidłowość	Prawidłowy	art. 5 ust. 1 lit. d)	☐						
	Uaktualniany		☐						
Ograniczenie przechowywania	Niezbędny	art. 5 ust. 1 lit. e)	☐						
	(*Wyjątki*)	art. 89 ust. 1	☐						
Bezpieczeństwo danych	Integralność i poufność	art. 5 ust. 1 lit. f)	☐						
	Bezpieczeństwo przetwarzania	art. 32	☐						
Uwzględnianie ochrony danych w fazie projektowania		art. 25 ust. 1	☐						
Domyślna ochrona danych		art. 25 ust. 2	☐						

Poziom 2: Kryteria dot. ograniczenia praw człowieka (art. 52 ust. 1 KPP UE) EXTRA

KROK 5 OCENA SKUTKÓW			**KROK 6 ZALECENIA**				
			Plan postępowania z ryzykiem, jeśli zasady nie są zrealizowane.				
Kryterium	*Spełnione?*	*Uzasadnienie*	*Wprowadzone środki*	*Środki do wprowadzenia*	*Osoba odpowie-dzialna*	*Priorytet*	*Termin*
LEGALNOŚĆ *Czy planowane przedsięwzięcie jest przewidziane przez prawo o wystarczającej jakości?*	☐						
POSZANOWANIE ISTOTY PRAWA *Czy planowane przedsięwzięcie nadal umożliwia korzystanie z podstawowego prawa lub wolności?*	☐						
PROPORCJONALNOŚĆ – ZASADNOŚĆ *Czy planowane przedsięwzięcie służy uzasadnionemu celowi?*	☐						
PROPORCJONALNOŚĆ – ADEKWATNOŚĆ *Czy planowane przedsięwzięcie pozwoli na osiągnięcie celu i jest adekwatne do jego realizacji?*	☐						
PROPORCJONALNOŚĆ – NIEZBĘDNOŚĆ *Czy planowane przedsięwzięcie jest niezbędne do osiągnięcia celu?*	☐						
PROPORCJONALNOŚĆ *SENSU STRICTO* (WAŻENIE) *Czy ingerencja w prawo jest uzasadniona w świetle korzyści wynikających z ochrony konkurencyjnego prawa lub interesu?*	☐						

RYZYKA DLA PRAW I WOLNOŚCI OSÓB FIZYCZNYCH

KROK 5 OCENA SKUTKÓW							**KROK 6 ZALECENIA**							
IDENTYFIKACJA RYZYKA		ANALIZA RYZYKA					OCENA RYZYKA							
							Odpowiedź na ryzyko					*Plan postępowania z ryzykiem*		
ID	*Ryzyko*	*Opis (źródła ryzyka, właściciel ryzyka, itp.)*	*Prawdopodobieństwo wystąpienia* P	*Waga konsekwencji materializacji ryzyka* W	*Poziom ryzyka (wynik)* R = P * W	*Uzasadnienie*	*Rodzaj*	*Opis*	*Skorygowany poziom ryzyka (punktacja) (Czy istnieje pozostałe ryzyko?)* P	W	R	*Wprowadzone środki*	*Środki do wprowadzenia*	*Osoba odpowiedzialna*	*Priorytet*	*Termin*
1	*[Uzupełnić]*															
2																
3																
4																

Matryca ryzyka

Przed zaleceniami	*Po zaleceniach*
[Wstawić schemat]	*[Wstawić schemat]*

INNE TECHNIKI OCENY EXTRA

Ocena	*Zalecenia*
[Uzasadnienie]	*[Uzasadnienie]*

ZALECENIA

	Synteza Zaleceń	*Decyzja administratora wraz z uzasadnieniem*
1	*[Uzasadnienie]*	
2		

	Ogólne zalecenia		*Decyzja administratora wraz z uzasadnieniem*
☐	Wdrożyć przedsięwzięcie bez zmian		
☐	Zmodyfikować przedsięwzięcie	*[Doprecyzować jak]*	
☐	Odwołać przedsięwzięcie	*[Doprecyzować jak]*	

KOMENTARZE

[Wypełnić]

POWTARZALNE KROKI W FAZIE II

KROK A ZAANGAŻOWANIE INTERESARIUSZY

	Zidentyfikowani interesariusze		*Jakie informacje zostały przekazane interesariuszom?*	*Jaki wkład wnieśli interesariusze (np. opinię)?*	*W jaki sposób uwzględniono wkład interesariuszy?* *Dlaczego został odrzucony?*
Wewnętrzni	Podmiot(y) przetwarzający(-e) dane				
	Inspektor(zy) ochrony danych				
	Odbiorcy (art. 4 ust. 9)				
	Przedstawiciel(e) (art. 27)				
	Specjalista(-ci) ds. bezpieczeństwa informacji				
	Obsługa prawna				
	Pracownicy, związki zawodowe, kontrahenci itp.				
	[Inni, doprecyzować]				
Zewnętrzni	Osoby, których dane dotyczą				
	Przedstawiciele osób, których dane dotyczą				
	Osoby, których dane nie dotyczą				
	Przedstawiciele osób, których dane nie dotyczą				
	Strony trzecie (art. 4 ust. 10)	sektor publiczny			
		sektor prywatny			
	Eksperci				

Organ(y) nadzoru			
[Inni, doprecyzować]			

Brak zaangażowania interesariuszy na obecnym etapie

[Jeśli interesariusze nie są zaangażowani w obecną fazę procesu OSOD, wyjaśnić dlaczego.]

KROK B* KONTROLA JAKOŚCI

Organ kontroli jakości	*Jaką informację zwrotną otrzymano?*	*Jak została wdrożona informacja zwrotna?* *Dlaczego została odrzucona?*
Inspektor(zy) ochrony danych		
Organ nadzoru		
[Inne, doprecyzować]		

Brak kontroli jakości na obecnym etapie

[Jeżeli jakość nie była kontrolowana na obecnym etapie procesu OSOD, wyjaśnić dlaczego.]

KOMENTARZE

[Wypełnić]

FAZA III: *KROKI EX POST*

KROK 7 UPRZEDNIE KONSULTACJE Z ORGANEM NADZORU

Cel

Celem tego kroku jest konsultacja z organem nadzoru w przypadku, gdy po przeprowadzeniu procesu OSOD stwierdzono wysoki poziom ryzyka szczątkowego, połączonego z brakiem środków podjętych przez administratora w celu ograniczenia tego ryzyka (art. 36).

Realizacja

Wiele organów nadzoru wymaga użycia specjalnych formularzy (szablonów), z których należy skorzystać, aby wystąpić o uprzednią konsultację; Europejska Rada Ochrony Danych (EROD) prowadzi aktualną listę członkowskich organów nadzoru.

O ile organ nadzoru uzna, że planowane operacje przetwarzania mogą naruszać RODO, przekaże administratorowi pisemne powiadomienie w terminie maksymalnie 8 tygodni. Okres ten może zostać przedłużony o 6 tygodni w zależności od stopnia złożoności wniosku. W razie potrzeby, administrator może po swojej stronie zażądać dodatkowych informacji; spowoduje to zawieszenie wyżej wymienionych terminów. Organ nadzoru może również skorzystać ze wszystkich swoich uprawnień, o których mowa w art. 58.

Właściwy(-e) organ(y) nadzoru	
Data złożenia	
Data otrzymania odpowiedzi	
Zapytanie (podsumowanie)	
Odpowiedź (podsumowanie)	
Decyzja administratora po konsultacji	

KOMENTARZE

[Wypełnić]

KROK 8 REWIZJA

Cel

Celem tego kroku jest podjęcie decyzji, czy i kiedy po wdrożeniu planowanych operacji przetwarzania należy ponownie przeprowadzić proces OSOD, w całości lub w części.

Realizacja

Zgodnie z kryteriami określonymi w *kroku 3h*, administrator dokonuje przeglądu procesu OSOD w razie potrzeby, ale przynajmniej gdy następuje zmiana ryzyka związanego z operacjami przetwarzania, tj. jeżeli charakter, zakres, kontekst lub cel operacji przetwarzania uległ zmianie, a tym samym zmienił się poziom ryzyka (art. 35 ust. 11). W takiej sytuacji należy, w całości lub w części, ponownie przeprowadzić proces OSOD.

Czynniki determinujące zmianę poziomu ryzyka są różnorodne: od modyfikacji operacji przetwarzania danych, przez kontekst ich wdrożenia, aż po zmianę prawa ochrony danych osobowych lub presję społeczną.

EXTRA Niezależnie od zmiany poziomu ryzyka, administrator może ustalić, że proces OSOD należy poddawać regularnym przeglądom, np. co 6 miesięcy, każdego roku etc.

	Kryterium		*Zmiana?*	*Uzasadnienie*
Opis kontekstowy	**Charakter** (*jaki rodzaj operacji przetwarzania? np. zbieranie, przechowywanie, usuwanie, itp.*)		☐	
	Zakres	Skala (*jak wiele? O jakim zasięgu?*)	☐	
		Czas (*kiedy? Jak długo?*)	☐	
	Kontekst (*w jakich okolicznościach* ?)	Wewnętrzny (*dotyczący administratora*)	☐	
		Zewnętrzny (*dotyczący poszczególnych osób, grup, społeczeństwa, itp.*)	☐	
	Cel operacji przetwarzania, w tym, w stosownych przypadkach, uzasadniony interes (*dlaczego?*)		☐	
	EXTRA **Korzyści** z operacji przetwarzania	Dla osób, w tym dla tych, których dane dotyczą	☐	
		Dla administratora	☐	
		Dla całego społeczeństwa	☐	

	EXTRA **Wady** operacji przetwarzania	Dla osób, w tym dla tych, których dane dotyczą	☐	
		Dla administratora	☐	
		Dla całego społeczeństwa	☐	
Opis techniczny	Kategorie danych osobowych *(jakie?)* ▪ *Szczególne kategorie danych osobowych* ▪ *Dane osób wymagających szczególnej opieki (np. dzieci)* ▪ *Dane o wysoce osobistym charakterze*		☐	
	Środki przetwarzania (infrastruktura) (*za pomocą jakich środków?*)		☐	
	Planowane przepływy danych (*skąd dokąd? od kogo do kogo?*)		☐	
	Bezpieczeństwo danych (*w jaki sposób jest zapewnione?*)		☐	
	Jurysdykcja/rynek (*gdzie?*)		☐	
	Podmioty w „łańcuchu dostaw” (*kto?*)		☐	
	[Inne, doprecyzować]		☐	

OGÓLNA REKOMENDACJA

Co zrobić z procesem oceny?		*Kiedy?*	*Decyzja administratora wraz z uzasadnieniem*
☐ Zrewidować	☐ w całości	*[Doprecyzować]*	
	☐ częściowo *[doprecyzować]*	*[Doprecyzować]*	
☐ Nie rewidować	*[Doprecyzować dlaczego]*		

KOMENTARZE

[Wypełnić]

POWTARZALNE KROKI W FAZIE III

KROK A ZAANGAŻOWANIE INTERESARIUSZY

	Zidentyfikowani interesariusze		*Jakie informacje zostały przekazane interesariuszom?*	*Jaki wkład wnieśli interesariusze (np. opinię)?*	*W jaki sposób uwzględniono ich wkład?* *Dlaczego został odrzucony?*
wewnętrzni	Podmiot(y) przetwarzający(-e) dane				
	Inspektor(zy) ochrony danych				
	Odbiorcy (art. 4 ust.9)				
	Przedstawiciel(e) (art. 27)				
	Specjalista(-ci) ds. bezpieczeństwa informacji				
	Obsługa prawna				
	Pracownicy, związki zawodowe, kontrahenci itp.				
	[Inni, doprecyzować]				
zewnętrzni	Osoby, których dane dotyczą				
	Przedstawiciele osób, których dane dotyczą				
	Osoby, których dane nie dotyczą				
	Przedstawiciele osób, których dane nie dotyczą				
	Strony trzecie (Art. 4 ust. 10)	sektor publiczny			
		sektor prywatny			
	Eksperci				
	Organ(y) nadzoru				

[Inni, doprecyzować]			

Brak zaangażowania interesariuszy w obecnej fazie

[Jeżeli interesariusze nie są zaangażowani w obecnej fazie procesu OSOD, wyjaśnić dlaczego.]

KROK B* KONTROLA JAKOŚCI

Organ kontroli jakości	*Jaką informację zwrotną otrzymano?*	*W jaki sposób informacja zwrotna została uwzględniona? Dlaczego została odrzucona?*
Inspektor(zy) ochrony danych		
Organ nadzoru		
[Inne, doprecyzować]		

Brak kontroli jakości w obecnej fazie

[Jeżeli jakość nie była kontrolowana na obecnym etapie procesu OSOD, wyjaśnić dlaczego.]

KOMENTARZE

[Wypełnić]

STRONA KOŃCOWA

ZATWIERDZENIA

Imię i nazwisko	*Rola*	*Uwagi*	*Podpis*	*Data*
	Oceniający			
	Inspektor ochrony danych			
	Administrator(zy) danych			
	[Inne, doprecyzować]			

KROK C* DOKUMENTACJA

Cel

Celem tego kroku o charakterze równoległym jest prowadzenie czytelnej i zrozumiałej dokumentacji wszystkich czynności podejmowanych w ramach danego procesu oceny, przygotowywanej z należytym poszanowaniem uzasadnionej tajemnicy. Dokumentacja może być prowadzona na piśmie lub w innym formacie (analogowym lub cyfrowym) zapewniającym odpowiedni poziom jej trwałości.

Realizacja

Dokumentacja składa się z niniejszego raportu i wymienionych poniżej załączników, zarówno wzorów jak i formularzy końcowych. Oceniający wyliczają przy tym wszystkie działania podjęte w ramach danego procesu oceny, np. przygotowywanie projektów poszczególnych wersji niniejszego raportu lub interakcje z osobami, których dane dotyczą i z organami nadzoru.

Należy zaznaczyć, że w danej jurysdykcji może istnieć (krajowy) rejestr przeprowadzonych procesów oceny skutków dla ochrony danych. Administratorzy mogą być wówczas zobowiązani do przedłożenia sprawozdania z procesu OSOD lub też może istnieć zalecenie w tym zakresie.

Za najlepszą praktykę można uznać udostępnianie publicznie (przynajmniej części) niniejszego sprawozdania z procesu OSOD oraz załączników (np. na stronie internetowej administratora), z należytym poszanowaniem uzasadnionej tajemnicy. Po zrewidowaniu procesu oceny, nowa wersja powinna także zostać udostępniona publicznie, z odpowiednim odniesieniem do poprzedniej wersji dokumentu.

DZIAŁANIA PODJĘTE W TRAKCIE OBECNEGO PROCESU OSOD

Data	*Uczestnik*	*Działanie*	*Opis*	*Komentarze*
[Doprecyzować]				

ZAŁĄCZNIKI

	Załącznik	*Stopień poufności*	*Czy załączone?*	*Komentarze*
Krok 1 Krok 4	Rejestr czynności przetwarzania		☐	
Krok 2	Zatwierdzone kodeksy postępowania		☐	

	Certyfikaty		☐	
	Wiążące reguły korporacyjne		☐	
	Standardowe klauzule umowne		☐	
	Polityka ochrony danych		☐	
	Kodeksy etyki zawodowej		☐	
	Umowy o wymianie danych	poufne	☐	
Krok 3	Kopia umowy o świadczenie usług (gdy OSOD jest przedmiotem outsourcingu)		☐	
	Wykaz i dane konsultowanych interesariuszy do kontaktu	poufne	☐	
	Plan konsultacji interesariuszy		☐	
Krok 7	Wniosek o uprzednią konsultację z organem nadzoru		☐	
	Odpowiedź od organu nadzoru		☐	
Krok A	Briefingi techniczne do konsultacji z interesariuszami		☐	
	Konsultacje z interesariuszami (raporty)		☐	
	Opinia inspektora ochrony danych (raport)		☐	
	[Raporty z innych technik oceny, doprecyzować]		☐	
	[Inne, doprecyzować]		☐	

KOMENTARZE

[Wypełnić]

2 UWAGI KOŃCOWE

W niniejszym dokumencie d.pia.lab zaproponowało szablon procesu OSOD dla UE/EOG, który opiera się na interpretacji wymogów prawnych RODO i odzwierciedla najlepsze praktyki w zakresie oceny skutków dla ochrony danych. Kształt niniejszego dokumentu nie ma waloru ostateczności. Obecnie zostanie on poddany testom, a następnie, w miarę wzrostu doświadczenia z jego użycia, stosownym przeglądom. W związku z powyższym d.pia.lab pozostaje otwarte na wszelkie uwagi na temat proponowanego szablonu, które zostaną uwzględnione m.in. w jego kolejnych aktualizacjach.

Jednocześnie, struktura, metodyka oraz szablon nie wyczerpują „architektury" oceny skutków dla ochrony danych. Dalsze elementy, głównie o charakterze technicznym, takie jak lista potencjalnych zagrożeń dla praw i wolności jednostek oraz odpowiadająca im lista możliwych środków zaradczych (tzw. „bazy wiedzy"), muszą zostać opracowane i przetestowane, a wraz ze wzrostem doświadczenia z ich użycia także właściwie zrewidowane. D.pia.lab podejmie się niniejszego w swojej dalszej pracy.

WYBRANE STOSOWNE ŹRÓDŁA

Margaret Hagan (n.d.), *Law by Design*, https://www.lawbydesign.co.

Kloza, Dariusz, Niels van Dijk, Raphaël Gellert, István Böröcz, Alessia Tanas, Eugenio Mantovani and Paul Quinn (2017) "Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals", *d.pia.lab Policy Brief* No. 1/2017, VUB: Brussels. https://cris.vub.be/files/32009890/dpialab_pb2017_1_final.pdf.

Kloza, Dariusz, Niels van Dijk, Simone Casiraghi, Sergi Vazquez Maymir, Sara Roda, Alessia Tanas and Ioulia Konstantinou (2019) "Towards a method for data protection impact assessment: Making sense of GDPR requirements", *d.pia.lab Policy Brief* No. 1/2019, VUB: Brussels. https://cris.vub.be/files/48091346/dpialab_pb2019_1_final.pdf.

Möller, Kai (2012) "Proportionality: Challenging the Critics", *International Journal of Constitutional Law*, 10(3), 709–731. doi: 10.1093/icon/mos024.

Peers, Steve, and Sacha Prechal (2015) "Article 52: Scope and Interpretation of Rights and Principles", in: Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds.) *The EU Charter of Fundamental Rights: A Commentary*, 1455–1522, Hart Publishing: London. doi: 10.5040/9781849468350.ch-056.

DALSZE POZYCJE: KLUCZOWE POJĘCIA

Barak, Aharon (2012) *Proportionality: Constitutional Rights and their Limitations*, Cambridge University Press: Cambridge. doi: 10.1017/CBO9781139035293.

Brkan, Maja (2019) "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning", *German Law Journal*, 20(6), 864–883. doi: 10.1017/glj.2019.66.

DALSZE POZYCJE: PRAKTYCZNE WSKAZÓWKI

Agencia Española de Protección de Datos [AEPD] (2018) *Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD*, Madrid. https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf.

Article 29 Working Party (2017) *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP248 rev. 01, Brussels. http://ec.europa.eu/newsroom/document.cfm?doc_id=47711.

Commission Nationale de l'Informatique et des Libertés [CNIL] (2018) *Privacy Impact Assessment (PIA) 3: knowledge bases*, Paris. https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf.

European Data Protection Supervisor [EDPS] (2018) *Accountability on the ground. Part II: Data Protection Impact Assessments & Prior Consultation*, Brussels. https://edps.europa.eu/sites/edp/files/publication/18-02-06_accountability_on_the_ground_part_2_en.pdf.

EDPS (2017) *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, Brussels. https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf.

EDPS (2019) *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, Brussels. https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

International Association of Privacy Professionals [IAPP] (2020) *2020 Privacy Tech Vendor Report*, Portsmouth, NH. https://iapp.org/resources/article/privacy-tech-vendor-report.

International Organization for Standardization [ISO] (2018) *Risk management – Guidelines*, ISO 31000:2018, Geneva. https://www.iso.org/iso-31000-risk-management.html.

ISO (2018) *Information technology – Security techniques – Information security risk management*, ISO 27005:2018, Geneva. https://www.iso.org/standard/75281.html.

ISO (2018) *Security and resilience – Business continuity management systems – Requirements*, ISO 22301:2019, Geneva. https://www.iso.org/standard/75106.html.

Mays, Claire (2004) *Stakeholder Involvement Techniques. Short Guide and Annotated Bibliography*, Organisation for Economic Co-operation and Development (OECD), Paris. http://www.oecd-nea.org/rwm/reports/2004/nea5418-stakeholder.pdf.

Sammut-Bonnici, Tanya, and David Galea (2015) "SWOT Analysis", in: Cary L. Cooper (ed.) *Wiley Encyclopedia of Management*, 1-8, John Wiley & Sons: Chichester. doi: 10.1002/9781118785317.weom120103.

NA TEMAT D.PIA.LAB

Brukselskie Laboratorium ds. Oceny Skutków na Prywatność i Ochronę Danych (d.pia.lab) łączy badania podstawowe, metodologiczne i stosowane; organizuje szkolenia i doradztwo w zakresie polityki związanej z ocenami wpływu w obszarach innowacji i rozwoju technologii. Zważywszy, że prawne aspekty prywatności i ochrony danych osobowych stanowią jego główny przedmiot zainteresowania, Laboratorium uwzględnia jednak w swoich pracach także inne dyscypliny, w tym etykę, filozofię, studia nt. inwigilacji oraz studia nad nauką i techniką (ang. STS). Powstałe w listopadzie 2015 roku Laboratorium bazuje na doświadczeniach Grupy Badawczej ds. Prawa, Nauki, Technologii i Społeczeństwa (LSTS) będącej częścią Vrije Universiteit Brussel (VUB) w Belgii.

Laboratorium zbudowało swoją bazę wiedzy w zakresie ocen wpływu z wielu ukończonych jak i trwających projektów badawczych, takich jak PERSONA, HR-RECYCLER i SYSTEM (współfinansowane przez UE). Poglądy wyrażone w niniejszym Policy Brief nie odzwierciedlają poglądów żadnej z agencji finansujących.

Dziękujemy – w kolejności alfabetycznej – następującym osobom: Jonas Breuer, Athena Christofi, Roger Clarke, Katerina Demetzou, Pierre Dewitte, Laura Drechsler, Rossana Ducato, Anna Johnston, Kristoffer Lidén, Gianclaudio Malgieri, Rotem Medzini, Anna Mościbroda, Laurens Naudts, Juraj Sajfert, Mistale Taylor oraz Heidi Waem za ich komentarze do wcześniejszych wersji niniejszego dokumentu. Tłumaczenie na język polski: Paweł Uściński (maj 2021), Maciej Otmianowski (konsultacje językowe).

dpialab.org | **dpialab@vub.ac.be**