Wytyczne nr 4/2019 dotyczące artykułu 25

Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

Wersja 2.0

Przyjęte 20 października 2020 r.

Historia wersji

Wersja 1.0	13 listopada 2019 r.	Przyjęcie wytycznych do konsultacji publicznych
Wersja 2.0	20 października 2020 r.	Przyjęcie wytycznych przez EROD po konsultacjach publicznych

Spis treści

Europejska Rada Ochrony Danych

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO"),

uwzględniając Porozumienie EOG, a w szczególności załącznik XI do niego i jego protokół 37, w brzmieniu zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.,

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

PRZYJMUJE NINIEJSZE WYTYCZNE:

Streszczenie

W świecie, w którym postępuje proces cyfryzacji, przestrzeganie wymogów ochrony danych w fazie projektowania oraz domyślnej ochrony danych odgrywają niezwykle ważną rolę w promowaniu prywatności i ochrony danych w społeczeństwie. Istotne jest zatem, aby administratorzy poważnie podchodzili do swojej odpowiedzialności i wdrażali zobowiązania wynikające z RODO przy projektowaniu operacji przetwarzania.

Niniejsze wytyczne zawierają ogólne wskazówki dotyczące obowiązku ochrony danych w fazie projektowania oraz domyślnej ochrony danych określonego w art. 25 RODO. Ochrona danych w fazie projektowania oraz domyślna ochrona danych dotyczą wszystkich administratorów danych, niezależnie od wielkości i stopnia złożoności przetwarzania danych. Aby można było wdrożyć wymogi ochrony danych w fazie projektowania oraz domyślnej ochrony danych, administrator danych powinien rozumieć zasady ochrony danych oraz prawa i wolności osoby, której dane dotyczą.

Głównym obowiązkiem jest wdrożenie *odpowiednich* środków i niezbędnych zabezpieczeń, które zapewnią *skuteczną realizację zasad ochrony danych,* a zatem również *praw i wolności osób, których dane dotyczą, już w fazie projektowania oraz jako domyślnej ochrony danych*. W art. 25 określono elementy dotyczące zarówno fazy projektowania, jak i domyślnej ochrony danych, które należy uwzględnić. Elementy te zostaną bardziej szczegółowo omówione w niniejszych wytycznych.

Artykuł 25 ust. 1 stanowi, że administratorzy powinni uwzględnić ochronę danych w fazie projektowania oraz domyślną ochronę danych odpowiednio wcześnie, na etapie planowania kolejnej operacji przetwarzania. Wdrażają oni ochronę danych w fazie projektowania oraz domyślną ochronę danych *przed* przetwarzaniem, a także *w sposób ciągły* podczas przetwarzania, dokonując regularnych przeglądów skuteczności wybranych środków i zabezpieczeń. Ochronę danych w fazie projektowania oraz domyślną ochronę danych stosuje się również do istniejących systemów, które przetwarzają dane osobowe.

Wytyczne zawierają również wskazówki dotyczące sposobów skutecznego wdrażania zasad ochrony danych określonych w art. 5, w ramach których wymieniono kluczowe elementy dotyczące ochrony danych w fazie projektowania i domyślnej ochrony danych, a także przykłady praktycznych rozwiązań. Administrator powinien rozważyć trafność proponowanych środków w kontekście określonego przetwarzania danych, o którym mowa.

EROD przedstawia zalecenia dotyczące sposobu, w jaki administratorzy, podmioty przetwarzające i producenci mogą współpracować w celu realizacji obowiązku ochrony danych w fazie projektowania oraz domyślnej ochrony danych. Zachęca także administratorów z branży, podmioty przetwarzające i producentów, aby stosowali ochronę danych w fazie projektowania oraz domyślną ochronę danych jako metodę, która umożliwi im uzyskanie przewagi konkurencyjnej podczas wprowadzania ich produktów do obrotu względem administratorów i osób, których dane te dotyczą. Nakłania również wszystkich administratorów danych do stosowania certyfikatów i kodeksów postępowania.

1 ZAKRES STOSOWANIA

1. Niniejsze wytyczne dotyczą przede wszystkim wdrażania ochrony danych w fazie projektowania oraz domyślnej ochrony danych przez administratorów zgodnie z obowiązkiem określonym w art. 25 RODO.[1] Inne podmioty, takie jak podmioty przetwarzające oraz wytwórcy produktów, usług i aplikacji (zwani dalej „wytwórcami"), do których art. 25 nie odnosi się bezpośrednio, mogą również uznać niniejsze wytyczne za użyteczne w wytwarzaniu produktów i usług zgodnych z RODO, umożliwiających administratorom wypełnianie ich obowiązków w zakresie ochrony danych.[2] W motywie 78 RODO wprowadzono zapis, że ochronę danych w fazie projektowania oraz domyślną ochronę danych należy uwzględnić w kontekście przetargów publicznych. Mimo że wszyscy administratorzy mają obowiązek włączenia ochrony danych w fazie projektowania oraz domyślnej ochrony danych do swoich czynności przetwarzania, przepis ten wspiera przyjęcie zasad, zgodnie z którymi administracje publiczne powinny dawać przykład. Administrator jest odpowiedzialny za realizację obowiązków w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrony danych z tytułu przetwarzania danych przez jego podmioty przetwarzające i podmioty podprzetwarzające i powinien to uwzględniać przy zawieraniu umów z tymi stronami.

2. Wymóg opisany w art. 25 zobowiązuje administratorów do uwzględnienia zasad ochrony danych już w fazie projektowania i jako domyślnej ochrony; ma to zastosowanie przez cały czas trwania procesu przetwarzania. Wymóg ochrony danych w fazie projektowania oraz domyślnej ochrony danych obejmuje również systemy przetwarzania danych istniejące przed wejściem w życie RODO. Administratorzy są zobowiązani do bieżącej aktualizacji przetwarzania danych zgodnie z RODO. Więcej informacji na temat sposobu utrzymania istniejącego systemu w zgodności z ochroną danych w fazie projektowania oraz domyślną ochroną danych znajduje się w podrozdziale 2.1.4 niniejszych wytycznych. Istotą tego przepisu jest zapewnienie *odpowiedniej* i *skutecznej* ochrony danych, zarówno *w fazie projektowania*, jak i *domyślnej ochrony*, co oznacza, że administratorzy danych powinni być w stanie wykazać, że dysponują odpowiednimi środkami i zabezpieczeniami w zakresie przetwarzania danych, aby zapewnić skuteczność zasad ochrony danych oraz praw i wolności osób, których dane dotyczą.

[1] Przedstawione tu interpretacje mają w równym stopniu zastosowanie do art. 20 dyrektywy (UE) 2016/680 i art. 27 rozporządzenia 2018/1725.

[2] W motywie 78 RODO wyraźnie wskazano tę konieczność: „Jeżeli opracowywane, projektowane, wybierane i użytkowane są aplikacje, usługi i produkty, które opierają się na przetwarzaniu danych osobowych albo przetwarzają dane osobowe w celu realizacji swojego zadania, należy zachęcać wytwórców tych produktów, usług i aplikacji, by podczas opracowywania i projektowania takich produktów, usług i aplikacji wzięli pod uwagę prawo do ochrony danych osobowych i z należytym uwzględnieniem stanu wiedzy technicznej zapewnili administratorom i podmiotom przetwarzającym możliwość wywiązania się ze spoczywających na nich obowiązków ochrony danych".

3. W rozdziale drugim niniejszych wytycznych skoncentrowano się na wykładni wymogów określonych w art. 25 oraz przeanalizowano zobowiązania prawne wprowadzone tym przepisem. W rozdziale trzecim przedstawiono przykłady dotyczące zastosowania ochrony danych w fazie projektowania oraz domyślnej ochrony danych w kontekście szczególnych zasad ochrony danych.

4. W rozdziale czwartym wytycznych omówiono możliwość ustanowienia mechanizmu certyfikacji w celu wykazania zgodności z art. 25, a w rozdziale piątym – sposoby egzekwowania przepisów tego artykułu przez organy nadzorcze. Ponadto wytyczne zawierają zalecenia dla zainteresowanych stron, dotyczące skutecznego wdrażania ochrony danych w fazie projektowania oraz domyślnej ochrony danych. EROD dostrzega trudności, z jakimi borykają się małe i średnie przedsiębiorstwa (zwane dalej „MŚP"), aby w pełni wypełnić obowiązki w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrony danych, i przedstawia dodatkowe zalecenia dla MŚP, które zawarto w rozdziale szóstym.

2 ANALIZA ART. 25 UST. 1 I UST. 2 UWZGLĘDNIANIE OCHRONY DANYCH W FAZIE PROJEKTOWANIA ORAZ DOMYŚLNA OCHRONA DANYCH

5. Celem niniejszego rozdziału jest przeanalizowanie i sformułowanie wytycznych dotyczących wymogów w zakresie ochrony danych w fazie projektowania określonych w art. 25 ust. 1 oraz domyślnej ochrony danych, o której mowa w art. 25 ust. 2. Ochrona danych w fazie projektowania oraz domyślna ochrona danych są pojęciami, które wzajemnie się uzupełniają i wzmacniają. Osoby, których dane dotyczą, odniosą większe korzyści z domyślnej ochrony danych, jeżeli będzie ona realizowana równocześnie z ochroną danych w fazie projektowania – i odwrotnie.

6. Ochrona danych w fazie projektowania oraz domyślna ochrona danych jest wymogiem, któremu podlegają wszyscy administratorzy, łącznie z małymi przedsiębiorstwami i korporacjami wielonarodowymi. W tym przypadku poziom złożoności procesu wdrażania ochrony danych w fazie projektowania oraz domyślnej ochrony danych może zależeć od poszczególnych operacji przetwarzania danych. Niezależnie jednak od ich skali, wprowadzenie ochrony danych w fazie projektowania oraz domyślnej ochrony danych może w każdym przypadku przynieść korzyści administratorom danych i osobom, których dane dotyczą.

2.1 Artykuł 25 ust. 1: Uwzględnianie ochrony danych w fazie projektowania

2.1.1 Obowiązek administratora polegający na wdrażaniu odpowiednich środków technicznych i organizacyjnych oraz niezbędnych zabezpieczeń w odniesieniu do przetwarzania

7. Zgodnie z art. 25 ust. 1 administrator wdraża *odpowiednie* środki techniczne i organizacyjne zaprojektowane w celu realizacji zasad ochrony danych oraz włączenia w proces przetwarzania *niezbędnych zabezpieczeń*, aby spełnić wymogi oraz chronić prawa i wolności osób, których dane dotyczą. Zarówno odpowiednie środki, jak i niezbędne zabezpieczenia, mają służyć temu samemu celowi polegającemu na ochronie praw osób, których dane dotyczą, oraz na zapewnieniu, aby ochrona ich danych osobowych stanowiła część przetwarzania.

8. *Środki techniczne i organizacyjne* oraz niezbędne *zabezpieczenia* mogą być rozumiane w szerokim znaczeniu jako dowolna metoda lub środek, które administrator może zastosować w procesie przetwarzania. Sformułowanie *odpowiednie* oznacza, że środki i niezbędne zabezpieczenia powinny

być dostosowane do osiągnięcia zamierzonego celu, to znaczy, że muszą one *skutecznie* realizować zasady ochrony danych[3]. Wymóg dotyczący odpowiedniości jest zatem ściśle związany z wymogiem dotyczącym skuteczności.

9. Środkiem technicznym lub organizacyjnym oraz zabezpieczeniem może być dowolne działanie, począwszy od zastosowania zaawansowanych rozwiązań technicznych, po podstawowe przeszkolenie pracowników. Przykłady, które mogą okazać się odpowiednie, w zależności od kontekstu i ryzyka związanego z danym przetwarzaniem, obejmują pseudonimizację[4] danych osobowych; przechowywanie danych osobowych dostępnych w ustrukturyzowanym formacie, powszechnie nadającym się do odczytu maszynowego; umożliwienie osobom, których dane dotyczą ingerencji w przetwarzanie; dostarczanie informacji na temat przechowywania danych osobowych; dysponowanie systemami wykrywania złośliwego oprogramowania; szkolenie pracowników w zakresie podstawowej higieny pracy w cyberprzestrzeni; wdrażanie systemów zarządzania prywatnością i bezpieczeństwem informacji, zobowiązujących umownie podmioty przetwarzające do wdrożenia określonych praktyk w zakresie minimalizacji danych itp.

10. Normy, najlepsze praktyki i kodeksy postępowania, honorowane przez stowarzyszenia i inne organy reprezentujące poszczególne kategorie administratorów, mogą być przydatne w ustalaniu odpowiednich środków. Administrator musi jednak sprawdzić, czy środki te są odpowiednie w odniesieniu do przedmiotowego przetwarzania danych.

2.1.2 Zaprojektowane w celu skutecznej realizacji zasad ochrony danych i ochrony praw i wolności osób, których dane dotyczą

11. *Zasady ochrony danych* określono w art. 5 (dalej zwane „zasadami"), *prawa i wolności osób, których dane dotyczą* stanowią podstawowe prawa i wolności osób fizycznych, w szczególności zaś ich prawo do ochrony danych osobowych, których ochrona została określona w art. 1 ust. 2 jako cel RODO (dalej zwane „prawami")[5]. Ich dokładne brzmienie znajduje się w Karcie praw podstawowych Unii Europejskiej. Ważne jest, aby administrator danych rozumiał znaczenie *zasad* i *praw* jako podstawy ochrony udzielanej na podstawie RODO, a zwłaszcza na podstawie obowiązku w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrony danych.

12. W przypadku wdrażania odpowiednich środków technicznych i organizacyjnych, środki i zabezpieczenia powinny być *zaprojektowane* z uwzględnieniem skutecznego wdrożenia każdej z wyżej wymienionych zasad i wynikającej z nich ochrony praw.

Omówienie kwestii skuteczności

13. Skuteczność jest pojęciem leżącym u podstaw uwzględniania ochrony danych w fazie projektowania. Wymóg skutecznego wdrożenia zasad oznacza, że administratorzy muszą wdrożyć niezbędne środki i zabezpieczenia w celu ochrony tych zasad, aby zagwarantować prawa osobom, których dane dotyczą. Każdy wdrożony środek powinien przynieść zamierzone rezultaty w odniesieniu do przetwarzania przewidzianego przez administratora. Spostrzeżenie to ma dwojakie konsekwencje.

14. Po pierwsze, oznacza to, że postanowienia art. 25 nie wymagają wdrożenia określonych środków technicznych i organizacyjnych, ale wskazują, że wybrane środki i zabezpieczenia powinny odnosić się konkretnie do wdrożenia zasad ochrony danych w ramach określonego przetwarzania. Tym samym

[3] Kwestię „skuteczności" omówiono poniżej w podrozdziale 2.1.2.
[4] Zdefiniowana w art. 4 ust. 5 RODO.
[5] Zobacz motyw 4 RODO.

środki i zabezpieczenia należy zaprojektować w taki sposób, aby były solidne, zaś administrator powinien mieć możliwość wdrożenia dodatkowych środków w celu dostosowania ich do potencjalnego wzrostu ryzyka[6]. Skuteczność środków będzie zatem zależeć od kontekstu danego przetwarzania oraz oceny niektórych elementów, które należy wziąć pod uwagę, określając sposoby przetwarzania. Wspomniane wyżej elementy omówiono poniżej w podrozdziale 2.1.3.

15. Po drugie, administratorzy powinni być w stanie wykazać zgodność z obowiązującymi zasadami.

16. Wdrożone środki i zabezpieczenia powinny zapewnić osiągnięcie pożądanego efektu w zakresie ochrony danych, natomiast administrator powinien posiadać dokumentację dotyczącą wdrożonych środków technicznych i organizacyjnych.[7] W tym celu administrator może określić odpowiednie główne wskaźniki skuteczności działania, aby potwierdzić ich skuteczność. Wskaźnik skuteczności działania jest mierzalną wartością wybraną przez administratora danych, która pokazuje, na ile skutecznie osiąga on swój cel w zakresie ochrony danych. Wskaźniki te mogą być *ilościowe*, takie jak odsetek fałszywych wyników pozytywnych lub fałszywych wyników negatywnych, zmniejszenie liczby skarg, skrócenie czasu reakcji, gdy osoby, których dane dotyczą korzystają ze swoich praw; lub *jakościowe*, takie jak oceny działania, stosowanie skali ocen lub oceny ekspertów. Zamiast stosowania wskaźników skuteczności działania administratorzy mogą wykazać, że zasady są skutecznie wdrażane, przedstawiając uzasadnienie oceny skuteczności wybranych środków i zabezpieczeń.

2.1.3 Elementy wymagające uwzględnienia

17. W art. 25 ust. 1 wymieniono elementy, jakie administrator musi uwzględnić przy określaniu środków dotyczących konkretnej operacji przetwarzania. Poniżej przedstawiono wytyczne dotyczące zastosowania tych elementów w fazie projektowania, w tym również projektowania ustawień domyślnych. Wszystkie te elementy pomagają ustalić, czy dany środek jest odpowiedni do skutecznego wdrożenia zasad. Z tego względu każdy z tych elementów nie stanowi celu samego w sobie, ale jest jednym z czynników, które należy uwzględnić łącznie, aby osiągnąć cel.

2.1.3.1 „stan wiedzy technicznej”

18. Pojęcie „stanu wiedzy technicznej” jest obecne w różnych elementach dorobku prawnego UE, np. w dziedzinie ochrony środowiska i bezpieczeństwa produktów. W RODO odniesienie do „stanu wiedzy technicznej”[8] występuje nie tylko w art. 32 w stosunku do środków bezpieczeństwa[9][10], lecz także w

[6] „Podstawowe zasady obowiązujące administratorów (tj. zasada zgodności z prawem, minimalizacji danych, ograniczenia celu, przejrzystości, integralności danych, prawidłowości danych) powinny pozostać bez zmian, niezależnie od przetwarzania i ryzyka dla osób, których dane dotyczą. Należyte uwzględnienie charakteru i zakresu takiego przetwarzania zawsze było jednak integralną częścią stosowania tych zasad, aby były z natury skalowalne”. Grupa Robocza Art. 29. „Stanowisko w sprawie podejścia opartego na ryzyku w ramach prawnych ochrony danych”. WP 218, 30 maja 2014 r., s. 3. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[7] Zob. motywy 74 i 78.

[8] Zobacz decyzja niemieckiego Federalnego Trybunału Konstytucyjnego w sprawie „Kalkar” z 1978 r.: https://germanlawarchive.iuscomp.org/?p=67, która może stanowić podstawę metodyki obiektywnej definicji pojęcia. Na tej podstawie poziom „stanu wiedzy technicznej” będzie określany w przedziale między poziomem technologicznym „istniejącej wiedzy naukowej i istniejących badań naukowych” a bardziej ugruntowanymi „ogólnie przyjętymi zasadami technologii”. „Stan wiedzy technicznej” można zatem określić jako poziom technologiczny usługi lub technologii lub produktu, który istnieje na rynku i jest najbardziej skuteczny w osiąganiu wyznaczonych celów.

[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security

[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

art. 25, rozszerzając tym samym zakres odniesienia na wszystkie środki techniczne i organizacyjne uwzględniane przy przetwarzaniu.

19. W kontekście art. 25 odniesienie do „stanu wiedzy technicznej" nakłada na administratorów obowiązek **uwzględnienia obecnego postępu w zakresie technologii** dostępnych na rynku przy określaniu odpowiednich środków technicznych i organizacyjnych. Od administratorów wymaga się więc, aby dysponowali aktualną wiedzą w zakresie postępu technologicznego i na bieżąco śledzili jego rozwój; w jaki sposób technologia może stwarzać ryzyko lub możliwości dla operacji przetwarzania danych; oraz w jaki sposób wdrażać i aktualizować środki i zabezpieczenia służące *bezpiecznej i skutecznej realizacji* zasad i praw osób, których dane dotyczą, biorąc pod uwagę zmieniający się krajobraz technologiczny.

20. „Stan wiedzy technicznej" jest dynamicznym pojęciem, którego nie można definiować statycznie w określonym czasie, ale należy go oceniać *na bieżąco* w kontekście postępu technologicznego. W obliczu postępu technologicznego administrator może stwierdzić, że środek, który kiedyś zapewniał odpowiedni stopień ochrony, już tego nie czyni. Nieśledzenie zmian technologicznych może zatem skutkować brakiem zgodności z art. 25.

21. Kryterium „stanu wiedzy technicznej" ma zastosowanie nie tylko do środków technologicznych, ale również do środków organizacyjnych. Brak odpowiednich środków organizacyjnych może przyczynić się do obniżenia, a nawet do całkowitego podważenia skuteczności wybranej technologii. Przykładem środków organizacyjnych może być wdrożenie polityki wewnętrznej, szkolenia w zakresie technologii, bezpieczeństwa i ochrony danych oraz strategie bezpieczeństwa technologii informacyjnych i zarządzanie nimi.

22. Istniejące i uznane ramy, standardy, certyfikaty, kodeksy postępowania itp. w różnych dziedzinach mogą mieć znaczenie dla wskazania aktualnego „stanu wiedzy technicznej" w ramach danego obszaru zastosowania. Jeśli normy takie istnieją i zapewniają wysoki stopień ochrony osoby, której dane dotyczą, zgodnie z wymogami prawnymi lub wykraczając poza te wymogi, administratorzy powinni je uwzględniać w fazie projektowania i wdrażania środków ochrony danych.

2.1.3.2 „koszt wdrażania"

23. Administrator może wziąć pod uwagę koszt wdrożenia, wybierając i stosując odpowiednie środki techniczne i organizacyjne oraz niezbędne zabezpieczenia, które zapewniają skuteczną realizację zasad w celu ochrony praw osób, których dane dotyczą. Koszt odnosi się do zasobów ogółem, w tym do czasu i zasobów ludzkich.

24. Element ten nie wiąże się z koniecznością wydatkowania przez administratora nieproporcjonalnie dużych zasobów, jeśli istnieją inne, bardziej ekonomiczne i wciąż skuteczne środki. Koszt wdrożenia jest jednak czynnikiem, który należy uwzględnić przy wdrożeniu ochrony danych w fazie projektowania, nie zaś podstawą do odstąpienia od tego wdrożenia.

25. Wybrane środki muszą więc zapewniać, aby czynność przetwarzania danych przewidziana przez administratora nie odbywała się z naruszeniem zasad, niezależnie od kosztów. Administratorzy powinni być w stanie zarządzać ogólnymi kosztami, aby mogli skutecznie wdrażać wszystkie zasady i, w konsekwencji, chronić prawa.

2.1.3.3 „charakter, zakres, kontekst i cele przetwarzania”

26. Ustalając niezbędne środki, administratorzy muszą brać pod uwagę charakter, zakres, kontekst i cel przetwarzania danych.

27. Czynniki te należy interpretować zgodnie z rolą, jaką pełnią one w innych przepisach RODO, jak na przykład w art. 24, 32 i 35, aby zaprojektować zasady ochrony danych jako część procesu ich przetwarzania.

28. W skrócie, pojęcie **charakteru** można rozumieć jako nieodłączną[11] cechę przetwarzania. **Zakres** odnosi się do wielkości i zasięgu przetwarzania. **Kontekst** związany jest z okolicznościami przetwarzania, które mogą wpływać na oczekiwania osoby, której dane dotyczą, natomiast **cel** odnosi się do celów przetwarzania.

2.1.3.4 „ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania”

29. W wielu przepisach zawartych w art. 24, 25, 32 i 35 RODO przyjęto spójne podejście oparte na ryzyku, aby określić odpowiednie środki techniczne i organizacyjne służące ochronie osób fizycznych, ich danych osobowych oraz zapewnieniu zgodności z wymogami RODO. Aktywa podlegające ochronie są zawsze takie same (osoby fizyczne, przez ochronę ich danych osobowych), są chronione przed takimi samymi zagrożeniami (w odniesieniu do praw i wolności osób fizycznych), z uwzględnieniem tych samych warunków (charakteru, zakresu, kontekstu i celów przetwarzania).

30. Przeprowadzając analizę ryzyka pod kątem zgodności z art. 25, administrator musi określić zagrożenia dla praw osób, których dane dotyczą, jakie stanowi naruszenie zasad, oraz określić prawdopodobieństwo i wagę tych zagrożeń w celu wdrożenia środków służących skutecznemu ich zminimalizowaniu. Systematyczna i gruntowna ocena przetwarzania danych ma kluczowe znaczenie przy dokonywaniu oceny ryzyka. Administrator ocenia na przykład szczególne zagrożenia związane z brakiem dobrowolnie wyrażonej zgody, stanowiącym naruszenie zasady zgodności z prawem, podczas przetwarzania danych osobowych dzieci i młodzieży poniżej 18. roku życia jako grupy szczególnie narażonej, w przypadku gdy nie ma innej podstawy prawnej, i wdraża odpowiednie środki w celu ograniczenia i skutecznego zminimalizowania zidentyfikowanych zagrożeń związanych z tą grupą osób, których dane dotyczą.

31. W „Wytycznych EROD dotyczących oceny skutków dla ochrony danych (DPIA)”[12], w których skoncentrowano się na określeniu, czy operacja przetwarzania może prowadzić do wysokiego ryzyka, przedstawiono również wskazówki dotyczące sposobu oceny ryzyka związanego z ochroną danych oraz sposobu przeprowadzania oceny ryzyka związanego z ochroną danych. Wytyczne te mogą być również przydatne podczas oceny ryzyka w odniesieniu do wszystkich wspomnianych wyżej artykułów, w tym art. 25.

[11] Przykładami są szczególne kategorie danych osobowych, automatyczne podejmowanie decyzji, wypaczone relacje władzy, nieprzewidywalne przetwarzanie, utrudnienia związane z korzystaniem z praw przez osobę, której dane dotyczą itp.

[12] Grupa Robocza Art. 29 „Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie »z dużym prawdopodobieństwem może powodować wysokie ryzyko«, do celów rozporządzenia 2016/679”. WP 248 rev.01, 4 października 2017 r. ec.europa.eu/newsroom/document.cfm?doc_id=47711 – zatwierdzone przez EROD.

32. Podejście oparte na ryzyku nie wyklucza stosowania punktów odniesienia, najlepszych praktyk ani norm. Elementy te mogą stanowić przydatny zestaw narzędzi dla administratorów służący przeciwdziałaniu podobnemu ryzyku w podobnych sytuacjach (charakter, zakres, kontekst i cele przetwarzania). Obowiązek określony w art. 25 (a także w art. 24, 32 i art. 35 ust. 7 lit. c) RODO) polegający na uwzględnieniu „ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikającego z przetwarzania" pozostaje jednak bez zmian. W związku z tym administratorzy, mimo że korzystają z takich narzędzi, muszą zawsze przeprowadzić indywidualną ocenę ryzyka w zakresie ochrony danych w odniesieniu do danej czynności przetwarzania danych oraz sprawdzić skuteczność odpowiednich środków i proponowanych zabezpieczeń. Dodatkowo wymagana może być wówczas ocena skutków dla ochrony danych lub aktualizacja istniejącej oceny skutków dla ochrony danych.

2.1.4 Aspekt dotyczący czasu

2.1.4.1 Przy określaniu sposobów przetwarzania

33. Uwzględnianie ochrony danych w fazie projektowania należy wdrażać *„przy określaniu sposobów przetwarzania"*.

34. Zakres „sposobów przetwarzania" obejmuje elementy projektowe przetwarzania, od ogólnych po szczegółowe, w tym architektura, procedury, protokoły, układ i wygląd.

35. „Czas określania sposobów przetwarzania" odnosi się do okresu, w którym administrator podejmuje decyzję o sposobie, w jaki przetwarzanie będzie prowadzone, oraz o sposobie, w jaki będzie ono przebiegać, a także w kwestii mechanizmów, które zostaną użyte do realizacji takiego przetwarzania. Podczas podejmowania takich decyzji administrator musi ocenić odpowiednie środki i zabezpieczenia w celu skutecznego wdrażania zasad i praw osób, których dane dotyczą, do procesu przetwarzania oraz musi uwzględnić elementy takie jak stan wiedzy technicznej, koszt wdrażania, charakter, zakres, kontekst i cel oraz ryzyko. Należy do nich również czas pozyskania i wdrożenia oprogramowania, sprzętu i usług do przetwarzania danych.

36. Wczesne uwzględnienie ochrony danych w fazie projektowania oraz domyślnej ochrony danych ma kluczowe znaczenie dla pomyślnego wdrożenia zasad i ochrony praw osób, których dane dotyczą. Ponadto, z perspektywy stosunku kosztów do korzyści, w interesie administratora leży szybsze uwzględnienie tej kwestii, ponieważ wprowadzanie zmian do istniejących już planów i zaprojektowanych już operacji przetwarzania mogłoby być trudne i kosztowne.

2.1.4.2 Podczas procesu przetwarzania (utrzymanie i przegląd wymogów w zakresie ochrony danych)

37. Po rozpoczęciu procesu przetwarzania administrator ma stały obowiązek utrzymania ochrony danych w fazie projektowania oraz domyślnej ochrony danych, tj. dalszego skutecznego wdrażania zasad w celu ochrony praw, śledzenia aktualnego stanu wiedzy technicznej, ponownej oceny poziomu ryzyka itd. Charakter, zakres i kontekst operacji przetwarzania, a także ryzyko mogą się zmieniać w toku przetwarzania, co oznacza, że administrator danych musi dokonać ponownej oceny operacji przetwarzania prowadząc regularne przeglądy i oceny skuteczności wybranych środków i zabezpieczeń.

38. Obowiązek utrzymania, przeglądu i aktualizacji, w miarę potrzeby, operacji przetwarzania dotyczy również wcześniej istniejących systemów. Oznacza to, że dotychczasowe systemy zaprojektowane przed wejściem w życie RODO należy poddawać przeglądom i konserwacji, aby zapewnić wdrożenie

środków i zabezpieczeń, które w skuteczny sposób wdrażają zasady i prawa osób, których dane dotyczą, jak określono w niniejszych wytycznych.

39. Zakres tego obowiązku obejmuje również wszelkie procesy przetwarzania prowadzone przez podmioty przetwarzające dane. Operacje podmiotów przetwarzających powinny być poddawane regularnym przeglądom i ocenom przez administratorów w celu zapewnienia, że umożliwiają one stałą zgodność z zasadami i pozwalają administratorowi danych na wykonywanie jego obowiązków w tym zakresie.

2.2 Artykuł 25 ust. 2: Domyślna ochrona danych

2.2.1 Domyślnie przetwarzane są wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania

40. „Wartość domyślna", zgodnie z definicją powszechnie stosowaną w dziedzinie informatyki, odnosi się do istniejącej wcześniej lub wstępnie wybranej wartości konfigurowalnego ustawienia przypisanego do oprogramowania użytkowego (aplikacji), programu komputerowego lub urządzenia. Ustawienia takie nazywane są również „ustawieniami domyślnymi" lub „ustawieniami fabrycznymi", szczególnie w przypadku urządzeń elektronicznych.

41. Dlatego też termin „domyślne" w przypadku przetwarzania danych osobowych odnosi się do podejmowania decyzji dotyczących wartości konfiguracyjnych lub opcji przetwarzania, które są ustawione lub zapisane w systemie przetwarzania, takim jak: aplikacja, usługa lub urządzenie, lub też ręczna procedura przetwarzania, mających wpływ na ilość gromadzonych danych osobowych, zakres ich przetwarzania, okres ich przechowywania i ich dostępność.

42. Administrator powinien wybrać i odpowiadać za wdrożenie domyślnych ustawień ochrony danych i opcji w taki sposób, aby jedynie przetwarzanie, które jest ściśle niezbędne do osiągnięcia określonego, zgodnego z prawem celu, było realizowane domyślnie. W takim przypadku administratorzy muszą polegać na swojej ocenie konieczności (niezbędności) przetwarzania w odniesieniu do podstaw prawnych art. 6 ust. 1. Oznacza to, że domyślnie administrator danych nie gromadzi większej liczby danych niż jest to niezbędne, nie przetwarza zgromadzonych danych w zakresie większym niż jest to niezbędne do realizacji celów, ani nie przechowuje danych dłużej niż jest to niezbędne. Podstawowy wymóg zakłada, że ochrona danych jest domyślnie wbudowana w ich przetwarzanie.

43. Administrator jest zobowiązany wstępnie określić konkretne, wyraźne i prawnie uzasadnione cele gromadzenia i przetwarzania danych osobowych[13]. Środki muszą być w sposób domyślny odpowiednie, aby zapewnić przetwarzanie wyłącznie tych danych osobowych, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. „Wytyczne dotyczące oceny konieczności i proporcjonalności środków ograniczających prawo do ochrony danych osobowych" przygotowane

[13] Artykuł 5 ust. 1 lit. b), c), d), e) RODO.

przez EIOD mogą być również użyteczne przy podejmowaniu decyzji dotyczących tego, które dane są niezbędne do przetworzenia, aby osiągnąć konkretny cel[14] [15] [16].

44. Jeżeli administrator korzysta z oprogramowania osób trzecich lub oprogramowania dostępnego na rynku, powinien przeprowadzić ocenę ryzyka związanego z produktem i upewnić się, że jego funkcje, które nie mają podstawy prawnej lub nie są zgodne z zamierzonymi celami przetwarzania, zostaną wyłączone.

45. Te same względy mają zastosowanie do środków organizacyjnych wspierających operacje przetwarzania. Należy je zaprojektować tak, aby na początku przetwarzać jedynie minimalną ilość danych osobowych, niezbędną do realizacji konkretnych operacji. Trzeba to szczególnie uwzględnić przy udzielaniu dostępu do danych pracownikom o różnych rolach i odmiennych potrzebach w zakresie dostępu.

46. Odpowiednie „środki techniczne i organizacyjne" w kontekście domyślnej ochrony danych są rozumiane w taki sam sposób, jak omówiono powyżej w sekcji 2.1.1, ale mają zastosowanie szczególnie do zasady minimalizacji danych.

47. Wspomniany wcześniej obowiązek polegający na przetwarzaniu wyłącznie tych danych osobowych, które są niezbędne dla osiągnięcia każdego konkretnego celu, ma zastosowanie do następujących elementów:

2.2.2 Wymiary obowiązku minimalizacji danych

48. W art. 25 ust. 2 wyszczególniono wymiary obowiązku minimalizacji danych w przypadku przetwarzania domyślnego, określając przy tym, że obowiązek ten ma zastosowanie do ilości gromadzonych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.

2.2.2.1 „ilości zbieranych danych osobowych"

49. Administratorzy muszą uwzględnić zarówno ilość danych osobowych, jak i rodzaje, kategorie i poziom szczegółowości danych osobowych wymagane do celów przetwarzania. Dokonując wyborów w zakresie projektowania, powinni oni uwzględnić zwiększone ryzyko dla zasad integralności i poufności, minimalizacji danych i ograniczenia ich przechowywania podczas gromadzenia dużych ilości szczegółowych danych osobowych oraz porównać je z ograniczeniem ryzyka podczas gromadzenia mniejszych ilości lub mniej szczegółowych informacji na temat osób, których dane dotyczą. W żadnym przypadku domyślne ustawienia nie mogą obejmować zbierania danych osobowych, które nie są niezbędne do osiągnięcia konkretnego celu przetwarzania. Innymi słowy, jeżeli określone kategorie danych osobowych są zbędne lub jeżeli szczegółowe dane nie są potrzebne, ponieważ mniej szczegółowe dane są wystarczające, nie można gromadzić żadnych nadwyżek danych osobowych.

[14] EIOD. „Wytyczne dotyczące oceny konieczności i proporcjonalności środków ograniczających prawo do ochrony danych". 25 lutego 2019 r. https://edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf

[15] Zob. również EIOD. „Ocena konieczności wprowadzenia środków ograniczających podstawowe prawo do ochrony danych osobowych: zestaw narzędzi" https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en

[16] Więcej informacji na temat konieczności, zob. Grupa Robocza Art. 29. „Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE". WP 217, 9 kwietnia 2014 r. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

50. Te same domyślne wymogi mają zastosowanie do usług niezależnie od tego, jakiej platformy lub jakiego urządzenia użyto. W tym kontekście można gromadzić jedynie dane osobowe niezbędne do realizacji danego celu.

2.2.2.2 „zakresu ich przetwarzania"

51. Operacje przetwarzania[17] przeprowadzane na danych osobowych nie wykraczają poza to, co niezbędne. Wiele operacji przetwarzania może przyczynić się do osiągnięcia celu przetwarzania. Fakt, że pewne dane osobowe są niezbędne do realizacji celu, nie oznacza jednak, że na danych mogą być wykonywane operacje przetwarzania każdego rodzaju i o dowolnej częstotliwości. Administratorzy powinni również uważać, by nie rozszerzać granic „zgodnych celów" określonych w art. 6 ust. 4 i mieć na uwadze taki zakres przetwarzania, który będzie zgodny z uzasadnionymi oczekiwaniami osób, których dane dotyczą.

2.2.2.3 „okresu ich przechowywania"

52. Zgromadzonych danych osobowych nie przechowuje się, jeżeli nie jest to niezbędne do celów ich przetwarzania oraz jeżeli nie istnieje inny zgodny cel i podstawa prawna zgodnie z art. 6 ust. 4. Każde zatrzymywanie danych powinno być w razie potrzeby obiektywnie uzasadnione przez administratora danych zgodnie z zasadą rozliczalności.

53. Administrator danych powinien ograniczyć okres zatrzymywania do niezbędnego minimum dla osiągnięcia danego celu. Jeżeli dane osobowe nie są już niezbędne do celów przetwarzania, są one domyślnie usuwane lub anonimizowane. Długość okresu zatrzymywania danych będzie zatem uzależniona od celu przetwarzania, o którym mowa. Obowiązek ten bezpośrednio wynika z zasady ograniczenia przechowywania, o której mowa w art. 5 ust. 1 lit. e), i jest realizowany w ramach domyślnej ochrony danych, tj. administrator danych powinien posiadać stałe procedury usuwania lub anonimizacji danych stanowiące cześć przetwarzania.

54. Anonimizacja[18] danych osobowych jest alternatywą dla ich usuwania, pod warunkiem że uwzględniono wszystkie odpowiednie elementy kontekstowe, a prawdopodobieństwo wystąpienia ryzyka i jego powaga, w tym ryzyko związane z ponowną identyfikacją, są regularnie oceniane[19].

2.2.2.4 „ich dostępności"

55. Administrator powinien wprowadzić ograniczenia dotyczące dostępu do danych osobowych oraz rodzaju tego dostępu na podstawie oceny konieczności, a także sprawdzić, czy dane osobowe są rzeczywiście dostępne dla podmiotów, którym są one potrzebne w razie potrzeby, na przykład w sytuacjach nadzwyczajnych. Kontroli dostępu należy przestrzegać podczas całego przepływu danych w ramach przetwarzania.

---

[17] Zgodnie z art. 4 ust. 2 RODO obejmują one zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

[18] Grupa Robocza Art. 29: „Opinia 05/2014 w sprawie technik anonimizacji". WP 216, 10 kwietnia 2014 r. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[19] Zobacz art. 4 ust. 1 RODO, motyw 26 RODO, Grupa Robocza Art. 29 „Opinia 05/2014 w sprawie technik anonimizacji". Zobacz również podsekcję „Ograniczenie przechowywania" w sekcji 3 niniejszego dokumentu, odnoszącą się do konieczności zapewnienia przez administratora skuteczności wdrożonych technik anonimizacji.

56. W art. 25 ust. 2 stwierdzono ponadto, że dane osobowe nie mogą być udostępniane nieokreślonej liczbie osób fizycznych bez interwencji danej osoby. Administrator domyślnie ogranicza dostępność danych i zapewnia osobie, której dane dotyczą, możliwość podjęcia interwencji przed opublikowaniem lub udostępnieniem w inny sposób jej danych osobowych w odniesieniu do nieokreślonej liczby osób fizycznych.

57. Udostępnienie danych osobowych nieokreślonej liczbie osób może skutkować dalszym rozpowszechnianiem danych niż to pierwotnie zamierzono. Jest to szczególnie istotne w kontekście Internetu i wyszukiwarek internetowych. W związku z tym administratorzy powinni w ramach domyślnej ochrony danych umożliwić osobom, których dane dotyczą, podjęcie odpowiednich działań przed udostępnieniem ich danych osobowych w otwartym Internecie. Ma to szczególne znaczenie w przypadku dzieci i grup szczególnie wrażliwych.

58. W zależności od podstawy prawnej przetwarzania, możliwość podjęcia interwencji może zmieniać się stosownie do kontekstu przetwarzania. Przykładem może być prośba o zgodę na powszechne udostępnienie danych osobowych lub o wprowadzenie ustawień prywatności, aby osoby, których dane dotyczą, mogły same kontrolować publiczny dostęp do nich.

59. Nawet jeżeli dane osobowe są udostępniane za zgodą i wiedzą osoby, której dane dotyczą, nie oznacza to, że każdy inny administrator posiadający dostęp do tych danych osobowych może je swobodnie przetwarzać do własnych celów – musi dysponować odrębną podstawą prawną[20].

3 WDRAŻANIE ZASAD OCHRONY DANYCH DO PROCESU PRZETWARZANIA DANYCH OSOBOWYCH Z WYKORZYSTANIEM UWZGLĘDNIANIA OCHRONY DANYCH W FAZIE PROJEKTOWANIA ORAZ DOMYŚLNEJ OCHRONY DANYCH

60. Na każdym etapie projektowania czynności przetwarzania, w tym zakupów, przetargów, outsourcingu, rozwoju, wsparcia, utrzymania, testowania, przechowywania, usuwania itp., administrator powinien wziąć pod uwagę i przeanalizować różne elementy ochrony danych w fazie projektowania oraz domyślnej ochrony danych, które zostaną zilustrowane przykładami w tym rozdziale w kontekście wdrażania zasad[21] [22] [23].

61. Administratorzy muszą wdrożyć zasady umożliwiające realizację ochrony danych w fazie projektowania oraz domyślnej ochrony danych. Zasady te obejmują: przejrzystość, zgodność z prawem, rzetelność, ograniczenie celu, minimalizację danych, prawidłowość, ograniczenie przechowywania, integralność i poufność oraz rozliczalność. Zasady te są przedstawione w art. 5 i w motywie 39 RODO. Aby w pełni zrozumieć sposób wdrażania ochrony danych w fazie projektowania oraz domyślnej ochrony danych, ważne jest zrozumienie znaczenia każdej z tych zasad.

[20] Zobacz sprawa Satakunnan Markkinapörssi Oy i Satamedia Oy przeciwko Finlandii, nr 931/13.
[21] Więcej przykładów znajduje się w wytycznych norweskiego organu ochrony danych: „Tworzenie oprogramowania z uwzględnieniem ochrony danych w fazie projektowania oraz domyślnej ochrony danych". 28 listopada 2017 r. www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729
[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers
[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

62. Prezentując przykłady dotyczące sposobu nadania wymiaru operacyjnego ochrony danych w fazie projektowania oraz domyślnej ochrony danych, sporządziliśmy wykazy **kluczowych elementów ochrony danych w fazie projektowania oraz domyślnej ochrony danych** w odniesieniu do każdej z zasad. Chociaż przedstawione przykłady podkreślają przedmiotową szczególną zasadę ochrony danych, mogą również pokrywać się z innymi ściśle powiązanymi zasadami. EROD podkreśla, że przedstawione poniżej kluczowe elementy i przykłady nie są wyczerpujące ani wiążące, lecz mają stanowić jedynie wytyczne dla każdej z zasad. Administratorzy powinni ocenić, w jaki sposób należy zagwarantować zgodność z zasadami w kontekście rozpatrywanej, konkretnej operacji przetwarzania.

63. Niniejsza część dotyczy wprawdzie wdrażania zasad, jednak administrator danych powinien też wprowadzić *odpowiednie* i *skuteczne* sposoby ochrony praw osób, których dane dotyczą, również zgodnie z rozdziałem III RODO, o ile nie wynika to już z samych zasad.

64. Nadrzędna jest tu zasada rozliczalności, która nakłada na administratora odpowiedzialność za wybór niezbędnych środków technicznych i organizacyjnych.

3.1 Przejrzystość[24]

65. Administrator musi zachować jasność i otwartość wobec osoby, której dane dotyczą, w kwestii sposobu, w jaki będzie gromadził, wykorzystywał i udostępniał jej dane osobowe. Przejrzystość polega na umożliwieniu osobom, których dane dotyczą, zrozumienia i – w razie konieczności – skorzystania z ich praw określonych w art. 15–22. Zasada ta jest zawarta w art. 12, 13, 14 i 34. Środki i zabezpieczenia wdrożone w celu wspierania zasady przejrzystości powinny również wspierać wykonanie przepisów tych artykułów.

66. Kluczowe elementy uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych w stosunku do zasady przejrzystości mogą obejmować:

- jasność – informacje są podawane jasnym i prostym językiem, są zwięzłe i zrozumiałe;
- semantykę – komunikacja ma jasne znaczenie dla danej grupy odbiorców;
- dostępność – informacje są łatwo dostępne dla osoby, której dane dotyczą;
- kontekst – informacje są przekazywane w odpowiednim czasie i w odpowiedniej formie;
- stosowność – informacje są stosowne i mają zastosowanie do konkretnej osoby, której dane dotyczą;
- uniwersalny projekt – informacje są dostępne dla wszystkich osób, których dotyczą dane, łącznie z wykorzystaniem języków odczytu maszynowego w celu ułatwienia i zautomatyzowania czytelności i przejrzystości;
- zrozumiałość – osoby, których dane dotyczą, muszą dokładnie rozumieć, czego mogą oczekiwać w odniesieniu do przetwarzania ich danych osobowych, szczególnie w przypadku, gdy osobami, których dane dotyczą, są dzieci lub członkowie innych grup szczególnie wrażliwych;
- wielokanałowość – informacje powinny być przekazywane za pośrednictwem różnych kanałów i mediów, nie tylko w formie tekstowej, w celu zwiększenia prawdopodobieństwa skutecznego dotarcia informacji do osoby, której dane dotyczą.
- warstwowość – informacje powinny być ułożone warstwowo w sposób, który rozwiązuje problem napięcia między kompletnością a zrozumieniem, przy jednoczesnym uwzględnieniu uzasadnionych oczekiwań osób, których dane dotyczą.

[24] Opracowanie dotyczące sposobu zrozumienia koncepcji przejrzystości znajduje się w wytycznych Grupy Roboczej Art. 29: „Wytyczne dotyczące przejrzystości na mocy rozporządzenia 2016/679". WP 260 rev.01, 11 kwietnia 2018 r. https://uodo.gov.pl/pl/file/1430 – zatwierdzone przez EROD.

Przykład[25]

Administrator danych projektuje politykę prywatności na swojej stronie internetowej w celu spełnienia wymogów przejrzystości. Polityka prywatności nie powinna zawierać obszernej masy informacji, które są trudne do przeniknięcia i zrozumienia dla przeciętnej osoby, której dane dotyczą. Powinna ona być sformułowana w jasnym i zwięzłym języku oraz umożliwiać użytkownikowi strony internetowej zrozumienie, w jaki sposób przetwarzane są jego dane osobowe. W związku z tym administrator dostarcza informacji w sposób wielowarstwowy, podkreślając najważniejsze punkty. Szczegółowe informacje są łatwo dostępne. Rozwijane menu i linki do innych stron służą dalszemu wyjaśnieniu różnych pozycji i pojęć zawartych w polityce. Administrator zapewnia również, aby informacje były przekazywane w sposób wielokanałowy, dostarczając filmy wideo w celu wyjaśnienia najważniejszych punktów informacji. Synergia pomiędzy poszczególnymi stronami jest niezbędna, aby zapewnić, że podejście warstwowe nie zwiększa dezorientacji, a raczej ją ogranicza.

Dostęp do polityki prywatności nie powinien być utrudniony dla osób, których dane dotyczą. Polityka prywatności jest zatem dostępna i widoczna na wszystkich wewnętrznych stronach WWW danej strony, tak aby osobę, której dane dotyczą, od uzyskania informacji dzieliło tylko jedno kliknięcie. Dostarczane informacje są również projektowane zgodnie z najlepszymi praktykami i standardami uniwersalnego projektowania, tak aby były dostępne dla wszystkich.

Ponadto niezbędne informacje muszą być również dostarczane we właściwym kontekście i w odpowiednim czasie. Ze względu na fakt, że administrator danych przeprowadza wiele operacji przetwarzania danych z wykorzystaniem danych zgromadzonych na stronie internetowej, ogólna polityka prywatności zawarta na stronie internetowej nie wystarczy, aby spełnić wymogi przejrzystości. Administrator projektuje zatem przepływ informacji, przedstawiając osobie, której dane dotyczą, istotne informacje w odpowiednim kontekście, wykorzystując np. fragmenty informacji lub wyskakujące okienka. Na przykład, prosząc osobę, której dane dotyczą, o wprowadzenie danych osobowych, administrator informuje tę osobę o sposobie, w jaki będą przetwarzane jej dane osobowe, oraz dlaczego przetwarzanie tych danych osobowych jest niezbędne.

3.2 Zgodność z prawem

67. Administrator określa ważną podstawę prawną przetwarzania danych osobowych. Środki i zabezpieczenia powinny wspierać wymóg dotyczący zagwarantowania, że cały proces przetwarzania danych jest zgodny z odpowiednimi podstawami prawnymi przetwarzania.

68. Kluczowe elementy uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych w stosunku do zgodności z prawem mogą obejmować:
    - stosowność – właściwe podstawy prawne mają zastosowanie do przetwarzania;
    - zróżnicowanie[26] – podstawa prawna stosowana w odniesieniu do każdej czynności przetwarzania jest zróżnicowana;

[25] Francuski organ ochrony danych opublikował szereg przykładów przedstawiających najlepsze praktyki w zakresie informowania użytkowników oraz innych zasad przejrzystości: https://design.cnil.fr/en/.
[26] EROD. „Wytyczne 2/2019 w sprawie przetwarzania danych osobowych zgodnie z art. 6 ust. 1 lit. b) RODO w kontekście świadczenia usług online osobom, których dane dotyczą". Wersja 2.0, 8 października 2019 r. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

- konkretny cel – właściwa podstawa prawna musi być wyraźnie powiązana z konkretnym celem przetwarzania[27];
- konieczność (niezbędność) – przetwarzanie musi być niezbędne i bezwarunkowe, aby jego cel był zgodny z prawem;
- autonomię – osobie, której dane dotyczą, należy przyznać najwyższy możliwy stopień autonomii w odniesieniu do kontroli nad danymi osobowymi w ramach podstawy prawnej;
- uzyskanie zgody – zgoda musi być dobrowolna, konkretna, świadoma i jednoznaczna[28]. Szczególną uwagę należy zwrócić na zdolność dzieci i młodzieży do wyrażenia świadomej zgody;
- wycofanie zgody – w przypadku gdy podstawą prawną jest zgoda, przetwarzanie danych powinno ułatwiać wycofanie zgody. Wycofanie musi być równie proste, jak udzielenie zgody. W przeciwnym razie mechanizm zgody administratora nie spełnia wymogów RODO[29].
- równoważenie interesów – w przypadku gdy podstawą prawną są prawnie uzasadnione interesy, administrator musi przeprowadzić wyważone równoważenie interesów, zwracając szczególną uwagę na brak równowagi sił, zwłaszcza w przypadku dzieci poniżej 18. roku życia i innych grup szczególnie wrażliwych. Muszą istnieć środki i zabezpieczenia mające na celu złagodzenie negatywnego wpływu na osoby, których dane dotyczą.
- ustalenie z góry – podstawa prawna jest ustalana przed rozpoczęciem przetwarzania danych;
- ustanie – jeżeli podstawa prawna przestaje mieć zastosowanie, należy odpowiednio przerwać przetwarzanie;
- dostosowanie – jeżeli nastąpiła ważna zmiana podstawy prawnej przetwarzania, faktyczne przetwarzanie należy dostosować zgodnie z nową podstawą prawną[30].
- podział odpowiedzialności – ilekroć przewiduje się współadministrowanie, strony muszą w wyraźny i przejrzysty sposób rozdzielić swoje właściwe obowiązki w stosunku do osoby, której dane dotyczą, oraz zaprojektować środki przetwarzania danych zgodnie z tym podziałem.

Przykład

Bank planuje zaoferować usługę w celu zwiększenia skuteczności zarządzania wnioskami kredytowymi. Założeniem usługi jest to, że bank, zwracając się do klienta o zgodę, jest w stanie pobrać dane o kliencie bezpośrednio od publicznych organów podatkowych. Niniejszy przykład nie uwzględnia przetwarzania danych osobowych z innych źródeł.

Pozyskanie danych osobowych dotyczących sytuacji finansowej osoby, której dane dotyczą, jest niezbędne do podjęcia działań na jej wniosek przed zawarciem umowy kredytowej[31]. Zbieranie danych osobowych bezpośrednio od organów podatkowych nie jest jednak uważane za konieczne, ponieważ klient może zawrzeć umowę, udostępniając informacje od organów podatkowych we własnym zakresie. Mimo że bank może mieć uzasadniony interes w uzyskaniu dokumentacji bezpośrednio od organów podatkowych, na przykład w celu zapewnienia skuteczności przetwarzania kredytu, udzielenie bankom takiego bezpośredniego dostępu do danych osobowych wnioskodawców stanowi ryzyko związane z wykorzystaniem lub potencjalnym nadużyciem praw dostępu.

[27] Zobacz sekcja dotycząca ograniczenia celu poniżej.
[28] Zob. wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pl
[29] Zob. wytyczne 05/2020 dotyczące na mocy rozporządzenia 2016/679, s. 24. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pl
[30] W przypadku gdy pierwotną podstawą prawną jest zgoda, zob. wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pl
[31] Zobacz art. 6 ust. 1 lit. b) RODO.

Realizując zasadę zgodności z prawem, administrator ma świadomość, że nie może wykorzystywać sformułowania „niezbędne do zawarcia umowy” w odniesieniu do tej części przetwarzania, która polega na gromadzeniu danych osobowych bezpośrednio od organów podatkowych. Fakt, że ten konkretny proces przetwarzania niesie ze sobą ryzyko mniejszego zaangażowania osoby, której dane dotyczą, w przetwarzanie jej danych, jest również istotnym czynnikiem w ocenie zgodności z prawem samego przetwarzania. Bank uznaje, że ta część przetwarzania musi opierać się na innej podstawie prawnej przetwarzania. W danym państwie członkowskim, w którym znajduje się siedziba administratora danych, istnieją przepisy krajowe umożliwiające bankowi bezpośrednie gromadzenie informacji od publicznych organów podatkowych, jeżeli osoba, której dane dotyczą, wyrazi na to wcześniej zgodę.

Bank przedstawia zatem informacje dotyczące przetwarzania danych na internetowej platformie do składania wniosków w sposób ułatwiający osobom, których dane dotyczą, zrozumienie, jaki zakres przetwarzania jest obowiązkowy, a jaki opcjonalny. Opcje przetwarzania domyślnie nie pozwalają na pozyskiwanie danych bezpośrednio ze źródeł innych niż sama osoba, której dane dotyczą, a możliwość bezpośredniego pozyskiwania informacji jest przedstawiona w sposób, który nie zniechęca osoby, której dane dotyczą, do wstrzymania się od tej czynności. Każda zgoda na zbieranie danych bezpośrednio od innych administratorów jest tymczasowym prawem dostępu do określonego zbioru informacji.

Każda udzielona zgoda jest przetwarzana elektronicznie w sposób umożliwiający dokumentację, a osobom, których dane dotyczą, przestawia się łatwy sposób kontrolowania tego, na co wyraziły zgodę, oraz wycofania tej zgody.

Administrator wcześniej ocenił te wymogi w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrony danych i uwzględnił wszystkie te kryteria w swojej specyfikacji wymagań do celów przetargu na zakup platformy. Administrator jest świadomy faktu, że jeżeli nie uwzględni wymogów w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrony danych w przetargu, później może być już zbyt późno na wdrożenie ochrony danych lub proces ten może być bardzo kosztowny.

3.3 Rzetelność

69. Rzetelność jest nadrzędną zasadą, która wymaga, aby dane osobowe nie były przetwarzane w sposób, który jest bezzasadnie szkodliwy, dyskryminujący, nieoczekiwany lub wprowadzający w błąd względem osoby, której dane dotyczą. Środki i zabezpieczenia, dzięki którym realizowana jest zasada rzetelności, wspierają również prawa i wolności osób, których dane dotyczą, szczególnie prawo do informacji (przejrzystości), prawo do interwencji (dostępu, usuwania, przenoszenia, sprostowania danych) oraz prawo do ograniczenia przetwarzania (prawo do niepodlegania zautomatyzowanemu podejmowaniu decyzji w indywidualnych przypadkach oraz niedyskryminacja osób, których dane dotyczą, w takich procesach).

70. Kluczowe elementy uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych w stosunku do rzetelności mogą obejmować:
    - autonomię – osobom, których dane dotyczą, należy przyznać najwyższy zakres autonomii, aby mogły decydować o sposobie wykorzystania ich danych osobowych, a także o zakresie i warunkach tego wykorzystania lub przetwarzania;
    - interakcję – osoby, których dane dotyczą, muszą mieć możliwość informowania o swoich prawach i korzystania z nich w odniesieniu do danych osobowych przetwarzanych przez administratora danych;

- oczekiwania – przetwarzanie powinno odpowiadać uzasadnionym oczekiwaniom osób, których dane dotyczą;
- niedyskryminację – administrator nie może niesprawiedliwie dyskryminować osoby, której dane dotyczą;
- niewykorzystywanie – administrator nie może wykorzystywać potrzeb ani słabości osób, których dane dotyczą;
- wybór konsumenta – administrator nie powinien uzależniać swoich użytkowników od jednego dostawcy w nieuczciwy sposób. W przypadku gdy usługa przetwarzania danych osobowych jest zastrzeżona, może to doprowadzić do „zablokowania" użytkownika w korzystaniu z usługi, które nie jest uczciwe, jeśli utrudnia osobom, których dane dotyczą, korzystanie z prawa do przenoszenia danych zgodnie z art. 20;
- równowagę sił – równowaga sił powinna być kluczowym celem relacji między administratorem a osobą, której dane dotyczą. Należy unikać nierównowagi sił. Jeśli nie jest to jednak możliwe, należy ją stwierdzić i wyjaśnić za pomocą odpowiednich środków zaradczych;
- brak przeniesienia ryzyka – administratorzy nie powinni przenosić ryzyka związanego z przedsiębiorstwem na osoby, których dane dotyczą;
- brak oszustw – informacje na temat przetwarzania danych i ich opcje należy przekazywać w sposób obiektywny i neutralny, unikając wszelkich mylących lub manipulujących sformułowań lub konstrukcji;
- poszanowanie praw – administrator musi przestrzegać podstawowych praw osób, których dane dotyczą oraz wdrażać odpowiednie środki i zabezpieczenia, a także nie może naruszać tych praw, chyba że jest to wyraźnie uzasadnione przez prawo;
- etykę – administrator powinien dostrzegać szerszy wpływ przetwarzania na prawa i godność osób fizycznych;
- prawdę – administrator jest zobowiązany do udostępnienia informacji na temat sposobu, w jaki przetwarza dane osobowe, oraz powinien działać tak, jak zadeklarował i nie wprowadzać w błąd osób, których dane dotyczą;
- interwencję człowieka – administrator musi uwzględnić *wykwalifikowaną* interwencję człowieka, dzięki której możliwe będzie wykrywanie błędów stronniczości, jakie maszyny mogą popełniać, zgodnie z prawem do niepodlegania zautomatyzowanemu podejmowaniu decyzji w indywidualnych przypadkach określonym w art. 22[32];
- uczciwe algorytmy – systematyczna ocena funkcjonowania algorytmów zgodnie z celami i dostosowanie algorytmów, aby ograniczyć wykryte uprzedzenia i zapewnić rzetelność w procesie przetwarzania. Osobom, których dane dotyczą, powinno się przekazywać informacje na temat funkcjonowania przetwarzania danych osobowych w oparciu o algorytmy analizujące lub prognozujące aspekty dotyczące tych osób, takie jak ich efekty pracy, sytuacja ekonomiczna, zdrowie, osobiste preferencje, wiarygodność lub zachowanie, lokalizacja lub przemieszczanie się[33].

Przykład 1

[32] Zob. wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679.
https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826
[33] Zobacz motyw 71 RODO.

Administrator obsługuje wyszukiwarkę internetową, która przetwarza głównie dane osobowe tworzone przez użytkowników. Administrator czerpie korzyści z posiadania dużej ilości danych osobowych oraz z możliwości wykorzystania ich do celów stosowania ukierunkowanych reklam. Administrator chce zatem wpłynąć na osoby, których dane dotyczą, aby zezwoliły na zbieranie i wykorzystywanie ich danych osobowych na szeroką skalę. Zgodę należy uzyskać poprzez przedstawienie opcji przetwarzania osobie, której dane dotyczą.

Realizując zasadę rzetelności, z uwzględnieniem charakteru, zakresu, kontekstu i celu przetwarzania, administrator ma świadomość, że nie może przedstawiać opcji w sposób nakłaniający osobę, której dane dotyczą, do zezwolenia administratorowi na zbieranie większej ilości danych osobowych niż w przypadku, gdyby opcje te przedstawiono w sposób jednakowy i neutralny. Oznacza to, że administratorzy nie mogą przedstawiać opcji przetwarzania w sposób utrudniający osobom, których dane dotyczą, wstrzymanie się od udostępniania swoich danych lub dostosowanie ich ustawień prywatności i ograniczenie przetwarzania. Są to przykłady złych wzorców, które są sprzeczne z duchem art. 25. Domyślne opcje przetwarzania nie powinny być inwazyjne, a możliwość wyboru dalszego przetwarzania powinna być przedstawiona w sposób, który nie wywiera presji na osobie, której dane dotyczą, aby wyraziła zgodę. Z tego względu administrator przedstawia opcje wyrażenia zgody lub wstrzymania się od jej udzielenia jako dwie równie widoczne możliwości wyboru, odpowiednio przedstawiające następstwa wyboru każdej z nich dla osoby, której dane dotyczą.

Przykład 2

Inny administrator przetwarza dane osobowe w celu świadczenia usługi przesyłania strumieniowego, w ramach której użytkownicy mogą wybrać między zwykłą subskrypcją o standardowej jakości a subskrypcją premium o wyższej jakości. W ramach subskrypcji premium subskrybenci otrzymują priorytetową obsługę klienta.

W odniesieniu do zasady rzetelności, priorytetowa obsługa klienta przyznana abonentom premium nie może dyskryminować stałych abonentów w zakresie dostępu do korzystania z ich praw zgodnie z art. 12 RODO. Oznacza to, że chociaż subskrybenci opcji premium otrzymują priorytetową obsługę, takie priorytetowe traktowanie nie może skutkować brakiem odpowiednich środków umożliwiających udzielenie odpowiedzi na wnioski od zwykłych subskrybentów bez zbędnej zwłoki, a w każdym razie w ciągu jednego miesiąca od otrzymania wniosków.

Klienci traktowani priorytetowo mogą płacić za lepszą obsługę, ale wszystkie osoby, których dane dotyczą, mają równy i niezróżnicowany dostęp do korzystania ze swoich praw i wolności zgodnie z wymogami art. 12.

3.4 Ograniczenie celu[34]

71. Administrator jest zobowiązany do zbierania danych w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz do nieprzetwarzania ich dalej w sposób niezgodny z celami, w jakich zostały

[34] Grupa Robocza Art. 29 przedstawiła wytyczne dotyczące zrozumienia zasady ograniczenia celu na mocy dyrektywy 95/46/WE. Chociaż EROD nie przyjęła przedmiotowej opinii, może ona być nadal istotna, ponieważ brzmienie zasady w ramach RODO jest takie samo. Grupa Robocza Art. 29. „Opinia 03/2013 w sprawie ograniczenia celu". WP 203, 2 kwietnia 2013 r. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

zebrane[35]. Projektowanie przetwarzania powinno być zatem kształtowane przez to, co niezbędne do osiągnięcia tych celów. Jeżeli dalsze przetwarzanie danych ma mieć miejsce, administrator musi najpierw upewnić się, że cele tego przetwarzania są zgodne z celami pierwotnymi, oraz odpowiednio zaprojektować takie przetwarzanie. Niezależnie od tego, czy nowy cel jest zgodny z celem pierwotnym, należy poddać go ocenie według kryteriów określonych w art. 6 ust. 4.

72. Kluczowe elementy uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych w stosunku do ograniczenia celu mogą obejmować:
    - ustalenie z góry – prawnie uzasadnione cele należy określić przed zaprojektowaniem przetwarzania;
    - specyfikę – podane są konkretne i wyraźne cele, w których przetwarzane są dane osobowe.
    - ukierunkowanie na cel – cel przetwarzania powinien kierować projektowaniem przetwarzania i stanowić podstawę granic przetwarzania;
    - niezbędność – na podstawie celu określa się, jakie dane osobowe są niezbędne do przetwarzania;
    - zgodność – każdy nowy cel musi być zgodny z celem pierwotnym, dla którego zebrano dane, i musi prowadzić do istotnych zmian w projekcie;
    - ograniczenie dalszego przetwarzania – administrator nie powinien łączyć zbiorów danych ani dokonywać dalszego przetwarzania w nowych, niezgodnych celach;
    - ograniczenie ponownego wykorzystania – administrator powinien stosować środki techniczne, w tym haszowanie (ang. hashing) i szyfrowanie, w celu ograniczenia możliwości ponownego wykorzystania danych osobowych w innym celu. Administrator powinien również dysponować środkami organizacyjnymi, takimi jak strategie i zobowiązania umowne, które ograniczają możliwość ponownego, nieuprawnionego wykorzystania danych osobowych;
    - przegląd – administrator ma obowiązek regularnie sprawdzać, czy przetwarzanie jest niezbędne do celów, dla których zebrano dane, a także testować projekt pod względem ograniczenia celu;

Przykład

Administrator przetwarza dane osobowe swoich klientów. Celem przetwarzania danych jest realizacja zamówienia, tj. dostarczenie towarów pod właściwy adres i otrzymanie zapłaty. Przechowywane dane osobowe obejmują historię zamówień, imię i nazwisko, adres, adres e-mail i numer telefonu.

Administrator rozważa zakup produktu przeznaczonego do zarządzania relacjami z klientami (CRM), który gromadzi wszystkie dane dotyczące klienta, takie jak sprzedaż, marketing i obsługa klienta, w jednym miejscu. Produkt umożliwia przechowywanie informacji na temat wszystkich połączeń telefonicznych, działań, dokumentów, wiadomości e-mail i kampanii marketingowych w celu uzyskania pełnego obrazu klienta. Dodatkowo, CRM może automatycznie analizować siłę nabywczą klientów poprzez wykorzystanie informacji publicznych. Celem analizy jest lepsze ukierunkowanie działań reklamowych. Działania te nie wchodzą w zakres pierwotnego, zgodnego z prawem celu przetwarzania danych.

Aby zachować zgodność z zasadą ograniczenia celu, administrator danych wymaga od dostawcy produktu, aby przedstawił mapę różnych działań związanych z przetwarzaniem, które wykorzystują dane osobowe do celów istotnych dla administratora.

[35] Artykuł 5 ust. 1 lit. b) RODO.

Po otrzymaniu wyników takiego mapowania administrator ocenia, czy nowy cel marketingowy i cel reklamy ukierunkowanej są zgodne z pierwotnymi celami określonymi w momencie zbierania danych oraz czy istnieje wystarczająca podstawa prawna do ich przetwarzania. Jeżeli ocena ta nie daje pozytywnej odpowiedzi, administrator nie wykorzystuje dalej odnośnych właściwości. Ewentualnie administrator może zrezygnować z oceny i nie korzystać z opisanych właściwości produktu.

3.5 Minimalizacja danych

73. Jedynie dane osobowe, które są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do osiągnięcia celu, są przetwarzane[36]. W rezultacie administrator musi z góry określić, które cechy i parametry systemów przetwarzania oraz ich funkcje pomocnicze są dopuszczalne. Minimalizacja danych uzasadnia i urzeczywistnia zasadę konieczności (niezbędności). W ramach dalszego przetwarzania administrator powinien okresowo rozważać, czy przetwarzane dane osobowe nadal są adekwatne, stosowne i ograniczone do tego, co niezbędne, oraz czy dane należy usunąć lub zanonimizować.

74. Przede wszystkim administratorzy muszą ustalić, czy w ogóle muszą przetwarzać dane osobowe do swoich odpowiednich celów. Administrator powinien sprawdzić, czy odpowiednie cele można osiągnąć, przetwarzając mniej danych osobowych lub posiadając mniej szczegółowe lub zagregowane dane osobowe, lub w ogóle bez konieczności przetwarzania danych osobowych[37]. Weryfikacja taka powinna mieć miejsce przed jakimkolwiek przetwarzaniem, ale może być również przeprowadzona w dowolnym momencie tego procesu. Jest to również zgodne z art. 11.

75. Minimalizacja może również odnosić się do stopnia identyfikacji. Jeżeli cel przetwarzania nie wymaga, aby ostateczny zbiór danych odnosił się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (jak w przypadku statystyk), ale wymaga tego pierwotne przetwarzanie (np. przed agregacją danych), administrator usuwa lub anonimizuje dane osobowe, gdy tylko identyfikacja nie jest już konieczna. Ewentualnie, jeżeli dalsza identyfikacja jest konieczna w odniesieniu do innych czynności przetwarzania, dane osobowe należy spseudonimizować, aby zminimalizować ryzyko naruszenia praw osób, których dane dotyczą.

76. Kluczowe elementy uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych w stosunku do minimalizacji danych mogą obejmować:
    - unikanie przetwarzania danych – całkowite unikanie przetwarzania danych osobowych, jeżeli jest to możliwe w określonym celu;
    - ograniczenie – ograniczenie ilości zbieranych danych osobowych do ilości niezbędnej do osiągnięcia danego celu;
    - ograniczenie dostępu – kształtowanie przetwarzania danych w taki sposób, aby minimalna liczba osób wymagała dostępu do danych osobowych w celu wykonywania swoich obowiązków, a także odpowiednie ograniczenie dostępu;
    - stosowność – dane osobowe mają znaczenie dla danego przetwarzania, a administrator musi być w stanie tę stosowność wykazać;

[36] Artykuł 5 ust. 1 lit. c) RODO.
[37] Motyw 39 RODO stanowi: „Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami".

- niezbędność – każda kategoria danych osobowych jest niezbędna do osiągnięcia określonych celów i powinna być przetwarzana tylko wtedy, gdy osiągnięcie tego celu w inny sposób nie jest możliwe;
- agregację – używanie zagregowanych danych, o ile to możliwe;
- pseudonimizację – gdy tylko posiadanie danych osobowych umożliwiających bezpośrednią identyfikację nie jest już konieczne, dane należy spseudonimizować, a klucze do identyfikacji przechowywać oddzielnie;
- anonimizację i usuwanie – w przypadku gdy dane osobowe nie są lub przestały być niezbędne do osiągnięcia celu, dane osobowe są anonimizowane lub usuwane;
- przepływ danych – przepływ danych musi być na tyle skuteczny, aby nie tworzyć większej liczby kopii niż jest to konieczne;
- „stan wiedzy technicznej"– administrator danych powinien stosować aktualne i odpowiednie technologie, aby ograniczyć i zminimalizować ilość danych.

Przykład 1

Księgarnia chce zwiększyć swoje dochody, sprzedając książki przez Internet. Właściciel księgarni chce opracować standardowy formularz dotyczący procesu zamawiania. Aby zapewnić sobie, że klient udzieli wszystkich potrzebnych informacji, właściciel księgarni wprowadza w formularzu wymóg wypełnienia wszystkich pól (jeśli klient nie wypełni wszystkich pól, nie będzie mógł złożyć zamówienia). Właściciel księgarni początkowo korzysta ze standardowego formularza kontaktowego, w którym klient proszony jest o podanie daty urodzenia, numeru telefonu i adresu zamieszkania. Nie wszystkie pola w formularzu są jednak bezwzględnie niezbędne do osiągnięcia celu, jakim jest zakup i dostawa książek. W tym konkretnym przypadku, jeżeli osoba, której dane dotyczą, płaci za produkt z góry, jej data urodzenia i numer telefonu nie są konieczne do zrealizowania zakupu produktu. Oznacza to, że pola te nie mogą być obowiązkowo wypełniane w formularzu internetowym na potrzeby zamówienia produktu, chyba że administrator danych potrafi wyraźnie uzasadnić, dlaczego dane te są niezbędne. Ponadto istnieją sytuacje, w których adres nie będzie niezbędny. Na przykład, zamawiając e-book, klient może pobrać produkt bezpośrednio na swoje urządzenie.

Właściciel sklepu internetowego podejmuje zatem decyzję o stworzeniu dwóch formularzy internetowych: formularza służącego do zamawiania książek, z polem dotyczącym adresu klienta, i formularza służącego do zamawiania książek elektronicznych, bez pola dotyczącego adresu klienta.

Przykład 2

Przedsiębiorstwo transportu publicznego pragnie zebrać informacje statystyczne w oparciu o trasy podróżnych. Jest to przydatne do celów dokonywania właściwych wyborów dotyczących zmian harmonogramów transportu publicznego i właściwych tras pociągów. Pasażerowie muszą przeciągnąć bilet przez czytnik za każdym razem, gdy wchodzą do środka transportu lub go opuszczają. Po przeprowadzeniu oceny ryzyka związanego z prawami i swobodami pasażerów w zakresie gromadzenia danych o trasach podróży, administrator danych stwierdza, że może ustalić tożsamość pasażerów w sytuacji, gdy mieszkają lub pracują na obszarach słabo zaludnionych, na podstawie pojedynczej trasy, za pomocą kodu identyfikacyjnego biletu. W związku z tym, ponieważ nie jest to niezbędne dla osiągnięcia celu optymalizacji harmonogramów transportu publicznego i tras pociągów, administrator

nie przechowuje identyfikatora biletu. Po zakończeniu podróży administrator przechowuje jedynie informacje dotyczące poszczególnych tras podróży, aby nie móc zidentyfikować podróży powiązanych z danym biletem, a jedynie zatrzymać informacje dotyczące odrębnych tras podróży.

W przypadkach, kiedy nadal może istnieć ryzyko ustalenia tożsamości osoby jedynie na podstawie trasy jej przejazdu transportem publicznym, administrator wprowadza środki statystyczne w celu zmniejszenia ryzyka, takie jak skrócenie początku i końca trasy.

Przykład 3

Celem kuriera jest przeprowadzenie oceny skuteczności dostaw pod kątem czasu dostawy, harmonogramu nakładu pracy i zużycia paliwa. Aby osiągnąć ten cel, kurier musi przetworzyć szereg danych osobowych dotyczących zarówno pracowników (kierowców), jak i klientów (adresy, przedmioty do dostarczenia itp.). Ta operacja przetwarzania pociąga za sobą ryzyko związane zarówno z monitorowaniem pracowników, które wymaga szczególnych zabezpieczeń prawnych, jak i ze śledzeniem nawyków klientów przy użyciu informacji na temat dostarczonych przedmiotów. Ryzyko to można znacznie ograniczyć za pomocą odpowiedniej pseudonimizacji pracowników i klientów. W szczególności, jeżeli klucze pseudonimizacji są często zmieniane, a zamiast szczegółowych adresów uwzględniane są obszary makro, dąży się do skutecznej minimalizacji danych, a administrator może skoncentrować się wyłącznie na procesie dostawy oraz na osiągnięciu celu optymalizacji zasobów, bez przekraczania progu monitorowania zachowań poszczególnych osób (klientów lub pracowników).

Przykład 4

Szpital gromadzi dane o swoich pacjentach w systemie informacji szpitalnej (elektroniczna karta zdrowia). Personel szpitala korzysta z dokumentacji medycznej pacjentów w celu podejmowania decyzji dotyczących opieki nad nimi i ich leczenia, a także aby udokumentować wszystkie podejmowane działania diagnostyczne, opiekuńcze i lecznicze. Domyślnie dostęp uzyskują jedynie ci członkowie personelu medycznego, którzy są przypisani do danego pacjenta na oddziale specjalistycznym, na którym przebywa pacjent. Grupa osób mających dostęp do dokumentacji pacjenta powiększa się, jeżeli w procesie leczenia uczestniczą inne oddziały lub jednostki diagnostyczne. Po wypisaniu pacjenta ze szpitala i dokonaniu rozliczeń, dostęp do jego dokumentacji zostaje ograniczony do niewielkiej grupy pracowników danego oddziału specjalistycznego, którzy – za zgodą pacjenta – udzielają informacji medycznych lub konsultacji, o które proszą inni dostawcy usług medycznych.

3.6 Prawidłowość

77. Dane osobowe muszą być prawidłowe i uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane[38].

78. Wymogi należy oceniać w kontekście ryzyka i konsekwencji faktycznego wykorzystania danych. Nieprawidłowe dane osobowe mogą powodować ryzyko naruszenia praw i wolności osób, których

[38] Artykuł 5 ust. 1 lit. d) RODO.

dane dotyczą, na przykład gdy prowadzą do błędnej diagnozy lub niewłaściwego traktowania protokołu zdrowia, lub błędny obraz osoby może prowadzić do podejmowania decyzji na niewłaściwej podstawie przy przetwarzaniu ręcznym, przy użyciu zautomatyzowanego procesu decyzyjnego albo sztucznej inteligencji.

79. Kluczowe elementy uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych w stosunku do prawidłowości mogą obejmować:
    - źródło danych – źródła danych osobowych powinny być wiarygodne pod względem prawidłowości danych;
    - stopień prawidłowości – każdy element danych osobowych musi być na tyle prawidłowy, na ile jest to niezbędne do osiągnięcia określonych celów;
    - mierzalną prawidłowość – zmniejszenie liczby fałszywych wyników dodatnich/ujemnych, na przykład stronniczości w zautomatyzowanych decyzjach i sztucznej inteligencji;
    - weryfikację – w zależności od charakteru danych, w odniesieniu do tego, jak często może się on zmieniać, administrator powinien weryfikować poprawność danych osobowych z osobą, której dane dotyczą, przed rozpoczęciem przetwarzania i na różnych jego etapach (np. w zależności od kryterium wieku);
    - usuwanie/sprostowanie – administrator musi usunąć lub sprostować nieprawidłowe dane bez zbędnej zwłoki. Administrator musi w szczególności ułatwić tę operację, jeśli osoby, których dane dotyczą, są lub były dziećmi i w późniejszym okresie chcą usunąć takie dane osobowe[39].
    - unikanie powielania błędów – administratorzy powinni ograniczać skutki skumulowanych błędów w łańcuchu przetwarzania;
    - dostęp – osoby, których dane dotyczą, powinny otrzymywać informacje na temat danych osobowych i skuteczny dostęp do nich zgodnie z art. 12–15 RODO, aby mogły kontrolować ich poprawność i w razie potrzeby je sprostować;
    - ciągłą prawidłowość – dane osobowe powinny być prawidłowe na wszystkich etapach przetwarzania; testy dotyczące prawidłowości należy przeprowadzać na krytycznych etapach;
    - aktualizację – dane osobowe muszą być aktualizowane, jeżeli jest to niezbędne do osiągnięcia celu;
    - projektowanie danych – zastosowanie właściwości technologicznych i organizacyjnych projektu w celu zmniejszenia nieprawidłowości, na przykład przedstawienie zwięzłych, z góry określonych opcji wyboru zamiast wolnych pól tekstowych.

Przykład 1

Firma ubezpieczeniowa chciałaby wykorzystać sztuczną inteligencję (SI) do profilowania klientów wykupujących ubezpieczenie jako podstawę do podejmowania decyzji przy obliczaniu ryzyka ubezpieczeniowego. Określając sposób, w jaki należy opracować rozwiązania z zakresu SI, firma określa sposoby przetwarzania i powinna uwzględnić ochronę danych w fazie projektowania przy wyborze SI od sprzedawcy oraz przy podejmowaniu decyzji o sposobie szkolenia SI.

W przypadku określania sposobu szkolenia SI administrator musi dysponować prawidłowymi danymi, aby osiągnąć dokładne wyniki. W związku z tym administrator musi zapewnić, aby dane stosowane do celów szkolenia SI były prawidłowe.

Zakładając, że istnieje ważna podstawa prawna do szkolenia SI z wykorzystaniem danych osobowych pochodzących z dużego pod-zbioru obecnych klientów, administrator wybiera pulę klientów będących przedstawicielami danej populacji, aby uniknąć błędu.

[39] Por. motyw 65.

Dane klientów są następnie pobierane z odpowiedniego systemu obsługi danych, w tym dane dotyczące rodzaju ubezpieczenia, np. ubezpieczenie zdrowotne, ubezpieczenie domu, ubezpieczenie podróżne itp. oraz dane z rejestrów publicznych, do których mają zgodnie z prawem dostęp. Wszystkie dane są pseudonimizowane przed przekazaniem ich do systemu stworzonego na potrzeby szkolenia modelu SI.

W celu zapewnienia, aby dane wykorzystane do szkolenia SI były możliwie najbardziej prawidłowe, administrator zbiera jedynie dane pochodzące ze źródeł danych z poprawnymi i aktualnymi informacjami.

Firma ubezpieczeniowa sprawdza, czy SI jest wiarygodna i zapewnia niedyskryminujące wyniki zarówno podczas opracowywania produktu, jak i ostatecznie przed jego wprowadzeniem na rynek. W przypadku gdy SI jest w pełni przeszkolona i sprawnie działająca, zakład ubezpieczeń wykorzystuje wyniki, aby uzupełnić ocenę ryzyka ubezpieczeniowego, nie opierając się jednak wyłącznie na SI przy podejmowaniu decyzji o przyznaniu ubezpieczenia, chyba że decyzja została podjęta zgodnie z wyjątkami określonymi w art. 22 ust. 2 RODO.

Zakład ubezpieczeń będzie również systematycznie dokonywać przeglądu wyników SI, aby zachować wiarygodność i w razie konieczności dostosować algorytm.

Przykład 2

Administratorem danych jest instytucja zdrowia publicznego poszukująca metod służących zapewnieniu integralności i prawidłowości danych osobowych w rejestrach klientów.

W sytuacjach gdy dwie osoby przybywają do instytucji w tym samym czasie i otrzymują jednakowe leczenie, istnieje ryzyko pomylenia tych dwóch osób, jeżeli jedynym parametrem, który je różni, jest ich imię i nazwisko. W celu zapewnienia prawidłowości administrator potrzebuje niepowtarzalnego identyfikatora dla każdej osoby, a zatem większej ilości informacji niż tylko imienia i nazwiska klienta.

Instytucja korzysta z szeregu systemów zawierających dane osobowe klientów i musi zapewnić, aby dane związane z klientem były zawsze poprawne, prawidłowe i zgodne we wszystkich systemach. Instytucja wyodrębniła kilka zagrożeń, jakie mogą wystąpić w przypadku zmiany informacji w jednym systemie, przy jednoczesnym braku zmian w innych systemach.

Administrator podejmuje decyzję o zminimalizowaniu ryzyka przez wykorzystanie techniki haszowania zapewniającej integralność danych w dzienniku leczenia. Dla zapisów w dziennikach leczenia i związanych z nimi klientów tworzone są stałe kryptograficzne znaczniki czasu, tak aby w razie potrzeby można było rozpoznać, skorelować i prześledzić wszelkie zmiany.

3.7 Ograniczenie przechowywania

80. Administrator musi zapewnić, aby dane osobowe były przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane[40].

[40] Artykuł 5 ust. 1 lit. c) RODO.

Istotne jest, aby administrator dokładnie wiedział, jakie dane osobowe są przetwarzane przez przedsiębiorstwo i w jakim celu. Cel przetwarzania jest głównym kryterium decydującym o tym, jak długo dane osobowe są przechowywane.

81. Środki i zabezpieczenia przyczyniające się do realizacji zasady ograniczenia przechowywania uzupełniają prawa i wolności osób, których dane dotyczą, w szczególności prawo do usunięcia danych i prawo sprzeciwu.

82. Kluczowe elementy uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych w stosunku do ograniczenia przechowywania mogą obejmować:
    - usuwanie i anonimizację – administrator powinien posiadać jasne wewnętrzne procedury i możliwości usuwania lub anonimizacji;
    - skuteczność anonimizacji/usuwania – administrator musi zapewnić, aby ponowna identyfikacja zanonimizowanych danych lub odzyskanie usuniętych danych nie były możliwe, a także powinien weryfikować, czy jest to możliwe;
    - automatyzację – usuwanie określonych danych osobowych powinno odbywać się w zautomatyzowany sposób;
    - kryteria przechowywania – administrator ma obowiązek określić, jakie dane są niezbędne do osiągnięcia danego celu i jak długo należy je przechowywać;
    - uzasadnienie – administrator danych powinien umieć uzasadnić, dlaczego okres przechowywania jest niezbędny dla danego celu i danych osobowych oraz wykazać podstawy prawne takiego okresu przechowywania;
    - egzekwowanie zasad polityki w zakresie zatrzymywania danych – administrator ma obowiązek egzekwować realizację zasad wewnętrznej polityki zatrzymywania danych oraz weryfikować, czy organizacja stosuje zasady tej polityki;
    - kopie zapasowe/rejestry – administratorzy ustalają dane osobowe niezbędne do tworzenia kopii zapasowych i rejestrów oraz czas ich przechowywania;
    - przepływ danych – administratorzy powinni zwracać uwagę na przepływ danych osobowych i przechowywanie wszelkich ich kopii oraz dążyć do ograniczenia ich „tymczasowego" przechowywania.

Przykład

Administrator danych gromadzi dane osobowe, jeżeli celem przetwarzania jest zarządzanie członkostwem osoby, której dane dotyczą. Dane osobowe są usuwane po zakończeniu członkostwa i nie ma podstawy prawnej do ich dalszego przechowywania.

Administrator opracowuje wewnętrzną procedurę dotyczącą zatrzymywania i usuwania danych. Zgodnie z powyższym pracownicy muszą ręcznie usuwać dane osobowe po upływie okresu zatrzymywania danych. Pracownicy przestrzegają procedury, zgodnie z którą regularnie korygują i usuwają dane ze wszelkich urządzeń, kopii zapasowych, rejestrów, wiadomości e-mail i innych odpowiednich nośników danych.

Aby zapewnić skuteczniejsze usuwanie danych i zmniejszyć podatność na błędy, administrator wdraża automatyczny system w celu zautomatyzowanego, rzetelnego i bardziej systematycznego usuwania danych. System jest skonfigurowany tak, aby działał zgodnie z określoną procedurą usuwania danych, która jest powtarzana w określonych z góry, regularnych odstępach czasu i służy usuwaniu danych osobowych ze wszystkich nośników danych przedsiębiorstwa. Administrator regularnie dokonuje przeglądu i testowania procedury zatrzymywania danych oraz zapewnia jej zgodność z aktualną polityką zatrzymywania danych.

3.8 Integralność i poufność

83. Zasada integralności i poufności obejmuje ochronę danych przed nieuprawnionym lub niezgodnym z prawem przetwarzaniem oraz przed przypadkową utratą, zniszczeniem lub uszkodzeniem, przy zastosowaniu odpowiednich środków technicznych lub organizacyjnych. Bezpieczeństwo danych osobowych wymaga odpowiednich środków, których celem jest zapobieganie przypadkom naruszenia ochrony danych i zarządzanie nimi; zagwarantowanie właściwej realizacji zadań związanych z przetwarzaniem danych oraz zgodności z innymi zasadami; a także ułatwienie skutecznego korzystania z praw przysługujących osobom fizycznym.

84. W motywie 78 stwierdzono, że jeden ze środków w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrony danych może polegać na umożliwieniu administratorowi „tworzenia i doskonalenia zabezpieczeń". W motywie 78, oprócz stosowania innych środków w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrony danych, sugeruje się, aby administratorzy byli odpowiedzialni za ciągłą ocenę tego, czy za każdym razem stosowane są odpowiednie sposoby przetwarzania oraz czy wybrane środki faktycznie przeciwdziałają istniejącym słabym punktom. Ponadto administratorzy danych powinni przeprowadzać regularne przeglądy środków bezpieczeństwa informacji zapewniających ochronę danym osobowym, a także procedur postępowania w przypadku naruszenia ochrony danych.

85. Kluczowe elementy uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych w stosunku do integralności i poufności mogą obejmować:
    - system zarządzania bezpieczeństwem informacji (SZBI) – posiadanie środków operacyjnych w ramach polityki zarządzania oraz procedur w zakresie bezpieczeństwa informacji;
    - analizę ryzyka – ocena zagrożeń dla bezpieczeństwa danych osobowych polegająca na analizie wpływu na prawa osób fizycznych i przeciwdziałaniu zidentyfikowanym zagrożeniom. Możliwość wykorzystania w ocenie ryzyka; opracowanie i utrzymanie kompleksowego, systematycznego i realistycznego „modelowania zagrożeń" oraz analizy obszaru ataku zaprojektowanego oprogramowania w celu ograniczenia wektorów ataku i możliwości wykorzystania słabych punktów;
    - bezpieczeństwo w fazie projektowania – uwzględnienie wymogów bezpieczeństwa na jak najwcześniejszym etapie projektowania i rozwoju systemu oraz ciągła integracja i wykonywanie odpowiednich testów;
    - utrzymanie – regularny przegląd i testowanie oprogramowania, sprzętu, systemów i usług itp. w celu wykrycia słabych punktów systemów wspomagających przetwarzanie;
    - zarządzanie kontrolą dostępu – dostęp do danych osobowych niezbędnych do realizacji zadań związanych z przetwarzaniem danych mają tylko upoważnieni pracownicy, a administrator powinien dokonać zróżnicowania uprawnień dostępu dla upoważnionych pracowników;
        - ograniczenie dostępu (przedstawiciele) – kształtowanie przetwarzania danych powinno przebiegać w taki sposób, aby minimalna liczba osób wymagała dostępu do danych osobowych w celu wykonywania swoich obowiązków; a także odpowiednie ograniczenie dostępu;
        - ograniczenie dostępu (treść) – w przypadku każdej operacji przetwarzania dostęp powinien być ograniczony tylko do tych atrybutów dla danego zbioru danych, które są potrzebne do wykonania tej operacji. Ponadto ograniczenie dostępu do danych osób, których dane dotyczą, podlegających kompetencjom danego pracownika;
        - rozdzielenie dostępu – kształtowanie procesu przetwarzania danych powinno przebiegać w taki sposób, aby żadna osoba nie wymagała pełnego dostępu do

wszystkich danych zebranych na temat osoby, której dane dotyczą, a tym bardziej do wszystkich danych osobowych konkretnej kategorii osób, których dane dotyczą;

- bezpieczne przekazywanie danych – przekazywanie danych powinno być zabezpieczone przed nieuprawnionym i przypadkowym dostępem i wprowadzeniem zmian;
- bezpieczne przechowywanie – przechowywanie danych musi być zabezpieczone przed nieuprawnionym dostępem i wprowadzaniem zmian. Powinny istnieć procedury pozwalające ocenić ryzyko scentralizowanego lub zdecentralizowanego przechowywania oraz kategorie danych osobowych, do których ma to zastosowanie. Niektóre dane mogą wymagać dodatkowych środków bezpieczeństwa lub odizolowania od innych danych;
- pseudonimizację – dane osobowe i kopie zapasowe/rejestry należy spseudonimizować w ramach środków bezpieczeństwa w celu zminimalizowania ryzyka potencjalnych naruszeń ochrony danych, np. przez zastosowanie haszowania lub szyfrowania;
- kopie zapasowe/rejestry – tworzenie kopii zapasowych i prowadzenie rejestrów w zakresie niezbędnym do zapewnienia bezpieczeństwa informacji, wykorzystywanie ścieżek audytu i monitorowanie wydarzeń w ramach rutynowej kontroli bezpieczeństwa. Są one chronione przed nieuprawnionym i przypadkowym dostępem i zmianą oraz regularnie poddawane przeglądowi, a wszelkie zdarzenia powinny być rozpatrywane bezzwłocznie;
- odzyskiwanie danych w przypadku awarii/ciągłość biznesowa – wymagania dotyczące odzyskiwania danych z systemu informacji adresowej w przypadku awarii oraz dotyczące ciągłości biznesowej w celu przywrócenia dostępności danych osobowych po poważnych incydentach;
- ochrona w zależności od ryzyka – wszystkie kategorie danych osobowych powinny być chronione za pomocą środków dostosowanych do ryzyka naruszenia bezpieczeństwa. Dane obarczone szczególnym ryzykiem powinny, w miarę możliwości, być oddzielone od reszty danych osobowych;
- zarządzanie reagowaniem na incydenty naruszające bezpieczeństwo – należy wprowadzić procedury, zasady postępowania i zasoby służące wykrywaniu naruszeń ochrony danych, ograniczaniu naruszeń, postępowaniu z nimi, zgłaszaniu ich i wyciąganiu z nich wniosków;
- zarządzanie incydentami – administrator powinien dysponować procesami umożliwiającymi reagowanie na naruszenia i incydenty, aby system przetwarzania danych był bardziej niezawodny. Dotyczy to również procedur zgłaszania, takich jak zarządzanie zgłoszeniami (do organu nadzorczego) i informacjami (do osób, których dane dotyczą).

Przykład

Administrator chce pobrać duże ilości danych osobowych z medycznej bazy danych zawierającej elektroniczną dokumentację zdrowotną (pacjentów) na dedykowany serwer bazy danych w firmie, aby przetwarzać pobrane dane dla celów związanych z zapewnieniem jakości. Przedsiębiorstwo oceniło ryzyko przekierowania wyciągów na serwer, który jest dostępny dla wszystkich pracowników przedsiębiorstwa, jako prawdopodobnie wysokie dla praw i wolności osób, których dane dotyczą. Ze względu na to, że w firmie istnieje tylko jeden dział, który zajmuje się przetwarzaniem pozyskanych danych pacjentów, administrator danych decyduje się na ograniczenie dostępu do serwera dedykowanego wyłącznie do pracowników tego działu. W celu dalszego zmniejszenia ryzyka, dane przed ich przekazaniem zostaną poddane pseudonimizacji.

Aby uregulować dostęp i zminimalizować ewentualne szkody wynikające ze złośliwego oprogramowania, przedsiębiorstwo postanawia wydzielić sieć i ustanowić środki kontroli dostępu do serwera. Ponadto ustanawia system monitorowania bezpieczeństwa oraz system wykrywania włamań i zapobiegania im, a także wyłącza go z regularnego użytkowania. Wdrożony zostaje zautomatyzowany

system kontroli w celu monitorowania dostępu i zmian. W konsekwencji, gdy określone zdarzenia związane z użytkowaniem zostają zaplanowane, generowane są sprawozdania i automatyczne powiadomienia. Administrator zapewnia, aby użytkownicy mieli dostęp tylko na zasadach ścisłej potrzeby i z zachowaniem odpowiedniego poziomu dostępu. Niewłaściwe wykorzystanie można szybko i łatwo wykryć.

Konieczne jest porównanie niektórych wyciągów z nowymi wyciągami, a zatem niezbędne jest przechowywanie ich przez trzy miesiące. Administrator decyduje o umieszczeniu ich w oddzielnych bazach danych na tym samym serwerze, a do ich przechowywania stosuje szyfrowanie zarówno transparentne, jak i na poziomie kolumn. Klucze do odszyfrowania danych na poziomie kolumn są przechowywane w dedykowanych modułach bezpieczeństwa, które mogą być używane tylko przez upoważnionych pracowników, jednak nie mogą zostać wyodrębnione.

Postępowanie w przypadku zbliżających się incydentów sprawia, że system jest bardziej solidny i niezawodny. Administrator rozumie, że zapobiegawcze i skuteczne środki i zabezpieczenia powinny stanowić element wszystkich działań w zakresie przetwarzania danych osobowych teraz i w przyszłości oraz że takie działanie może pomóc w zapobieganiu takim naruszeniom ochrony danych w przyszłości.

Administrator ustanawia te środki bezpieczeństwa, aby zapewnić prawidłowość, integralność i poufność, a także aby zapobiec rozprzestrzenianiu się złośliwego oprogramowania w wyniku cyberataków w celu zapewnienia solidnego rozwiązania. Solidne środki bezpieczeństwa przyczyniają się do budowania zaufania wśród osób, których dane dotyczą.

3.9 Rozliczalność[41]

86. Zasada rozliczalności przewiduje, że administrator jest odpowiedzialny za przestrzeganie wszystkich wyżej wymienionych zasad i jest w stanie wykazać ich przestrzeganie.

87. Administrator powinien mieć możliwość wykazania zgodności z tymi zasadami. W ten sposób może on przedstawić skuteczność środków, które zostały podjęte, aby chronić prawa osób, których dane dotyczą, oraz uzasadnić, dlaczego środki te zostały uznane za odpowiednie i skuteczne. Na przykład wykazanie, dlaczego dany środek można uznać za odpowiedni i skuteczny w celu zapewnienia przestrzegania zasady ograniczenia przechowywania.

88. Administrator powinien dysponować zarówno wiedzą na temat ochrony danych, jak i możliwością jej wdrożenia, aby móc odpowiedzialnie przetwarzać dane osobowe. Oznacza to, że administrator danych powinien rozumieć swoje obowiązki w zakresie ochrony danych wynikające z RODO i wywiązywać się z nich.

4 ARTYKUŁ 25 UST. 3 – CERTYFIKACJA

89. Zgodnie z art. 25 ust. 3 certyfikacja na podstawie art. 42 może być stosowana jako element wykazujący zgodność z ochroną danych w fazie projektowania oraz domyślną ochroną danych. Z kolei dokumenty wykazujące zgodność z ochroną danych w fazie projektowania oraz domyślną ochroną danych mogą być również użyteczne w procesie certyfikacji. Oznacza to, że jeżeli operacja przetwarzania przez administratora lub podmiot przetwarzający została poświadczona certyfikatem zgodnie z art. 42, organy nadzorcze uwzględniają to w swojej ocenie zgodności z RODO, w szczególności w odniesieniu do ochrony danych w fazie projektowania oraz domyślnej ochrony danych.

[41] Zob. motyw 74, zgodnie z którym administratorzy są zobowiązani do wykazania skuteczności wprowadzonych przez siebie środków.

90. W przypadku gdy operacja przetwarzania przez administratora lub podmiot przetwarzający jest certyfikowana zgodnie z art. 42, czynnikami, które przyczyniają się do wykazania zgodności z art. 25 ust. 1 i 2, są procesy projektowania, tj. procesy ustalania sposobów przetwarzania, zarządzania oraz środków technicznych i organizacyjnych służących wdrożeniu zasad ochrony danych. Kryteria certyfikacji w zakresie ochrony danych są określane przez podmioty certyfikujące lub właścicieli systemów certyfikacji, a następnie zatwierdzane przez właściwy organ nadzorczy lub przez EROD. Więcej informacji na temat mechanizmów certyfikacji można znaleźć w wytycznych EROD dotyczących certyfikacji[42] oraz innych odpowiednich wytycznych, opublikowanych na stronie internetowej EROD.

91. Nawet w przypadku gdy operacja przetwarzania jest certyfikowana zgodnie z art. 42, administrator nadal jest odpowiedzialny za ciągłe monitorowanie i ulepszanie zgodności z kryteriami ochrony danych w fazie projektowania oraz domyślnej ochrony danych określonymi w art. 25.

5 EGZEKWOWANIE PRZEPISÓW ART. 25 I KONSEKWENCJE

92. Organy nadzorcze mogą przeprowadzić ocenę zgodności z art. 25 zgodnie z procedurami określonymi w art. 58. Uprawnienia naprawcze określono w art. 58 ust. 2 i obejmują one wydawanie ostrzeżeń, udzielanie upomnień, nakazanie poszanowania praw osób, których dane dotyczą, wprowadzenie ograniczenia lub zakazu przetwarzania, zastosowanie administracyjnej kary pieniężnej itp.

93. Ochrona danych w fazie projektowania oraz domyślna ochrony danych są także czynnikiem określającym wysokość sankcji pieniężnych za naruszenie przepisów RODO, zob. art. 83 ust. 4[43] [44].

6 ZALECENIA

94. Wprawdzie art. 25 nie odnosi się bezpośrednio do podmiotów przetwarzających i wytwórców, jednak są oni również uznawani za kluczowe podmioty zapewniające realizację ochrony danych w fazie projektowania oraz domyślnej ochrony danych i powinni zdawać sobie sprawę, że administratorzy danych są zobowiązani do przetwarzania danych osobowych wyłącznie za pomocą systemów i technologii, które mają zintegrowaną ochronę danych.

95. Przetwarzając dane w imieniu administratorów lub dostarczając rozwiązania administratorom danych, podmioty przetwarzające i wytwórcy powinni wykorzystywać swoją wiedzę fachową do budowania zaufania i kierowania działaniami swoich klientów, w tym MŚP, w zakresie projektowania/zapewniania rozwiązań, które włączają ochronę danych do procesów przetwarzania. Oznacza to zaś, że projektowanie produktów i usług powinno wychodzić naprzeciw potrzebom administratorów danych.

96. Wdrażając postanowienia art. 25, należy pamiętać, że głównym celem projektowania jest *skuteczna realizacja* zasad i *ochrona* praw osób, których dane dotyczą, przy zastosowaniu odpowiednich środków przetwarzania. Aby ułatwić i usprawnić przyjęcie ochrony danych w fazie projektowania oraz

[42] EROD. „Wytyczne 1/2018 dotyczące certyfikacji i określania kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia". Wersja 3.0, 4 czerwca 2019 r. https://uodo.gov.pl/pl/file/1462

[43] W art. 83 ust. 2 lit. d) RODO stwierdzono, że przy ustalaniu wysokości kar pieniężnych za naruszenie przepisów RODO zwraca się „należytą uwagę" na „stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32".

[44] Więcej informacji na temat kar pieniężnych znajduje się w wytycznych Grupy Roboczej Art. 29. „Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia nr 2016/679". WP 253, 3 października 2017 r. https://uodo.gov.pl/pl/file/21 – zatwierdzone przez EROD

domyślnej ochrony danych, przekazujemy poniższe zalecenia administratorom, a także wytwórcom i podmiotom przetwarzającym:

- Administratorzy powinni myśleć o ochronie danych już na *początkowych etapach* planowania operacji przetwarzania, nawet przed określeniem sposobów przetwarzania.
- W przypadku gdy administrator danych ma inspektora ochrony danych (IOD), EROD zachęca IOD do aktywnego udziału w procedurach zamówień i rozwoju ochrony danych w fazie projektowania oraz domyślnej ochrony danych, jak również w całym procesie przetwarzania.
- Operacja przetwarzania może być *certyfikowana*. Możliwość uzyskania certyfikacji operacji przetwarzania stanowi wartość dodaną dla administratora danych przy dokonywaniu wyboru między różnymi rodzajami oprogramowania, sprzętu, usług lub systemów przetwarzania pochodzących od wytwórców lub podmiotów przetwarzających. Wytwórcy powinni zatem dążyć do wykazania ochrony danych w fazie projektowania oraz domyślnej ochrony danych w całym procesie opracowywania rozwiązania w zakresie przetwarzania. Pieczęć (znak jakości) certyfikacji może również stanowić dla osób, których dane dotyczą, wskazówkę przy dokonywaniu wyboru między różnymi towarami i usługami. Możliwość uzyskania certyfikacji przetwarzania może służyć jako przewaga konkurencyjna dla wytwórców, podmiotów przetwarzających i administratorów, a nawet zwiększa zaufanie osób, których dane dotyczą, do przetwarzania ich danych osobowych. W przypadku braku certyfikacji administratorzy powinni dążyć do uzyskania innych *form gwarancji* zapewniających, że wytwórcy lub podmioty przetwarzające spełniają wymogi ochrony danych w fazie projektowania oraz domyślnej ochrony danych.
- Administratorzy, podmioty przetwarzające i wytwórcy powinni uwzględnić swoje obowiązki w zakresie zapewnienia dzieciom poniżej 18. roku życia i innym grupom szczególnie wrażliwym szczególnej ochrony w zakresie zgodności z wymogami ochrony danych w fazie projektowania oraz domyślnej ochrony danych.
- Wytwórcy i podmioty przetwarzające powinni dążyć do tego, by ułatwić realizację ochrony danych w fazie projektowania oraz domyślnej ochrony danych w celu wsparcia potencjału administratora w zakresie spełniania obowiązków wynikających z art. 25. Z drugiej strony administratorzy nie powinni wybierać wytwórców lub podmiotów przetwarzających, którzy nie oferują systemów umożliwiających administratorowi spełnienie wymogów art. 25 lub wspierających go w tym procesie, ponieważ administratorzy zostaną pociągnięci do odpowiedzialności za brak ich wdrożenia.
- Wytwórcy i podmioty przetwarzające powinni odgrywać czynną rolę w zapewnieniu spełnienia kryteriów dotyczących „stanu wiedzy technicznej" oraz informować administratorów o wszelkich zmianach „stanu wiedzy technicznej", które mogą wpływać na skuteczność wdrożonych środków. Administratorzy powinni uwzględnić ten wymóg jako klauzulę umowną, aby mieć pewność, że będą informowani na bieżąco.
- EROD zaleca administratorom, aby wymagali od wytwórców i podmiotów przetwarzających wykazania, w jaki sposób ich sprzęt, oprogramowanie, usługi lub systemy umożliwiają administratorowi spełnienie wymogów w zakresie rozliczalności zgodnie z ochroną danych w fazie projektowania oraz domyślną ochrony danych, na przykład poprzez zastosowanie kluczowych wskaźników wydajności w celu wykazania skuteczności środków i zabezpieczeń przy wdrażaniu zasad i praw.
- EROD podkreśla również potrzebę zharmonizowanego podejścia do skutecznego wdrażania zasad i praw oraz zachęca stowarzyszenia lub organy przygotowujące kodeksy postępowania

zgodnie z art. 40 do uwzględnienia w nich wytycznych w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrony danych dla poszczególnych sektorów.

- Administratorzy powinni być uczciwi w stosunku do osób, których dane dotyczą, oraz przejrzyści w sposobie oceny i wykazywania skuteczności wdrażania ochrony danych w fazie projektowania oraz domyślnej ochrony danych, podobnie jak administratorzy wykazują zgodność z przepisami RODO w ramach zasady rozliczalności.
- Technologie służące wzmocnieniu ochrony prywatności (PETs), które osiągnęły najwyższy poziom rozwoju, mogą być stosowane jako środek zgodny z wymogami ochrony danych w fazie projektowania oraz domyślnej ochrony danych, w stosownych przypadkach w ramach podejścia opartego na ryzyku. Technologie te nie muszą same w sobie uwzględniać obowiązków wynikających z art. 25. Administratorzy danych oceniają, czy dany środek jest odpowiedni i skuteczny w zakresie wdrażania zasad ochrony danych i praw osób, których dane dotyczą.
- Istniejące dotychczas systemy podlegają tym samym obowiązkom ochrony danych w fazie projektowania oraz domyślnej ochrony danych, co nowe systemy. Jeżeli nie są one już zgodne z wymogami ochrony danych w fazie projektowania oraz domyślnej ochrony danych, a nie można dokonać zmian w celu spełnienia tych wymogów, wówczas przestają spełniać wymogi RODO i nie mogą być dalej wykorzystywane do przetwarzania danych osobowych.
- W art. 25 nie obniżono progu wymogów dla MŚP. Poniższe punkty mogą ułatwić MŚP przestrzeganie przepisów art: 25:
    - przeprowadzanie wczesnych ocen ryzyka
    - wprowadzenie przetwarzania na małej próbie, a następnie rozszerzanie zakresu przetwarzania i stopnia jego zaawansowania
    - oczekiwanie od wytwórcy i pomiotu przetwarzającego gwarancji realizowania ochrony danych w fazie projektowania oraz domyślnej ochrony danych, takich jak certyfikacja i stosowanie kodeksu postępowania
    - korzystanie z pomocy partnerów posiadających dobre wyniki
    - konsultacje z organami ochrony danych
    - zapoznanie się z wytycznymi organów ochrony danych i EROD
    - stosowanie kodeksów postępowania, jeżeli są one dostępne
    - korzystanie z profesjonalnej pomocy i porady.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)