FUNDACJA PANOPTYKON

NOWA FILOZOFIA W OCHRONIE DANYCH OSOBOWYCH:

od oceny ryzyka do spójnej strategii w organizacji

Opracowanie: Katarzyna Szymielewicz | Fundacja Panoptykon, panoptykon.org

Na czym polega zmiana regulacyjnego podejścia wynikająca z ogólnego rozporządzenia o ochronie danych osobowych (RODO)?

Jak przełożyć nowe, elastyczne mechanizmy – takie jak ocena ryzyka – na praktykę działania organizacji?

Czy procesy, których wymaga RODO, można wykorzystać także dla osiągnięcia korzyści biznesowych? Jak to zrobić?

Oto praktyczny poradnik dla wszystkich przetwarzających dane osobowe.

Nowa filozofia o ochronie danych osobowych:
od oceny ryzyka do spójnej strategii w organizacji

Opracowanie: Katarzyna Szymielewicz
Korekta: Urszula Dobrzańska
Projekt graficzny i skład: Mariana Wybieralska

Październik 2017

panoptykon.org

Spis treści

SŁOWO WSTĘPU

Dużymi krokami zbliża się moment, w którym wszystkie podmioty wykorzystujące dane osobowe będą musiały przestawić się na nowy regulacyjny paradygmat. General-ne rozporządzenie o ochronie danych osobowych (RODO)[1] weszło w życie w 2016 r., a po 25 maja 2018 r. zacznie być w pełni stosowane. To oznacza realne ryzyko kar finansowych i innych sankcji dla podmiotów (zarówno komercyjnych, jak i niekomercyjnych), które do tego czasu nie dostosują swoich procedur.

Na te zmiany można patrzeć albo w kategorii wyzwań i koniecznych kosztów, albo szans i możliwych korzyści – także w wymiarze biznesowym. Proponując to drugie spojrzenie, nie zamierzamy pomijać oczywistego faktu, że wdrożenie nowych procedur oznacza realny wysiłek dla każdej organizacji. Uważamy jednak, że zamiast traktować ten etap jako zło konieczne (koszt działania zgodnie z prawem) **warto pójść krok dalej i wykorzystać procesy, których wdrożenia wymaga RODO, do rozwoju i wzmocnienia całej organizacji**.

W niniejszym opracowaniu podpowiadamy:

1. jak w siedmiu krokach przeprowadzić ocenę ryzyka i skutków dla ochrony danych;
2. jakie pytania postawić, żeby ocenić, czy dane są przetwarzane zgodnie z prawem;
3. jak przełożyć prawa osób, których dane są przetwarzane, na konkretne procedury w organizacji;
4. jak zidentyfikować rodzaje zagrożeń, ich źródła i prawdopodobieństwo;
5. wreszcie – jak nie zmarnować inwestycji, jaką jest pełne wdrożenie RODO, i wejść na kolejny poziom: wypracować strategię zarządzania danymi w organizacji.

Staraliśmy się możliwie prosto – ale nie upraszczając – przedstawić skomplikowaną, w tym prawną i techniczną, materię. Stąd wybór konstrukcji, w której najpierw opisujemy zależności między poszczególnymi procesami wynikającymi z RODO (rozdział 2), następnie ogólny schemat oceny ryzyka i skutków dla ochrony danych (rozdział 3), a na koniec praktyczne wskazówki i metody, które w ramach takiej oceny warto wykorzystać (rozdział 4). Ponadto przypominamy, dlaczego warto zmierzyć się z RODO (rozdział 1), i pokazujemy, jak odpowiedzialne zarządzanie danymi na stałe wpisać w życie organizacji (rozdział 5).

Zapraszamy do lektury! →

1 Źródło: http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016R0679.

ROZDZIAŁ I

DLACZEGO WARTO ZMIERZYĆ SIĘ Z RODO?

Organizacje, które planują przyszłość i liczą się z konsekwencjami swoich działań, w zasadzie nie mają wyboru: muszą się zmierzyć z obowiązkami wynikającymi z RODO. Konsekwencje zaniedbania tej sfery mogą być bardzo namacalne, przede wszystkim w wymiarze finansowym. Ale nie chodzi tylko o pieniądze, chodzi także o relacje z coraz więcej oczekującymi konsumentami i budowanie przewagi konkurencyjnej na nowym rynku.

Z perspektywy konsumentów wdrożenie RODO to obietnica lepszego doświadczenia i większej kontroli w relacji z administratorami (czyli osobami – fizycznymi lub prawnymi – które ustalają cele i sposoby przetwarzania danych osobowych). W szczególności mogą oni liczyć na:

- szczegółową, a jednocześnie przystępną informację (podaną w tzw. ludzkim języku) o tym, jakie ich dane i w jakich celach są przetwarzane;
- prawo do przeniesienia danych w formacie, który umożliwia ich załadowanie do innej aplikacji/usługi;
- wyjaśnienie, jaka logika stoi za automatycznym podejmowaniem decyzji w ich sprawie, oraz na ludzką interwencję;
- domyślne ustawienia w maksymalny sposób chroniące ich prywatność;
- możliwość pozwania każdej firmy, która te standardy narusza, we własnym kraju.

Jeśli w praktyce okaże się, że firmy lub inne organizacje przetwarzające dane osobowe tych standardów nie przestrzegają, na fali mocno nagłośnionej reformy i rosnących oczekiwań **konsumenci będą się skarżyć i dochodzić swoich praw**. Biorąc pod uwagę wzmocnione i szybsze procedury egzekwowania prawa, jakie przewiduje polska ustawa wdrażająca RODO[2], w tym możliwość wnoszenia skarg także przez organizacje konsumenckie, ten scenariusz wydaje się bardzo prawdopodobny.

W polskim porządku prawnym pojawi się też **nowa, wzmocniona instytucja** odpowiedzialna za egzekwowanie przepisów o ochronie danych osobowych: **Urząd Ochrony Danych Osobowych** (UODO), kierowany przez prezesa Urzędu (PUODO). Przynajmniej w pierwszych latach obowiązywania nowego prawa administratorzy mogą zatem spodziewać się kontroli podejmowanych z urzędu[3], szczególnie kiedy w grę wchodzi duża skala przetwarzania danych (banki, firmy telekomunikacyjne, brokerzy danych) lub innowacyjne – a jednocześnie ryzykowne – rozwiązania (np. tzw. Internet rzeczy).

2 Por. Ministerstwo Cyfryzacji, *Nowe prawo ochrony danych osobowych*, https://www.gov.pl/cyfryzacja/dokumenty27.

3 Por. art. 57 i 58 RODO.

Dotkliwe sankcje administracyjne

PUODO będzie miał do dyspozycji całą paletę **perswazyjnych lub korygujących środków**, takich jak:

- ostrzeżenia (o możliwości naruszenia przepisów);
- udzielanie upomnień (w przypadku naruszenia przepisów);
- nakazanie spełnienia żądania osoby, której dane dotyczą;
- nakazanie dostosowania operacji przetwarzania do przepisów RODO;
- wprowadzenie czasowego lub całkowitego ograniczenia przetwarzania danych (w tym transferów międzynarodowych).

Niektóre z tych środków mogą się okazać **kosztowne lub dotkliwe w realizacji** – PUODO może przecież nakazać administratorowi niezwłoczne poinformowanie o zmianie w celach przetwarzania danych tysięcy klientów albo wprowadzić zakaz przetwarzania danych uderzający w jeden z kluczowych procesów biznesowych (np. zablokować możliwość przekazywania danych poza Unię Europejską korporacji, która procesy obsługi klientów realizuje w Indiach czy USA). Te przykłady pokazują, w jaki sposób **zagrożenie praw i wolności podmiotów danych** (wcześniej najwyraźniej zignorowane przez administratora) może stać się podstawą korygującej decyzji PUODO i przełożyć się na **ryzyko biznesowe** dla samego administratora.

Za przetwarzanie danych niezgodnie z przepisami RODO będą grozić także **wysokie kary pieniężne** (do 20 mln euro lub 4% rocznego obrotu przedsiębiorstwa). Z punktu widzenia samego administratora, jego inwestorów, a pośrednio także pracowników i innych interesariuszy, ich dotkliwość będzie bardzo duża. To konkretny, przekładający się bezpośrednio na wyniki finansowe, czynnik ryzyka, którego żadna organizacja nie może bagatelizować, planując wdrożenie RODO.

W jakich sytuacjach pojawia się ryzyko kary finansowej?

Organ ochrony danych może nałożyć karę w wysokości do 20 mln euro, a w przypadku przedsiębiorstwa – do 4% jego całkowitego rocznego światowego obrotu, jeśli administrator:

- narusza **podstawowe zasady przetwarzania danych osobowych**, w tym warunki udzielonej mu zgody na przetwarzanie danych (art. 5, 6, 7 oraz 9 RODO);
- **nie realizuje swoich obowiązków względem osób, których dane dotyczą** (art. 12–20);
- narusza zasady dotyczące transferów danych (art. 44–49);
- nie przestrzega nakazów organu ochrony danych (np. tymczasowego ograniczenia przetwarzania).

Niższe kary (w wysokości do 10 mln euro, a w przypadku przedsiębiorstwa – do 2% jego całkowitego rocznego światowego obrotu) grożą m.in. w przypadku:

- nieuwzględnienia ochrony danych w fazie projektowania lub nieuwzględnienia zasad domyślnej ochrony danych (*privacy by design* i *privacy by default*) (art. 25 RODO);
- zaniedbania **oceny skutków dla ochrony danych** (w przypadku stwierdzenia wysokiego ryzyka dla praw i wolności podmiotów danych) lub (jeśli są wymagane) **uprzednich konsultacji z organem** ochrony danych (art. 35, 36);
- zaniedbania wymaganych ustaleń między współadministratorami (art. 26) lub między administratorem i podmiotem przetwarzającym dane (art. 26 i 28);
- naruszenia obowiązków przez podmioty certyfikujące (art. 42 i 43);
- naruszenia warunków wyrażenia zgody przez dziecko (art. 8);
- zbierania danych identyfikujących podmiot danych, mimo że nie wymagają tego cele administratora (art. 11)[4].

Wymierzając karę i decydując o jej wysokości, organ ochrony danych nie działa automatycznie. Bierze pod uwagę takie czynniki jak: umyślność, stopień współpracy ze strony administratora, wagę naruszenia oraz sposób, w jaki dowiedział się o naruszeniu. Zgodnie z RODO powinien rozpatrywać sprawy indywidualnie i starać się, by jego rozstrzygnięcia były proporcjonalne, ale też odstraszające.

Jak było do tej pory? GIODO i środki egzekucyjne

Generalny Inspektor Ochrony Danych Osobowych (organ odpowiedzialny za egzekwowanie polskich przepisów o ochronie danych osobowych) może stosować środki egzekucyjne, także o charakterze pieniężnym. Egzekucji podlegają jego decyzje administracyjne, jeśli nadał im rygor natychmiastowej wykonalności albo stały się ostateczne (nie przysługuje już od nich odwołanie).

W jakich sytuacjach mogą się pojawić sankcje finansowe wg starych zasad? Przede wszystkim w sytuacji, w której na administratora został nałożony konkretny obowiązek (np. zaprzestania przetwarzania danych czy poinformowania podmiotu danych), ale ten go nie realizuje. Wówczas GIODO może nałożyć grzywnę „w celu przymuszenia".

Do tej pory skala stosowania takich środków była niewielka. W 2015 r. GIODO wydał 97 decyzji zawierających nakaz wykonania i podlegających egzekucji, ale tylko w dwóch przypadkach nałożył grzywnę (obie w wysokości 40 000 zł).

4 Por. art. 58 RODO.

Nie tylko ryzyko: RODO jako szansa na przewagę konkurencyjną

Jak podkreśla Minister Cyfryzacji Anna Streżyńska, odpowiedzialna w Polsce za wdrożenie nowych przepisów, **RODO to nie tylko kary**[5]. To przede wszystkim szansa dla odpowiedzialnych i innowacyjnych firm, by na nowo zaprojektować swoją strategię zarządzania danymi i relacje z osobami, których dane przetwarzają. Nie czekając na twarde działania ze strony organów państwa, mogą budować w tym obszarze swoją przewagę konkurencyjną.

Przejrzyste zasady przetwarzania danych i przyjazne procedury w relacjach z konsumentami i użytkownikami budują zaufanie. A zaufanie, w dłuższym horyzoncie czasowym, przekłada się na lojalność oraz większą skłonność do dzielenia się informacjami. Człowiek, który rozumie, co się dzieje z jego danymi, i czuje, że ma realną kontrolę w tej sferze, chętniej ujawni swoje rzeczywiste preferencje, wejdzie w dialog z marketerem i otworzy się na oferowaną mu usługę czy produkt.

Odpowiedzialnego podejścia do zarządzania informacją i otwartej komunikacji na temat tego, co się dzieje z ich danymi, zaczynają oczekiwać od firm sami konsumenci. Według badań przeprowadzonych w Polsce i USA przez firmę Deloitte konsumenci są skłonni wybierać produkty i usługi tych firm, które lepiej chronią ich dane osobowe[6]. Wielu z nich obawia się utraty kontroli nad swoimi danymi. Dlatego oczekują od firm większej przejrzystości, wysokich standardów ochrony danych (np. przyjaznych im domyślnych ustawień w usługach internetowych) i prostych procedur (np. kiedy chcą zgłosić sprzeciw albo przenieść dane gdzie indziej).

Pełne wdrożenie RODO może się okazać wyzwaniem dla wielu firm, szczególnie tych, które wykorzystują dane osobowe na masową skalę. Tego procesu nie należy jednak utożsamiać z samymi obciążeniami. To także szansa na uproszczenie procedur oraz zbudowanie z klientami relacji opartej na zaufaniu i zrozumieniu ich potrzeb związanych z ochroną prywatności.

5 Por. Fundacja Panoptykon, *Śledzenie i profilowanie w sieci. W czym problem? Co się zmieni w prawie? Jak może wyglądać przyszłość?* (z komentarzem minister Anny Streżyńskiej), 2017, https://panoptykon.org/sites/default/files/publikacje/sledzenie_i_profilowanie_w_sieci_scenariusze_po_reformie_ue_wrzesien_2017.pdf.

6 Deloitte, *Building consumer trust Protecting personal data in the consumer product industry*, 2014, https://dupress.deloitte.com/dup-us-en/topics/risk-management/consumer-data-privacy-strategies.html; Deloitte, *Raport: Rok do RODO – ochrona danych osobowych oczami polskich konsumentów*, 2017, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/raport-rok-do-rodo-ochrona-danych-osobowych-oczami-polskich-konsumentow.html.

ROZDZIAŁ 2

REWOLUCJA CZY LIFTING DOTYCHCZAS OBOWIĄZUJĄCYCH ZASAD, CZYLI CO ZMIENIA RODO

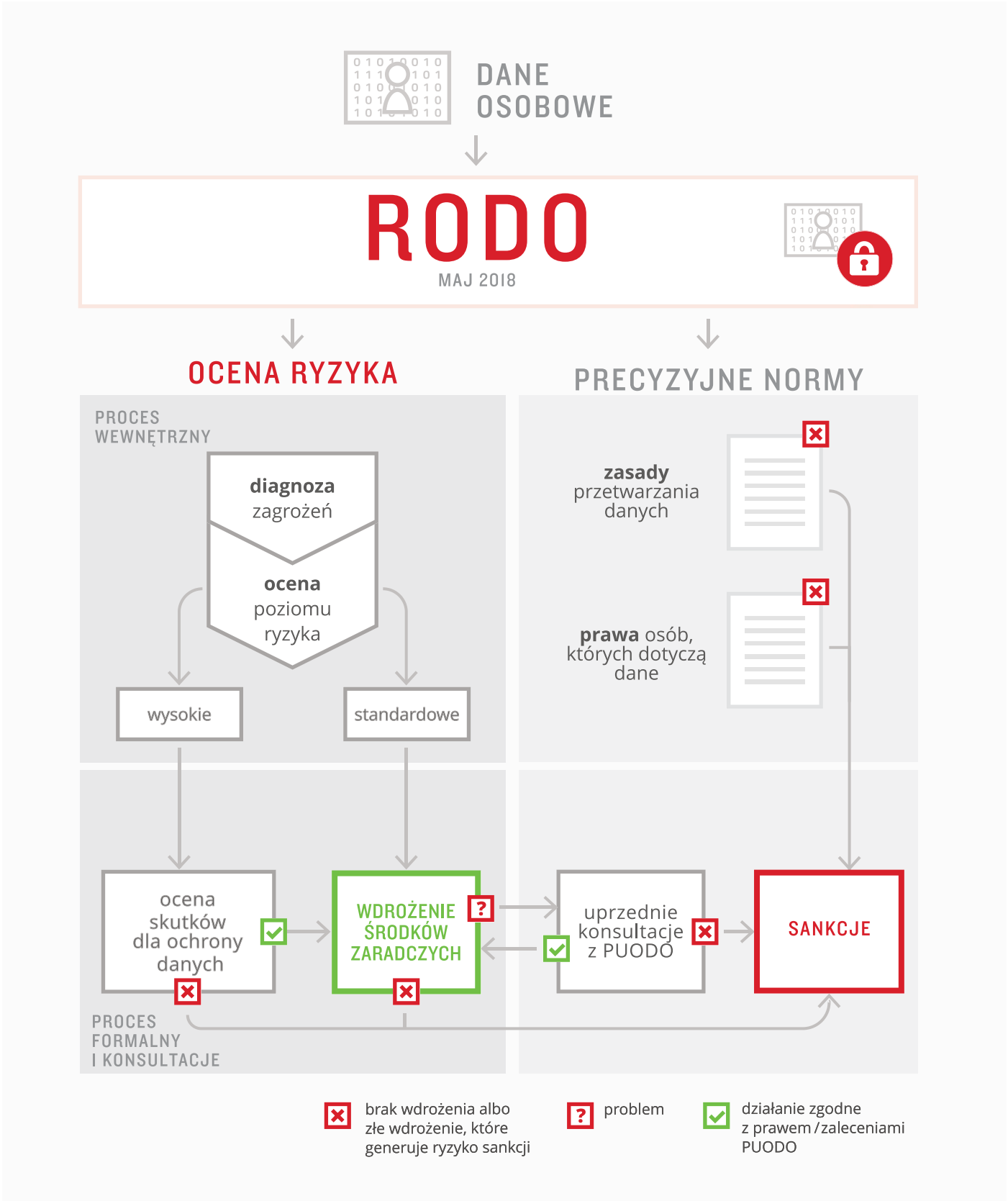
Przetwarzanie danych jest traktowane w RODO jako proces, który z definicji stwarza pewne ryzyka dla praw i wolności osób fizycznych. Nie oznacza to, że danych osobowych nie wolno wykorzystywać. Owszem, można to robić, ale tylko w ściśle określonych prawem ramach wyznaczonych przez tzw. **zasady przetwarzania danych** (por. kolejny punkt). W praktyce oznacza to, że każdy, kto zamierza podjąć taką działalność, już na wstępie powinien się zmierzyć z konkretną listą pytań:

- Jakie rodzaje danych będą przetwarzane, w jakich celach i w jaki sposób?
- Czy przetwarzanie wszystkich tych informacji jest niezbędne i proporcjonalne?
- Czy jesteśmy w stanie określić podstawy prawne ich przetwarzania?
- Czy – mimo formalnego spełnienia obowiązków prawnych z przetwarzaniem tych danych może się wiązać ryzyko dla osób, których one dotyczą (tj. określone zagrożenia)?
- Czy potrafimy zidentyfikować rodzaje, źródła i poziom tych zagrożeń?
- Czy potrafimy tym zagrożeniom zaradzić, a przynajmniej je zminimalizować?

Zmierzenie się z wymogami RODO warto zacząć od rzetelnego **zmapowania źródeł i przepływów danych**, następnie należy ocenić **legalność ich przetwarzania**, a dopiero w kolejnym kroku analizować możliwe konsekwencje takiego działania dla podmiotów danych (**ocena ryzyka sensu stricto**). Jeśli już na pierwszym etapie zaczną się pojawiać wątpliwości, stanowić to będzie sygnał ostrzegawczy, że może nie warto iść dalej.

Weryfikacji zgodności przetwarzania danych z RODO nie dokonuje się tylko raz – ale cyklicznie – i nie ma ona linearnego charakteru. Czasem (np. w przypadku zdiagnozowania wysokiego ryzyka związanego z przetwarzaniem danych) RODO nakazuje powtórzenie pewnych czynności. Każdy etap rozwija się w kolejny proces, co powoduje, że mamy do czynienia ze złożoną konstrukcją. Kolejne rozdziały tego opracowania zawierają praktyczne wskazówki, jak się zmierzyć z poszczególnymi etapami i procesami.

Mapa drogowa: jak się odnaleźć w RODO?



Ugruntowane zasady

Mimo dużej elastyczności, jaką administratorom danych daje RODO, pewne rzeczy są stałe. Na poziomie podstawowych zasad przetwarzania danych i konkretnych praw przysługujących osobom, których dane dotyczą, rozporządzenie nie wprowadza rewolucji: to raczej lifting dotychczas obowiązujących przepisów. Dla wszystkich, którzy już wcześniej mierzyli się z ochroną danych, te przepisy będą brzmiały znajomo. Oto podstawowe zasady przetwarzania danych osobowych:

- legalność;
- ograniczenie celem;
- adekwatność, niezbędność i minimalizacja;
- prawidłowość;
- maksymalny czas przetwarzania;
- poufność i integralność;
- przejrzystość[7].

Te zasady to **podstawowa checklista każdego administratora**. W praktyce musi się z nimi zmierzyć albo zarząd organizacji (firmy, instytucji publicznej), albo osoba przez ten zarząd oddelegowana (zgodnie z nowymi regułami będzie to inspektor ochrony danych). Podstawowym obowiązkiem administratora jest zapewnienie przestrzegania tych zasad: zadbanie o to, by w organizacji nie było danych osobowych nieadekwatnych do celu, niepoprawnych, narażonych na ryzyko wycieku bądź przetwarzanych bez podstawy prawnej, w innym celu niż pierwotnie zakładany czy po prostu zbyt długo.

Logiczną konsekwencją zasad broniących dostępu do danych osobowych są – wynikające z nich bezpośrednio – **prawa osób, których dane są przetwarzane**. Jeśli administrator jest w stanie wykazać, że przetwarza dane zgodnie z zasadami, jakie przewiduje RODO, nie powinien mieć też żadnego problemu ze zrealizowaniem swoich obowiązków względem osób, których te dane dotyczą. Podążając za wewnętrzną logiką tej regulacji, można spojrzeć na prawa osób, których dane są przetwarzane, jako na drugi bastion chroniący przed ryzykownymi lub nielegalnymi praktykami.

Jeśli fundamentalne zasady przetwarzania danych to granica, poza którą żaden administrator danych nie powinien wychodzić, prawa podmiotów danych to treść, bez której standard ochrony danych przewidziany w RODO byłby pusty.

7 Na gruncie RODO przejrzystość jest traktowana jako bezwzględny warunek zgodności przetwarzania danych z prawem, podobnie jak pozostałe zasady. Jednak, w praktyce, trudno ją sprowadzić do twardego kryterium (jest/nie ma). Dlatego w tym przewodniku traktujemy ją jako standard, którego administrator powinien przestrzegać w relacji z podmiotami danych. Opisujemy ją w punkcie poświęconym uprawnieniom osób, których dane są przetwarzane (s. 12), a nie w rozdziale zawierającym praktyczne wskazówki dla oceny zgodności przetwarzania danych z prawem (s. 27).

Jakie uprawnienia dla osób, których dane są przetwarzane, przewiduje RODO?

- prawo do **informacji** o tym, jakie dane i w jakich celach są przetwarzane, a w przypadku zautomatyzowanego podejmowania decyzji (w tym profilowania) – także do informacji o zasadach ich podejmowania, znaczeniu i przewidywanych konsekwencjach takiego przetwarzania (zgodnie z art. 12, 13 i 14);
- prawo do **udostępniania i przeniesienia danych** (zgodnie z art. 15 i 20);
- prawo do poprawienia i usunięcia danych (zgodnie z art. 16 i 17);
- prawo do **wycofania zgody** w każdym momencie, **zgłoszenia sprzeciwu** lub żądania ograniczenia przetwarzania danych (zgodnie z art. 7, 18 i 21);
- prawo do **ludzkiej interwencji** i zakwestionowania decyzji w sytuacji, kiedy system mówi „nie" (zgodnie z art. 22).

Wśród tych praw trudno wskazać ważne i ważniejsze. Realne konsekwencje ich naruszenia mogą mieć różne znaczenie w zależności od kontekstu i sytuacji życiowej osoby, której dane dotyczą. Na przykład prawo poprawienia danych będzie miało inny wymiar w kontekście marketingowym (źle dopasowana reklama), a inny w relacji z bankiem czy państwem (kiedy w grę wchodzi błędna i wiążąca decyzja).

A jednak trudno sobie wyobrazić sensowne żądanie sprostowania czy usunięcia danych albo zgłoszenie sprzeciwu wobec praktyk marketingowych bez wiedzy na temat tego, jakie dane rzeczywiście są przetwarzane. **Dostęp do rzetelnych informacji ma kluczowe** znaczenie z punktu widzenia praktycznej możliwości zrealizowania pozostałych uprawnień. W tym sensie uprawnienia wynikające z art. 12–14 RODO są bazą i warunkiem umożliwiającym realizację pozostałych. **Zasada przejrzystości** wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem.

Europejski regulator naruszenie każdego z uprawnień, jakie wynikają z RODO (art. 12–20), traktuje z równą powagą i obwarowuje najpoważniejszymi sankcjami: administracyjnymi karami pieniężnymi w wysokości do 20 mln euro lub 4% globalnego obrotu). Zobacz punkt: Dotkliwe sankcje administracyjne.

Co ma znaczenie dla osoby, której dane są przetwarzane?

1	Czy wiem i rozumiem, co się dzieje z moimi danymi? Czy administrator mówi do mnie ludzkim językiem?
2	Czy naprawdę mogę powiedzieć „nie” (np. nie udostępnić dodatkowych danych lub nie zgodzić się na marketing innych podmiotów) i nadal korzystać z usługi?
3	Czy usługa/produkt nie wymaga ode mnie podawania więcej danych, niż to konieczne?
4	Czy moje dane nie są wykorzystywane poza moją kontrolą (np. w innych celach, niż się umawialiśmy)?
5	Czy rozumiem logikę profilowania i automatycznego podejmowania decyzji na mój temat? Czy mogę liczyć na to, że ostatecznie zweryfikuje ją człowiek?
6	Czy rzeczywiście mogę zabrać i przenieść swoje dane gdzie indziej?
7	Czy mogę zaufać, że moje dane są bezpieczne; a jeśli już wycieką – że zostanę o tym natychmiast poinformowany/-a?
8	Czy i w jaki sposób mogę się „wymazać” z serwisu/usługi, jeśli okaże się, że tego chcę?
9	Czy moje dane będą chronione nawet wtedy, kiedy sam/-a nic w tym kierunku nie zrobię (tj. na podstawie tzw. domyślnych ustawień)?

Nowe mechanizmy

O ile na poziomie samych zasad i praw osób, których dane dotyczą, RODO nie wprowadza rewolucji, o tyle proponuje inną filozofię ich wdrażania i weryfikowania. Aby wykazać, że wszystko odbywa się zgodnie z prawem, nie wystarczy już prawidłowe wypełnienie formularza (np. na etapie rejestracji zbioru danych, od której to procedury RODO zupełnie odchodzi) czy dobrze napisany regulamin na stronę internetową.

W miejsce sztywnych procedur pojawiają się elastyczne – ale też bardziej wymagające od administratorów – procesy, takie jak **ocena ryzyka i skutków dla ochrony danych**. Co więcej: RODO wymaga uwzględnienia wysokiego standardu ochrony danych już **na etapie projektowania technologii** i w **domyślnych ustawieniach** prywatności. Chodzi zatem nie tylko o wykazanie zgodności przetwarzania danych z przepisami prawa, ale też zagwarantowanie, że ten stan nie zmieni się wraz z przejściem na poziom biznesowych nawyków i faktycznego działania (*business as usual*).

Europejski regulator wychodzi z założenia, że **dane osobowe to ryzykowna i żywa substancja**, wymykająca się statycznym ocenom i ustandaryzowanym formularzom. Każdy, kto zamierza przetwarzać dane osobowe, musi się zmierzyć z konsekwencjami (w tym zagrożeniami), jakie taka decyzja za sobą pociąga. Dlatego RODO wymaga od administratorów samodzielnego przeprowadzania tzw. oceny ryzyka. Administrator powinien ją przeprowadzić nie tylko na początku – kiedy decyduje się na zbieranie danych – ale za każdym razem, kiedy w grę wchodzą nowe czynniki wpływające na poziom ryzyka.

Ocena ryzyka to standardowy proces towarzyszący każdemu przetwarzaniu danych, bez względu na jego skalę i związane z nim zagrożenia. Dopiero na podstawie jego wyników administrator będzie mógł zdecydować, czy potrzebne są kolejne kroki: formalny, angażujący zewnętrzne podmioty proces oceny skutków dla danych osobowych, a nawet uprzednie konsultacje z organem nadzorczym (→ **Mapa drogowa**).

Zgodnie art. 24 RODO, przystępując do wdrożenia „odpowiednich środków technicznych i organizacyjnych" (zapewniających zgodność przetwarzania danych z prawem), administrator powinien uwzględnić:

- charakter, zakres, kontekst i cele przetwarzania,
- stan wiedzy technicznej i koszt wdrażania oraz
- ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.

W kontekście RODO ryzyko to nic innego, jak scenariusz opisujący konkretne zdarzenie i jego konsekwencje (dla praw i wolności osób, których dane są przetwarzane), oszacowane pod kątem ich dotkliwości oraz prawdopodobieństwa.

W grę wchodzi nie tylko ryzyko naruszenia prywatności. Nieuprawnione, nadmiarowe czy po prostu błędnie zaprojektowane przetwarzanie danych może skutkować dyskryminacją, kradzieżą tożsamości, oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, znaczną szkodą gospodarczą lub społeczną. Osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi[7].

Czym różni się ocena ryzyka od oceny skutków dla ochrony danych?

Oba procesy – oceny ryzyka oraz oceny skutków dla ochrony danych – mają ten sam cel: określić, a następnie **wyeliminować lub ograniczyć ryzyko, jakie przetwarzanie danych może stanowić dla osób, których te dane dotyczą**. Ze względu na możliwe skutki prawne (w tym kary finansowe) i reputacyjne, to ryzyko przenosi się na poziom administratora i całej organizacji. RODO stawia jednak w centrum prawa i wolności osób fizycznych, i to ich perspektywę nakazuje przyjąć przy mapowaniu możliwych zagrożeń. Ta zmiana perspektywy odróżnia procesy opisane w RODO od standardowych ocen ryzyka, z którymi mają do czynienia zarządy komercyjnych organizacji (np. ocena ryzyka inwestycyjnego czy kredytowego). Niemniej jednak sam sposób definiowania ryzyka oraz metody przeprowadzenia jego oceny są analogiczne.

Przebieg i istotne cechy obu procesów są bardzo podobne, dlatego warto przyjąć spójną metodykę ich przeprowadzania w organizacji. **W praktyce ocena skutków dla ochrony danych to po prostu pełniejsza i nieco bardziej rozbudowana ocena ryzyka**. O ile w przypadku wewnętrznego, niesformalizowanego procesu oceny ryzyka konsultacje z podmiotami danych i zewnętrznymi ekspertami są po prostu dobrą praktyką, o tyle w pełnej ocenie skutków dla ochrony danych są już wymaganym standardem. Nic nie stoi jednak na przeszkodzie, by już ten pierwszy proces – wstępnej oceny ryzyka – przeprowadzać wg podobnej metody (→ **rozdział 3: Ocena ryzyka i skutków dla ochrony danych: krok po kroku**).

Ocenę ryzyka związanego z przetwarzaniem danych trzeba odróżnić od formalnej oceny jego zgodności z prawem. Zweryfikowanie, czy wszystkie zasady przetwarzania danych zostały spełnione, a wszystkie prawa osób, których dane dotyczą, dostatecznie zagwarantowane, to baza, bez której administrator po prostu nie może działać. Ocena ryzyka to kolejny krok, odpowiadający na pytanie: co może pójść „nie tak", przy założeniu, że organizacja działa legalnie?

8 Por. motyw 75 RODO.

Kiedy jest wymagana pełna ocena skutków dla ochrony danych?

Zgodnie z art. 35 RODO przeprowadzenie pełnej oceny skutków dla ochrony danych jest wymagane wtedy, gdy „dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować **wysokie ryzyko naruszenia praw lub wolności osób fizycznych**". Oczywiście, nie sposób tego stwierdzić bez przeprowadzenia wstępnej oceny ryzyka. Im rzetelniej zostanie potraktowany ten wstępny etap, tym lepsza będzie diagnoza możliwych zagrożeń i wdrożone środki zaradcze. W efekcie może się okazać, że kolejne (bardziej sformalizowane) etapy nie są już potrzebne.

Wysokie ryzyko naruszenia praw lub wolności osób fizycznych zwykle pojawia się, jeśli w grę wchodzi:

- ocena lub punktacja (w tym profilowanie lub prognozowanie) na podstawie danych osobowych (np. kształtowanie oferty dla klienta w oparciu o jego dotychczasowe nawyki zakupowe lub prognozowaną siłę nabywczą);
- podejmowanie automatycznych decyzji mających skutki prawne lub w podobny sposób istotnie wpływających na sytuację osoby, której dane dotyczą;
- przetwarzanie danych w celu systematycznego obserwowania, monitorowania lub kontroli osób, których dane dotyczą (np. wykorzystanie kamer do monitorowania ruchu na autostradach, monitorowanie pracowników);
- przetwarzanie danych wrażliwych (nie tylko wyraźnie wskazanych w art. 9 RODO – np. danych medycznych czy o osobach skazanych – ale też danych dotyczących komunikacji elektronicznej, danych o lokalizacji czy danych finansowych);
- przetwarzanie danych na dużą skalę, biorąc pod uwagę liczbę osób, których przetwarzanie dotyczy, wielkość lub różnorodność zbioru, czas i zasięg terytorialny przetwarzania danych;
- porównywanie lub łączenie zbiorów danych (np. w ramach akcji marketingowych prowadzonych na różnych platformach, tzw. *cross-platform targeting*, albo łączenie danych z różnych źródeł na potrzeby rekrutacji);
- przetwarzanie danych osób wymagających szczególnej ochrony (np. pracowników, dzieci, pacjentów czy osób starszych);
- innowacyjne użycie technologicznych lub organizacyjnych rozwiązań (np. połączenie identyfikacji odciskiem palca oraz mechanizmu rozpoznawania twarzy w celu kontrolowania dostępu do pomieszczeń, wykorzystanie w komercyjnych usługach sensorów ruchu podłączonych do sieci);
- transgraniczny transfer danych poza Unię Europejską;
- uniemożliwienie osobom, których dane dotyczą, skorzystania z praw lub usług (np. screening przed zaoferowaniem kredytu, ubezpieczenia czy oferty pracy)[9].

9 Przykłady za art. 35 RODO oraz wytycznymi Grupy Roboczej art. 29. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679.

ROZDZIAŁ 3

OCENA SKUTKÓW DLA OCHRONY DANYCH: KROK PO KROKU

Praktyczne wskazówki

Kiedy trzeba się zmierzyć z oceną ryzyka?

Warto to zrobić **tak wcześnie, jak to możliwe**. Najlepiej już na etapie projektowania procesów przetwarzania danych – nawet jeśli niektóre szczegóły i zmienne nie są jeszcze znane. Prawidłowo prowadzona ocena ryzyka lub skutków dla ochrony danych to żywy proces, który powinien być aktualizowany wraz ze zmieniającą się sytuacją w organizacji przetwarzającej dane. Jeśli pojawiają się nowe zmienne (kategorie danych, cele, metody przetwarzania) albo nowe zagrożenia, trzeba wrócić do oceny ryzyka i te czynniki uwzględnić. Zgodnie z wytycznymi Grupy Roboczej art. 29 cały proces należy powtarzać przynajmniej raz na 3 lata lub częściej, jeśli wymaga tego natura przetwarzania (np. szczególnie wysokie ryzyko) lub dynamicznie zmieniające się okoliczności[10].

Kto jest odpowiedzialny za przeprowadzenie tego procesu?

Zawsze administrator danych, czyli **osoba – fizyczna lub prawna – która ustala cele i sposoby przetwarzania danych osobowych**. Oczywiście, administrator może delegować to zadanie wewnątrz swojej organizacji (np. na inspektora ochrony danych) lub zaangażować do niego zewnętrznych ekspertów. To jednak nie zmienia faktu, że to on pozostaje odpowiedzialny za rzetelne przeprowadzenie oceny ryzyka/skutków dla ochrony danych i za wdrożenie wynikających z niej wytycznych.

10 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679.

Kogo warto zaangażować?

Przede wszystkim **osoby, których dane mają być przetwarzane**, ponieważ to ich prawa i wolności mogą być zagrożone. To dobra praktyka w każdym procesie oceny ryzyka związanego z przetwarzaniem danych, a w przypadku formalnej oceny skutków dla ochrony danych – swoisty obowiązek wynikający z RODO („w stosownych przypadkach administrator zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli”[11]). Aby realnie uwzględnić perspektywę podmiotów danych, administrator powinien stworzyć swoim klientom (konsumentom, użytkownikom, pacjentom, interesantom etc.) możliwość zabrania głosu w procesie oceny ryzyka (np. w formie ankiety lub badania fokusowego), a przynajmniej włączyć organizacje reprezentujące ich interesy (np. związki zawodowe, organizacje konsumenckie, organizacje broniące praw człowieka). Zgodnie z art. 35 RODO administrator powinien także zasięgnąć rady inspektora ochrony danych (jeśli ma takiego w swojej organizacji). Wreszcie: organy ochrony danych osobowych (ICO, CNIL) i Grupa Robocza art. 29 w swoich wytycznych zachęcają do zasięgania opinii niezależnych, zewnętrznych ekspertów: prawników, techników, ekspertów ds. bezpieczeństwa, socjologów, etyków etc.

Sam przebieg procesu oceny ryzyka i wynikające z niego wnioski powinny być **udokumentowane**, a w tym zakresie, w jakim dotyczą innych osób – także im udostępnione. W szczególności: jeśli administrator nie zgodził się z opiniami niezależnych ekspertów, organizacji konsumenckich lub zastrzeżeniami zgłoszonymi przez swoich klientów (użytkowników etc.) w procesie konsultacji, powinien im tę decyzję przekazać i uzasadnić.

Jaką metodę wybrać?

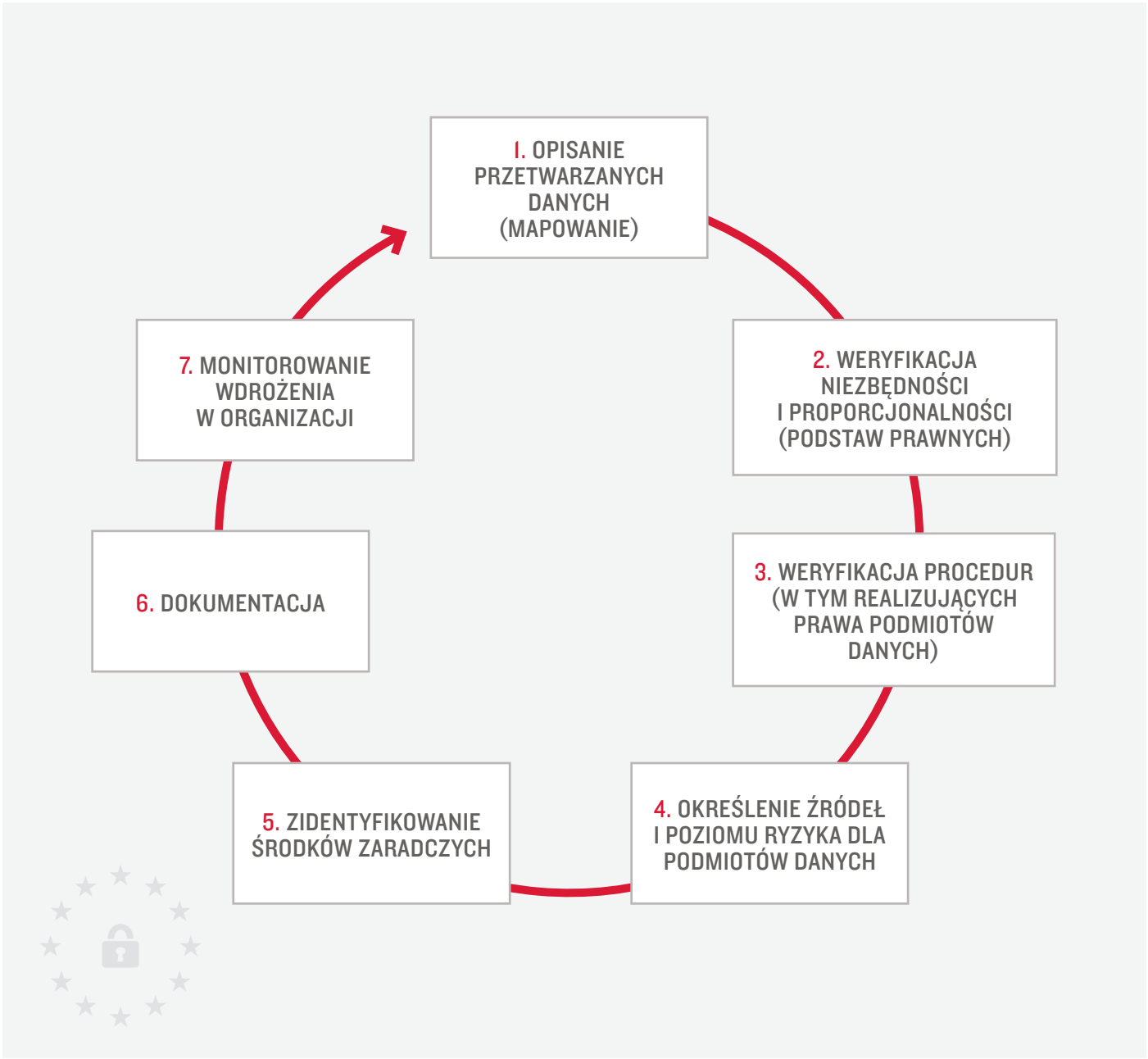
Formalna ocena skutków dla ochrony danych powinna, zgodnie z art. 35 RODO, obejmować określone etapy: opis procesów przetwarzania, ocenę niezbędności i proporcjonalności przetwarzania danych, właściwą ocenę ryzyka i wypracowanie środków zaradczych. Ani rozporządzenie, ani wytyczne Grupy Roboczej art. 29[12] nie narzucają jednak administratorowi konkretnej metody przeprowadzenia tego procesu.

Grupa Robocza art. 29 zachęca do korzystania z metod wypracowanych (jeszcze pod rządami starych przepisów) przez europejskie organy ochrony danych osobowych, np. brytyjski ICO i francuski CNIL. Na podstawie ich wytycznych opracowaliśmy **standardową metodę przeprowadzenia pełnej oceny skutków dla ochrony danych** (wraz z oceną ryzyka) w siedmiu krokach (por. kolejny punkt).

11 Por. art. 35 ust. 9 RODO.

12 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk” for the purposes of Regulation 2016/679.

7 kroków do pełnej oceny skutków dla ochrony danych



KROK I. MAPOWANIE BAZ I PRZEPŁYWÓW DANYCH

Pierwszy krok to zmapowanie wszystkich operacji, które angażują dane osobowe. W ramach systemów zarządzania informacjami dane osobowe muszą być odrębnie traktowane ze względu na wyższy poziom ochrony, jakiej wymagają. To z definicji wrażliwy zasób.

Co powinno się znaleźć na mapie danych osobowych?

- funkcjonalny opis wszystkich procesów angażujących dane osobowe (na czym polegają, czemu służą, jaką rolę odgrywają w nich dane osobowe);
- zakres i cele, w jakich dane są przetwarzane;
- rodzaje wykorzystywanych danych (w tym danych wrażliwych);
- kategorie osób, których te dane dotyczą (klienci, pracownicy, kontrahenci etc.);
- odbiorcy, którym dane są przekazywane (jeśli ma to miejsce);
- okresy, przez jakie dane są przechowywane;
- zasoby, na których jest oparte przetwarzanie danych (ludzie, sprzęt, oprogramowanie, papierowa dokumentacja).

Na jakie procesy warto zwrócić uwagę, mapując dane osobowe w organizacji?

- realizujące cele biznesowe (np. sprzedaż, marketing, obsługa klientów – w tym reklamacje i sprawy sporne);
- wymagane przez prawo (podatkowe, ubezpieczeń społecznych, bankowe etc.);
- niezbędne do zrealizowania obowiązków względem osób, których dane są przetwarzane (np. prawo do informacji, prawo do skorygowania, usunięcia czy przeniesienia danych).

Dane osobowe czasem **spoczywają** w wyodrębnionych zbiorach (np. baza kontaktów, archiwum obsługi klienta, e-maile), a czasem **są w ruchu** (np. logi z serwerów, numery IP, generowane na bieżąco dane finansowe). Obie sytuacje wymagają analizy pod kątem oceny ryzyka.

KROK 2. KONTROLA LEGALNOŚCI („STANU ZDROWIA")

Drugi krok to weryfikacja, czy wszystkie przetwarzane dane i związane z nimi procesy są niezbędne i proporcjonalne. To moment na kompleksową kontrolę stanu zdrowia organizacji pod kątem podstawowych zasad przetwarzania danych i obowiązków administratora, jakie przewiduje RODO.

Pełny opis tego procesu:
→ **Rozdział 4: Więcej praktycznych wskazówek, część: Jak ustalić, czy przetwarzanie danych jest zgodne z prawem? Kontrola „stanu zdrowia".**

Sprawdź:

- Czy jako organizacja w każdym przypadku potraficie wskazać (zgodny z prawem) cel przetwarzania danych i podstawę ich przetwarzania (np. realizacja umowy, zgoda podmiotu danych, przepis prawa, uzasadniony interes administratora)?
- Czy możecie osiągnąć ten sam cel, gromadząc i przetwarzając mniej danych?
- Czy część z nich można poddać anonimizacji lub pseudonimizacji?
- Czy nie przechowujecie danych zbyt długo? Czy usuwacie je, kiedy przestają być potrzebne?
- Czy w prosty i przystępny sposób informujecie osoby, których dane dotyczą, o celach, zakresie i czasie ich przetwarzania?
- Czy realizujecie pozostałe obowiązki względem tych osób (w tym prawo do skorygowania, przeniesienia, usunięcia danych)?

KROK 3. WERYFIKACJA KLUCZOWYCH PROCEDUR

Po zmapowaniu danych osobowych i upewnieniu się, że ich przetwarzanie jest zgodne z prawem, przychodzi moment na zweryfikowanie lub wprowadzenie (jeśli jeszcze ich nie ma) w organizacji konkretnych procedur, które będą realizować obowiązki prawne administratora. W grę wchodzą przede wszystkim procedury zabezpieczające prawa osób, których dane są przetwarzane, ale też określające relacje z kontrahentami (odbiorcami danych czy podmiotem przetwarzającym dane na zlecenie) i organem nadzorczym (np. uprzednie konsultacje).

Podstawowe procedury do wdrożenia w organizacji:

- aktywne informowanie podmiotów danych (zgodnie z art. 12, 13 i 14 RODO);
- udostępnianie i przenoszenie danych na żądanie podmiotów danych (zgodnie z art. 15 i 20);
- poprawianie i usuwanie danych na żądanie podmiotów danych;
- obsługa wycofania zgody na przetwarzanie danych, sprzeciwu lub żądania ograniczenia przetwarzania danych (zgodnie z art. 7, 16–19 i 21);
- umowy określające zasady przekazywania i odpowiedzialności za dane w relacjach z odbiorcami danych lub podmiotami je przetwarzającymi (zgodnie z art. 28);
- określenie i udokumentowanie wymaganych przez prawo gwarancji dla transferów danych poza UE, jeśli mają miejsce (zgodnie z rozdziałem V RODO);
- procedura działania w razie konieczności przeprowadzenia uprzednich konsultacji z organem nadzorczym (zgodnie z art. 36).

Konsultacje – nie zawsze obowiązek, ale zawsze dobra praktyka

W pełnym procesie oceny skutków przetwarzania danych osobowych RODO wymaga włączenia podmiotów danych[13] – czyli osób, których te skutki rzeczywiście będą dotyczyć – lub ich przedstawicieli (np. organizacji konsumenckich). Ten przepis posługuje się sformułowaniem „w stosownych przypadkach", a więc zostawia margines dla sytuacji, w których takie konsultacje mogą nie mieć sensu, okazać się niemożliwe czy generować dodatkowe ryzyko. Jednak w typowej relacji firma–klient skonfrontowanie poglądów administratora na ryzyko naruszenia praw osób, których dane dotyczą, z poglądami tych osób, co do zasady będzie wskazane.

Takich wymagań nie ma w przypadku podstawowej oceny ryzyka, której przebieg nie został skodyfikowany w RODO. Teoretycznie administrator może ją zatem przeprowadzić we własnej głowie. Osiągnie jednak lepsze rezultaty, jeśli już na tym etapie włączy niezależne głosy (np. ekspertów z dziedziny ochrony danych) i skonfrontuje swoje opinie z tym, jak ryzyko przetwarzania danych postrzegają osoby, których dane dotyczą.

13 Por. art. 35 (9) RODO.

KROK 4. OKREŚLENIE ŹRÓDEŁ I POZIOMU RYZYKA

Zweryfikowanie, czy dane są przetwarzane zgodnie z prawem, i wprowadzenie odpowiednich procedur w organizacji to baza, bez której administrator nie może działać. Zignorowanie tych etapów w ocenie skutków dla ochrony danych byłoby jednoznaczne z naruszeniem przepisów RODO. Jednak upewnienie się, że nie dochodzi do formalnego naruszenia prawa, to nie wszystko: w kolejnym kroku trzeba się zmierzyć z ryzykiem, że coś pójdzie „nie tak" (dane wyciekną; dostaną się w niepowołane ręce; będą - w praktyce - przetwarzane w innym celu niż zakładany etc.).

Szczegółowe wytyczne:
→ **Rozdział 4: Więcej praktycznych wskazówek, część: Modelowanie ryzyka: jak ustalić rodzaje, źródła i poziom zagrożeń?**

Sprawdź:

- Jakich zagrożeń/ negatywnych konsekwencji dla organizacji lub osób, których dane są przetwarzane, się obawiacie?
- Z czego te zagrożenia mogą wynikać (działania konkretnych osób, awarie sprzętu, zewnętrzne okoliczności etc.)?
- Jakie jest prawdopodobieństwo, że wystąpią? Od czego ono zależy?
- Jak duży (negatywny) wpływ i na kogo będą miały, jeśli się zrealizują?

KROK 5. ZIDENTYFIKOWANIE ŚRODKÓW ZARADCZYCH

Logicznym krokiem następującym po diagnozie zagrożeń jest określenie środków zaradczych: procedur, narzędzi i inwestycji, które pozwolą ograniczyć – a najlepiej wyeliminować – ryzyko naruszenia prawa i negatywnych konsekwencji dla podmiotów danych. W grę mogą wchodzić rozwiązania techniczne i organizacyjne (np. lepsze zabezpieczenia systemów informatycznych, zmiana oprogramowania czy sprzętu na mniej zawodny, regularne szkolenia dla osób pracujących z danymi osobowymi), ale też głębsze zmiany w sposobie zarządzania danymi czy relacjach z kontrahentami.

Sprawdź:

- Jakie słabe punkty zostały zidentyfikowane w procesie oceny ryzyka? Czy mają one związek z konkretnymi pracownikami lub polityką zatrudnienia? Sprzętem? Stylem i sposobem zarządzania? Kontrahentami? Konkurencją? Zewnętrznymi czynnikami, takimi jak cyberprzestępczość?
- Jakie środki zaradcze mogą pomóc je wyeliminować lub ograniczyć? Które z nich jesteście w stanie wprowadzić od zaraz, a które wymagają głębszych zmian w organizacji?
- Kto (w organizacji lub poza nią) jest w stanie zaprojektować i przeprowadzić potrzebne zmiany?

Co może zwiększyć bezpieczeństwo danych?

- pseudonimizacja i szyfrowanie danych osobowych;
- środki zapewniające poufność, integralność i odporność systemów;
- procedury szybkiego przywracania dostępności danych w razie incydentu fizycznego lub technicznego;
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych.

KROK 6. DOKUMENTACJA

Ocena skutków dla ochrony danych nie może odbywać się tylko w głowach osób zarządzających organizacją. Jak pokazują poprzednie kroki, na ten proces składa się wiele etapów i operacji (nie tylko myślowych). Sposób ich przeprowadzenia oraz wszystkie czynniki, jakie rzeczywiście zostały wzięte pod uwagę, trzeba udokumentować. Taka dokumentacja ma wartość nie tylko dla zewnętrznych podmiotów (np. organu nadzorczego, który zawsze może zapukać do drzwi organizacji i o to zapytać), ale też dla zarządzających i osób odpowiedzialnych za ochronę danych osobowych. W ten sposób powstaje swoisty punkt odniesienia, do którego będzie można wracać w przyszłości.

Sprawdź:

- Czy wszystkie etapy oceny skutków dla ochrony danych (od mapowania przepływów danych po określenie zagrożeń i środków zaradczych) zostawiły jakiś ślad w dokumentacji?
- Czy pełen opis tego procesu można zebrać w jednym miejscu (np. folderze)?
- Kto czuwa nad kompletnością, rzetelnością i aktualnością tej dokumentacji?
- Czy osoby odpowiedzialne za zarządzanie lub ochronę danych w organizacji będą w stanie łatwo do niej sięgnąć i ją zrozumieć?

KROK 7. MONITOROWANIE WDROŻENIA W ORGANIZACJI

O ile papier wszystko zniesie, o tyle organizacja jest żywym organizmem, który – szczególnie w momentach zmian – wymaga zarządzania. Wnioski z oceny skutków dla ochrony danych pozostaną martwe, jeśli nie znajdą się osoby nadzorujące ich wdrażanie. Ponieważ te procesy dotykają różnych sfer działania organizacji (od dokumentacji, przez procesy informatyczne i obsługę interesariuszy, po relacje z kontrahentami), wynikające z nich zadania również mogą trafiać do różnych osób i działów. Niemniej jednak jedna osoba w organizacji powinna spinać i monitorować ten proces. Osoba ta powinna mieć też umocowanie do tego, by w razie potrzeby powtórzyć ocenę skutków dla ochrony danych.

Więcej na ten temat:
→ **Rozdział 5: Jak wpisać odpowiedzialne zarządzanie danymi w życie organizacji?**

Sprawdź:

- Kto jest odpowiedzialny za wdrażanie wniosków wypływających z oceny skutków dla ochrony danych w organizacji?
- Czy taka osoba ma silne umocowanie ze strony zarządu? Czy dysponuje odpowiednim budżetem i wsparciem organizacyjnym?
- Czy osoby, które z nią współpracują w różnych miejscach organizacji, rozumieją szerszy kontekst i cel powierzanych im zadań (np. czemu służy dana inwestycja lub szkolenie)?
- Do kogo inne osoby z organizacji mogą się zgłaszać, jeśli mają wątpliwości związane z legalnością lub bezpieczeństwem przetwarzania danych osobowych?

W procesie oceny ryzyka lub skutków dla ochrony danych trzeba brać pod uwagę ewentualność, że zagrożenia związane z przetwarzaniem danych okażą się niemożliwe do usunięcia. Wówczas nie wystarczy zaprojektowanie środków zaradczych (np. dodatkowych zabezpieczeń). Jedyną sensowną rekomendacją w takiej sytuacji będzie zaprzestanie lub ograniczenie przetwarzania danych. Trudne lub niemożliwe do zarządzenia ryzyko może wystąpić, w szczególności, w związku z przetwarzaniem danych wrażliwych i wymagających szczególnej ochrony (np. ujawniających pochodzenie rasowe lub etniczne, orientację seksualną, poglądy polityczne).

FUNDACJA PANOPTYKON

ROZDZIAŁ 4

WIĘCEJ PRAKTYCZNYCH WSKAZÓWEK

Jak ustalić, czy przetwarzanie danych jest zgodne z prawem? Kontrola „stanu zdrowia”

Zasady przetwarzania danych określone w RODO to **podstawowa checklista każdego, kto przetwarza dane osobowe**. Nie są nowe, ponieważ w tym zakresie RODO nie wprowadza rewolucji, ale pozostają niezmiennie ważne. Obowiązkiem każdego administratora jest zapewnienie tego, by w organizacji nie było danych osobowych nieadekwatnych do celu, niepoprawnych, narażonych na ryzyko wycieku, przetwarzanych bez podstawy prawnej, w innym celu niż pierwotnie zakładany czy po prostu zbyt długo. Jak przełożyć te zasady na praktykę działania organizacji i sprawdzić, czy są przestrzegane?

I. Legalność

Dane osobowe muszą być przetwarzane zgodnie z prawem. Dla każdego rodzaju danych i każdego celu przetwarzania administrator danych musi zatem wykazać, że owo przetwarzanie spełnia **przynajmniej jeden warunek**:

- jest niezbędne do zawarcia lub wykonania umowy, której stroną jest osoba, której dane dotyczą;
- osoba, której dane dotyczą, wyraziła na to (jednoznaczną i dobrowolną) zgodę;
- jest niezbędne do wypełnienia obowiązku wynikającego z prawa UE lub państwa członkowskiego (które jest „niezbędnym i proporcjonalnym środkiem, zapewniającym realizację ważnych celów leżących w interesie publicznym");
- jest niezbędne do ochrony interesu mającego istotne znaczenie dla życia osoby, której dane dotyczą, lub innej osoby fizycznej;
- jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej;
- ma podstawę w prawnie uzasadnionym interesie administratora lub strony trzeciej, chyba że nad tym interesem przeważają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą (jest to oceniane w kontekście rozsądnych oczekiwań osób, których dane dotyczą, i ich powiązań z administratorem).

Sprawdź:

- ☐ Czy jako organizacja jesteście w stanie wskazać i obronić podstawę prawną dla każdego rodzaju danych i każdego celu, w jakim dane są przetwarzane?
- ☐ Czy te podstawy prawne zostały zebrane w jednym miejscu (choćby wewnętrznym dokumencie)?
- ☐ Kto i jak często weryfikuje, czy w organizacji nie pojawiają się dane przetwarzane bez podstawy prawnej (np. folder z niestandardową korespondencją, pozostałości po zamkniętej już rekrutacji)?
- ☐ Jeśli jedną z podstaw przetwarzania danych jest zgoda, w jaki sposób jest ona zbierana, jak jest dokumentowana i kto kontroluje, czy nie została odwołana? Jaka procedura jest uruchamiana w przypadku odwołania zgody?
- ☐ Jeśli jedną z podstaw przetwarzania danych jest uzasadniony interes administratora, w jaki sposób został określony i zakomunikowany na zewnątrz? Kto i w jaki sposób przeprowadził test ważenia interesów i praw, którego w takiej sytuacji wymaga RODO? Czy ten test został w jakiś sposób udokumentowany?

2. Ograniczenie celem

Dane osobowe mogą być przetwarzane tylko w konkretnym, wyraźnie określonym i zgodnym z prawem celu. Administrator musi ten cel określić, zanim pozyska dane, i nie może go jednostronnie modyfikować. Raz pozyskanych danych nie można przetwarzać w celach niezgodnych z pierwotnie określonym (np. danych zebranych w celu realizacji umowy wykorzystać do marketingu podmiotów trzecich).

Sprawdź:

- ☐ Czy jako organizacja potraficie wskazać cel każdego procesu w organizacji, który angażuje dane osobowe?
- ☐ Czy te cele spinają się w spójną i kompletną strategię dla całej organizacji? Czy zostały lub mogą zostać łatwo zebrane i sklasyfikowane w jednym miejscu?
- ☐ Czy zdarzają się sytuacje, w których te same dane służą różnym celom? Jeśli tak, czy wszystkie te cele zostały zakomunikowane osobom, których dane dotyczą?
- ☐ Czy w miarę rozwoju organizacji mogą się pojawiać nowe cele wykorzystywania danych? Kto i w jaki sposób będzie oceniać ich kompatybilność z pierwotnie określonymi celami?[13] Z jakiej podstawy prawnej organizacja zamierza skorzystać w przypadku braku kompatybilności (czy np. będzie pozyskiwana zgoda od osób, których dane dotyczą)?

3. Adekwatność, niezbędność i minimalizacja

Dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są przetwarzane. To kryterium przekłada się na rodzaj i zakres danych. Nie można zatem zbierać danych, które nie mają związku z celem przetwarzania (np. dane na temat zdrowia w kontekście usług finansowych), są bezużyteczne dla jego realizacji (np. nierzetelne czy nieaktualne) albo nadmiarowe (np. dane bardzo szczegółowe). Mówiąc najprościej: wolno zbierać tylko to, co rzeczywiście niezbędne.

Sprawdź:

- ☐ W jaki sposób dane przetwarzane w ramach danego procesu/projektu łączą się z jego celem?
- ☐ Czy ten sam cel można osiągnąć, zbierając mniej danych lub dane mniej szczegółowe?
- ☐ Czy wszystkie przetwarzane dane mają wpływ na ostateczny wynik procesu/projektu? Jeśli nie, dlaczego nadal krążą w organizacji? W jaki sposób i przez kogo ich przydatność jest weryfikowana?

14 Por. art. 6 ust. 4 RODO.

4. Prawidłowość

Przetwarzane dane osobowe powinny być prawidłowe i w razie potrzeby uaktualniane. Administrator powinien niezwłocznie usunąć albo sprostować dane, które okazały się nieprawidłowe w świetle celów ich przetwarzania. W praktyce ta zasada oznacza, że nie warto zbierać danych, które szybko się starzeją lub pochodzą z niepewnych źródeł, ponieważ mogą się okazać dla organizacji większym ciężarem niż korzyścią.

Sprawdź:

- ☐ Czy wszystkie przetwarzane w organizacji dane są dobrej jakości? Czy macie pewność co do wiarygodności źródeł, z których są pozyskiwane? Jeśli nie, w jaki sposób weryfikujecie prawidłowość danych?
- ☐ Jak często i przez kogo jest weryfikowana aktualność danych?
- ☐ Czy wykorzystywane w organizacji oprogramowanie pozwala poprawiać dane zawsze, kiedy jest to potrzebne?

5. Maksymalny czas przetwarzania

Dane osobowe można przetwarzać nie dłużej, niż to niezbędne do celów, w których te dane są przetwarzane. W szczególności chodzi tu o dane umożliwiające (np. w przypadku wycieku) identyfikację osoby, której dotyczą. Na przykład granicą przechowywania archiwalnych danych o transakcjach z klientami powinien być moment przedawnienia roszczeń lub wygaśnięcia obowiązków prawnych (wynikających z prawa skarbowego, bankowego itp.). Granicą dla przetwarzania aktualnych danych o zakupach klientów w celach marketingowych (uzasadniony interes administratora) jest moment, w którym te dane tracą aktualność lub cel marketingowy zostaje zrealizowany.

Sprawdź:

- ☐ Kto i w jaki sposób weryfikuje, czy dane w organizacji nie są przetwarzane dłużej, niż to niezbędne do realizacji założonego celu?
- ☐ Czy terminy usuwania danych w systemach informatycznych są z góry ustalane? Jeśli tak, od czego zależy długość tych terminów? Jeśli nie, jak często przydatność danych jest weryfikowana?
- ☐ Czy oprogramowanie, z którego korzysta organizacja, pozwala na usunięcie danych wtedy, kiedy przypada wyznaczony termin lub dane okazują się nieprzydatne?

6. Poufność i integralność

Dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym ich wykorzystaniem. W praktyce ta zasada oznacza nie tylko konieczność zabezpieczenia systemów informatycznych (przynajmniej przed typowymi atakami), ale też wprowadzenia procedur, które ograniczą ryzyko związane z tzw. czynnikiem ludzkim.

Sprawdź:

- ☐ W jaki sposób systemy informatyczne działające w organizacji zostały zabezpieczone przed nieuprawnionym dostępem (hasła, tokeny etc.)?
- ☐ Czy każdy nowo wprowadzany system przechodzi jakiś rodzaj sprawdzenia pod kątem bezpieczeństwa (testy wewnętrzne, konsultacje z zewnętrznymi ekspertami)?
- ☐ Czy kiedykolwiek doszło w organizacji do utraty danych (wycieku, zgubienia, nieautoryzowanego dostępu)? Jeśli tak, jakie wyciągnęliście z tego wnioski?
- ☐ Jakie szkolenia i instrukcje otrzymują osoby pracujące z danymi w organizacji? Czy są przygotowane na typowe zagrożenia? Jak często ich wiedza i umiejętności w tym zakresie są weryfikowane?

Modelowanie ryzyka: jak ustalić rodzaje, źródła i poziom zagrożeń?

Istotą procesu oceny ryzyka nie jest mnożenie formalności ani produkowanie dokumentacji, która będzie później zalegać w organizacji. Ma on pomóc administratorowi: (i) **określić możliwe zagrożenia** dla praw i wolności osób, których dane przetwarza, oraz (ii) **odpowiedzieć na nie poprzez wdrożenie konkretnych środków zaradczych**.

W praktyce oznacza to konieczność zidentyfikowania rodzajów, źródeł i realnego poziomu tych zagrożeń. Przeprowadzając taką analizę, administrator nie musi wynajdywać koła na nowo. Może skorzystać z już rozwiniętych i sprawdzonych w praktyce metod modelowania ryzyka[14].

Oto standardowy przebieg takiego procesu:

14 Metodyka oceny ryzyka opracowana na podstawie zaleceń Commission Nationale de l'Informatique et des Libertés (CNIL), Methodology for Privacy Risk Management and PIA Tools.

I. Możliwe scenariusze: co może pójść „nie tak”?

Standardowo pierwszym krokiem w procesie oceny ryzyka jest wyobrażenie sobie możliwych niepożądanych konsekwencji przetwarzania danych. Co konkretnie może pójść „nie tak”? Czego się obawiamy?

Przykłady zagrożeń, które warto rozważyć:

- proces, który jest obowiązkowy z punktu widzenia organizacji, przestaje działać (np. osoby, których dane dotyczą, nie są w stanie skutecznie przenieść swoich danych, ponieważ przestał działać zaprojektowany w tym celu interfejs, albo tracą dostęp do wymaganych prawem informacji, ponieważ ze strony zniknęła polityka prywatności etc.);
- proces biznesowy nie działa tak, jak został zaprojektowany, przez co dochodzi do zmiany celu lub zakresu przetwarzania danych (np. dane o lokalizacji klientów, zbierane wyłącznie w celach serwisowych, zaczynają być wykorzystywane w celach reklamowych; zwierzchnicy, niezgodnie z prawem, wykorzystują dane o zwyczajach swoich pracowników, szukając pretekstów do ich zwolnienia);
- osoby niepowołane (wewnątrz lub spoza organizacji) dostają dostęp do danych osobowych (np. dane identyfikujące klientów, powiedzmy banku, są przechwytywane i wykorzystywane do nadużyć finansowych);
- dochodzi do niechcianej i nieautoryzowanej modyfikacji przetwarzanych danych (np. danych medycznych, co powoduje błędy w terapii, a nawet zagrożenie dla zdrowia lub życia pacjentów);
- dane zostają utracone (np. wnioski o pomoc społeczną znikają z systemu, co powoduje, że osoby starające się o takie wsparcie muszą ponownie przechodzić przez formalności i dłużej czekać).

2. Jak może do tego dojść?

Kiedy już wiemy, co nam zagraża, warto zidentyfikować i opisać źródła tych zagrożeń oraz te aktywa w organizacji, które rzeczywiście są zagrożone. Czy źródła znajdują się wewnątrz czy na zewnątrz organizacji? Czy są to osoby czy zjawiska niespersonalizowane? Czy mamy na nie jakiś wpływ? Czy zagrażają oprogramowaniu, sprzętowi, pracownikom, a może kluczowym procesom zarządczym? Wreszcie: warto przeanalizować, w jaki konkretnie sposób może dojść do tego, że dane zagrożenie się zrealizuje.

Możliwe źródła zagrożeń:

- osoby wewnątrz organizacji: użytkownicy systemów informatycznych, administratorzy, deweloperzy, zarządzający etc.;
- osoby spoza organizacji: klienci, odbiorcy usług, dostawcy, konkurenci, ciekawscy, osoby o przestępczych zamiarach, organy państwa, osoby postronne etc.;
- zewnętrzne, niezależne od nas okoliczności: wirus komputerowy, awaria (np. serwerowni), klęski żywiołowe, epidemie etc.

Aktywa, jakie mogą zostać dotknięte zagrożeniem:

- sprzęt (komputery, węzły komunikacyjne, nośniki USB, twarde dyski);
- oprogramowanie (systemy operacyjne, bazy danych, aplikacje do komunikacji wewnętrznej i zewnętrznej; aplikacje biznesowe, np. służące do zarządzania projektami);
- sieci telekomunikacyjne (kable, światłowody, routery);
- ludzie (użytkownicy systemów informatycznych, administratorzy, zarządzający);
- nośniki papierowe (wydruki, kopie dokumentów, tradycyjne foldery);
- kanały dystrybucji mediów papierowych (poczta wewnętrzna, systemy obiegu dokumentów).

W jaki sposób zagrożenie może się zrealizować?

- zmiana funkcji (tzw. *function creep*) – aktywa zostają wykorzystane w inny sposób, niż było to zamierzone, bez ich uszkodzenia czy modyfikacji (np. pracownik wykorzystuje bazę adresów, która miała służyć wyłącznie do obsługi zapytań klientów, w celach marketingowych podmiotów trzecich);
- szpiegostwo, czyli monitorowanie aktywów bez ich uszkodzenia (np. atakujący instaluje trojana na komputerze administratora danych i zyskuje zdalny podgląd operacji wykonywanych na tym urządzeniu);
- zniszczenie aktywów w wyniku katastrofy lub awarii (np. zalanie serwerów, awaria dysku twardego);
- utrata aktywów w wyniku kradzieży lub sprzedaży (np. konkurent kradnie nośnik z danymi klientów podczas wizyty w biurze).

3. Jakie jest prawdopodobieństwo, że zagrożenie się zrealizuje?

Świadomość zagrożeń – ich źródeł i sposobów, w jakie mogą się zrealizować – to jedno. Ustalenie, na ile są realne, to zupełnie inna sprawa. Zanim podejmiemy decyzję o zainwestowaniu (czasu, pieniędzy czy innych zasobów) w środki zaradcze, warto oszacować poziom każdego ze zidentyfikowanych zagrożeń. W tym ćwiczeniu chodzi przede wszystkim o stwierdzenie, czy wśród możliwych zagrożeń występują bardziej prawdopodobne lub takie, które w przypadku zrealizowania się pociągną za sobą szczególnie dotkliwe konsekwencje. Wówczas w pierwszej kolejności warto skupić się na eliminowaniu ich właśnie, a w dalszej – zająć się mniej prawdopodobnymi i mniej dotkliwymi.

Pytania kontrolne:

- **Jak łatwo będzie można połączyć dane z konkretnymi osobami (w przypadku zrealizowania się zagrożenia)?** Stopień identyfikowalności można oznaczyć na czterostopniowej skali: od pomijalnego (identyfikacja niemal niemożliwa), poprzez ograniczony i znaczący, po maksymalny (identyfikacja bardzo łatwa). To, z jakim stopniem identyfikowalności mamy do czynienia, naturalnie zależy od zakresu i rodzaju przetwarzanych danych osobowych. O ile pojedyncza i często występująca w populacji cecha (np. imię) będzie trudna do połączenia z konkretną osobą, o tyle szeroki zestaw cech demograficznych, tworzący unikatową kompozycję, już nie.
- **Jak dotkliwe w skutkach (dla osób, których dane są przetwarzane) może być zrealizowanie się zagrożenia?** Dotkliwość skutków również można oznaczyć w czterostopniowej skali: od pomijalnych (takich jak chwilowa irytacja czy konieczność ponownego wprowadzenia danych do systemu), poprzez ograniczone (np. dodatkowe koszty, przerwa w dostępie do usług, krótkotrwały stres) i znaczące (np. pogorszenie sytuacji majątkowej, utrata pracy, trafienie na czarną listę), aż po maksymalne (np. trwała niezdolność do pracy, głębokie zadłużenie).
- **Jak podatne na zidentyfikowane zagrożenia są wasze aktywa?** Aby ocenić poziom podatności aktywów, warto nazwać i przeanalizować konkretne cechy, które na nią wpływają (np. podłączenie do sieci czy częstość aktualizacji oprogramowania w przypadku sprzętu; poziom wyszkolenia i motywacji w przypadku pracowników).
- **Jakimi zasobami dysponują zidentyfikowane źródła zagrożeń (osoby lub organizacje)?** A więc: jak bardzo są zdeterminowane, jakimi umiejętnościami dysponują, ile mają czasu i pieniędzy, czy są blisko zagrożonych aktywów, czy mogą czuć się bezkarne? Taka ocena wymaga przede wszystkim dobrego rozpoznania źródeł zagrożeń, czasem tzw. białego wywiadu.

Przykład

JAKA KONKRETNIE NIEPOŻĄDANA SYTUACJA MOŻE SIĘ WYDARZYĆ?	Osoby niepowołane spoza organizacji dostają dostęp do danych osobowych klientów i wykorzystują je do nadużyć finansowych.
JAKIE JEST ŹRÓDŁO TEGO ZAGROŻENIA?	Osoby wewnątrz organizacji (np. pracownicy zarządzający danymi) przechowują nośniki papierowe z danymi w taki sposób, że mają do nich dostęp osoby zewnętrzne.
JAKIE AKTYWA MOGĄ ZOSTAĆ DOTKNIĘTE TYM ZAGROŻENIEM?	Nośniki papierowe z danymi klientów (wydruki).
W JAKI SPOSÓB ZAGROŻENIE MOŻE SIĘ ZREALIZOWAĆ (JAK MOŻE DO NIEGO DOJŚĆ)?	Ktoś zostawił wydruki w kserokopiarce, która stoi na korytarzu, do którego dostęp mają osoby postronne.

FUNDACJA PANOPTYKON

ROZDZIAŁ 5

JAK WPISAĆ ODPOWIEDZIALNE ZARZĄDZANIE DANYMI W ŻYCIE ORGANIZACJI?

Pełne wdrożenie RODO może być wyzwaniem dla organizacji przyzwyczajonych do formalistycznego podejścia do ochrony danych osobowych. Rejestry zbiorów danych, sztywne formularze, w które administratorzy wpisywali podstawy przetwarzania danych (skrupulatnie, ale nie zawsze zgodnie ze stanem faktycznym) odchodzą do lamusa. W ich miejsce pojawiają się **elastyczne procesy, takie jak ocena ryzyka i skutków dla ochrony danych**. RODO nie wymaga od administratorów wypełnienia określonych rubryk w tabeli, nie podpowiada też gotowych procedur, które trzeba wdrożyć w każdej organizacji. Wymaga za to realnego, strategicznego zmierzenia się z tym tematem.

To wyzwanie, ale też szansa dla zarządzających. Skoro i tak zgodnie z RODO organizacja powinna przejść przez wieloaspektowy, złożony proces oceny ryzyka, dlaczego nie pójść dalej i nie stworzyć pełnej strategii zarządzania danymi? Zmapowanie przepływów danych w organizacji, zweryfikowanie, czy wszystkie te dane są niezbędne, opisanie możliwych zagrożeń i wprowadzenie środków zaradczych to już wielki krok w tym kierunku.

Zgodnie z wytycznymi organów ochrony danych ocena ryzyka i skutków dla ochrony danych to żywe procesy, które powinny być cyklicznie powtarzane. Warto tę okazję wykorzystać, by nie tylko spełnić wymogi prawne i zabezpieczyć się przed ryzykiem – bezpośrednio dotyczącym podmiotów danych, pośrednio całej organizacji, jej pracowników, kontrahentów i inwestorów – ale też wprowadzić takie procedury, które rzeczywiście usprawnią zarządzanie danymi. Przetwarzanie zbyt dużych ilości danych, przechowywanie ich zbyt długo, słabe zabezpieczenia czy brak odpowiednich szkoleń dla pracowników to nie tylko źródła ryzyka prawnego, ale też realne problemy, które warto rozwiązać.

Jak przejść od punktowej oceny ryzyka lub skutków dla ochrony danych do pełnej strategii zarządzania danymi w organizacji? Jak uciec od reagowania na konkretne problemy („gaszenia pożarów") w stronę wyprzedzającego myślenia strategicznego? Nie ma na to gotowego przepisu. To zadanie, z którym powinni się zmierzyć sami zarządzający, ponieważ to oni najlepiej znają potrzeby swojej organizacji.

Oto kilka praktycznych wskazówek, jak uruchomić taki proces:

Strategia zarządzania danymi w organizacji – krok po kroku

I. Postawcie właściwe pytania

Projektowanie procesów przetwarzania danych w organizacji, jak każdy projekt, zaczyna się od postawienia właściwych pytań:

- Czemu te dane mają służyć?
- Co chcemy dzięki nim osiągnąć?
- Czy możemy to zrobić niższym kosztem (dla podmiotów danych, ale też dla organizacji)?

W udzieleniu na nie odpowiedzi pomoże rzetelnie przeprowadzona **ocena skutków dla ochrony danych** (por. punkt 7 kroków do pełnej oceny skutków dla ochrony danych). Postawienie tych pytań już na etapie planowania działań i projektowania nowych rozwiązań to szansa na uzgodnienie kultury organizacji i jej wizji z wymaganiami, jakie stawia prawo.

Na tym etapie zarządzający muszą też zmapować wszystkie przepływy danych w organizacji:

- Skąd i w jakim celu są pozyskiwane? Czy i komu są przekazywane dalej?
- Przez kogo i na jakim sprzęcie są przetwarzane?
- Czy trafiają do chmury?

W prześledzeniu drogi danych osobowych w organizacji mogą pomóc dostępne na rynku narzędzia analityczne (te same programy, które integrują i analizują dane, by stworzyć profil klienta albo lepiej zarządzać relacjami biznesowymi, np. system CRM).

2. Potraktujcie ochronę danych jak (normalny) proces

Nawet najlepiej zaprojektowane zasady ochrony danych będą martwe, jeśli nie zostaną potraktowane jak normalny proces i tym samym **wpięte w życie organizacji**. Najlepiej to widać na przykładzie bezpieczeństwa danych, które musi się przełożyć na konkretne standardy w zakupach i utrzymaniu sprzętu, szkolenia dla pracowników i zadania w dziale IT (lub zewnętrznych kontrahentów).
Ta sama logika obowiązuje w innych aspektach ochrony danych osobowych: pilnowaniu podstaw prawnych, przestrzeganiu fundamentalnych zasad (jak minimalizacja danych czy ograniczenie celem), realizowaniu praw podmiotów danych. W każdej z tych sfer teoria musi się przełożyć na praktykę poprzez konkretny proces. Projektowanie i wdrażanie takich rozwiązań zajmuje czas, a więc administratorzy, którzy chcą zdążyć przed majem 2018 r., muszą się pospieszyć.

3. Ćwiczcie i rozmawiajcie, rozmawiajcie i ćwiczcie

Każda głębsza zmiana w organizacji, każdy nowy proces wymaga jasnego **zakomunikowania i przećwiczenia**. Nie raz, ale – przynajmniej w fazie oswajania – wielokrotnie. Pracownicy, użytkownicy systemów informatycznych, kontrahenci, a nawet klienci powinni rozumieć, z jakiej filozofii i celu wynika dany proces i do czego zmierza. Czy chodzi o to, żeby dane były bezpieczne?A może o to, żeby było ich jak najmniej lub żeby były możliwie najlepszej jakości? Jakiej zmiany w moim zachowaniu to wymaga? Co się stanie, jeśli nie zastosuję się do tych reguł? Czy ja również na tym stracę? Zrozumienie celów i konsekwencji wspiera dobrą realizację.

4. Kontrolujcie, wdrażajcie środki techniczne i automatyzujcie

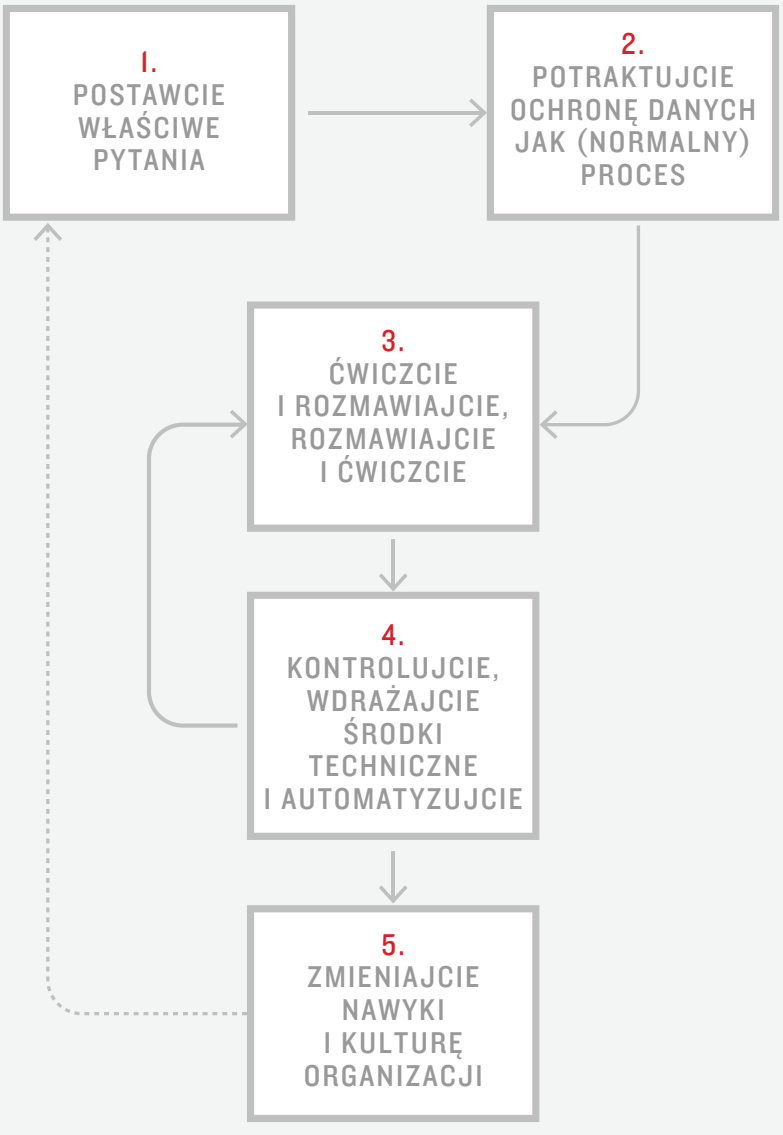
Nawet najlepiej zakomunikowany i przećwiczony proces może pójść „nie tak". Ostatecznie **wszystko jest w rękach ludzi**. Administrator, który chce się ustrzec przed negatywnymi konsekwencjami (w tym ryzykiem wysokich kar), musi być na taką ewentualność przygotowany. W tym kontekście warto:

- wdrożyć odpowiednie procesy kontrolne (kto, jak często i w jaki sposób weryfikuje, czy założona strategia zarządzania danymi jest rzeczywiście realizowana?);
- tam, gdzie to możliwe, wbudować w systemy informatyczne zabezpieczenia i mechanizmy chroniące dane osobowe (np. automatyczne flagowanie danych, które spełniają kryteria danych osobowych, a następnie ich szyfrowanie, bez konieczności podejmowania decyzji przez człowieka; automatyczne ostrzeżenia i – widoczne dla innych pracowników – flagi w przypadku, gdy dane są przetwarzane dłużej, niż było to zakładane);
- wprowadzić twardy wymóg pseudonimizacji danych osobowych w każdej sytuacji, w której bezpośrednia identyfikacja (użytkownika, pracownika, konsumenta) nie jest konieczna;
- wprowadzić techniczne ograniczenia w dostępie do (konkretnych baz) danych osobowych dla osób (również zarządzających), które nie są uprawnione do ich przetwarzania.

5. Zmieniajcie nawyki i kulturę organizacji

Pełne wdrożenie każdej strategii – także w sferze zarządzania danymi – przejawia się w tym, że staje się ona **elementem kultury organizacji**. Zarządzający, pracownicy i kontrahenci już nie zmagają się z nowymi procesami czy zasadami, ale traktują je jak coś oczywistego. W organizacji zaczynają spontanicznie pojawiać się pytania w rodzaju: „czy na pewno powinniśmy to robić z danymi naszych klientów?" albo „jak długo już mamy te dane i czy na pewno jeszcze możemy je przetwarzać?".

To najlepsza gwarancja tego, że cele strategii zarządzania danymi rzeczywiście zostaną zrealizowane. W kolejnych iteracjach pracy nad strategią ta zmiana kultury, praktyk i oczekiwań przekłada się na większą spójność celów, metod i zakładanych rezultatów. To głęboka zmiana, która wymaga czasu. Ale nigdy nie jest zbyt późno, żeby zacząć.



Źródła i polecane materiały

Wytyczne organów ochrony danych

Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679* (2017).

Commission Nationale de l'Informatique et des Libertés (CNIL), *Methodology for Privacy Risk Management and PIA Tools* (2012).

Information Commissioner's Office, *Conducting Privacy Impact Assessment – code of practice* (2014).

Standardy techniczne

International Organization for Standardization, *ISO 22307:2008 Financial services – Privacy impact assessment* (standard zrewidowany w 2012).

IEEE Standards Association, *P7003 – Algorithmic Bias Considerations* (projekt w toku).

Opracowania akademickie i wyniki projektów badawczych

Felix Bieker, Michael Friedewald, Marit Hansen, Hannah Obersteller, Martin Rost, *A Process for Data Protection Impact Assessment under the European General Data Protection Regulation* (2016).

Niels van Dijk, Raphaël Gellert, Kjetil Rommetveit, *A risk to a right? Beyond data protection risk assessments* (2016).

Privacy Impact Assessment Framework: Paul De Hert, Dariusz Kloza, David Wright, *A Privacy Impact Assessment Framework for data protection and privacy rights* (2011)

Privacy Impact Assessment Framework: *Recommendations for the Privacy Impact Assessment framework for the European Union* (2012).

O autorce

Katarzyna Szymielewicz

Prawniczka specjalizująca się problematyce praw człowieka i nowych technologii. Współzałożycielka i prezeska Fundacji Panoptykon. Wiceprzewodnicząca European Digital Rights. Od 2005 do 2009 r. związana z międzynarodową kancelarią prawną Clifford Chance. Od 2011 do 2016 r. członkini rady społecznej przy Ministrze ds. Cyfryzacji. Od 2015 r. stypendystka Ashoki – międzynarodowej sieci przedsiębiorców społecznych. W 2014 r. znalazła się na liście NewEurope 100, w 2015 r. trafiła do Top Ten kobiet polskiego sektora teleinformatycznego (badanie przeprowadzone przez Znane Ekspertki), od kilku lat stale gości w rankingu najbardziej wpływowych prawników Dziennika Gazety Prawnej.