PORADNIK

Unijne Rozporządzenie o Ochronie Danych Osobowych

Co powinieneś wiedzieć?

ODO 24

Ochrona Danych Osobowych

BEZPIECZEŃSTWO INFORMACJI

Fellowes

WORK BETTER™

SPIS TREŚCI

ODO 24
Ochrona Danych Osobowych
BEZPIECZEŃSTWO INFORMACJI

Partnerem merytorycznym niniejszego poradnika jest firma ODO 24 Sp. z o.o. oferująca kompleksowe rozwiązania w zakresie ochrony danych osobowych i bezpieczeństwa informacji. Dzięki doświadczonemu zespołowi ekspertów z zakresu m.in. prawa, informatyki, zarządzania kryzysowego oraz ciągłości działania dostarcza organizacjom praktyczne rozwiązania, pozwalające skutecznie zabezpieczyć posiadane zasoby informacyjne.

WSTĘP

Wszyscy przedsiębiorcy oraz instytucje, które przetwarzają dane osobowe muszą przygotować się na rewolucyjne zmiany. 25 maja 2016 r. weszły w życie, a od 2018 r. zaczną obowiązywać przepisy unijnego rozporządzenia o ochronie danych osobowych.[1] Pełna nazwa tego aktu to: Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), które dalej określane jest w skrócie jako Rozporządzenie, w Polsce potocznie określane mianem RODO, a w Europie rozpoznawane jako GDPR.

RODO

to unijne ogólne rozporządzenie o ochronie danych osobowych

Dwa lata między wejściem przepisów w życie, a rozpoczęciem ich obowiązywania ma służyć głównie dostosowaniu przepisów krajowych, i umożliwić administratorom danych przygotowanie się, co też zostało wybitnie podkreślone w motywie 171 preambuły: przetwarzanie, które w dniu rozpoczęcia stosowania niniejszego rozporządzenia już się toczy, powinno w terminie dwóch lat od wejścia niniejszego rozporządzenia w życie zostać dostosowane do jego przepisów.

Do tego czasu należy stosować obowiązujące przepisy o ochronie danych osobowych, w szczególności przepisy ustawy o ochronie danych osobowych z 1997 r. (z późn. zm.) oraz akty wykonawcze do niej.

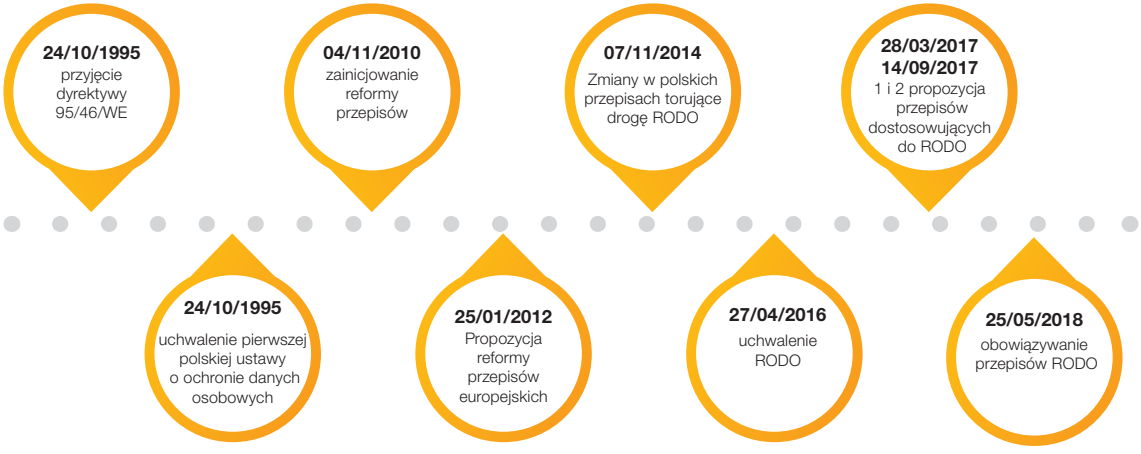
Proces dostosowywania jest długotrwały, przygotowania należy zacząć jak najszybciej, jednak do tego niezbędna jest wiedza o tym, jak się przygotować, dlatego oddajemy w Państwa ręce przewodnik po wybranych kluczowych założeniach nowego prawa.

[1] http://ec.europa.eu/health/data_collection/docs/com_2010_0609_pl.pdf

[2] Skrót RODO pochodzi od „ogólne rozporządzenie o ochronie danych osobowych", zaś GDPR pochodzi od „general data protection regulation". W zasadzie skrót powinien brzmieć ORODO, gdyż mowa o „ogólnym" rozporządzeniu, ale czteroliterowy skrót łatwiej przyjął się na polskim rynku.

NOWE PRZEPISY O OCHRONIE DANYCH OSOBOWYCH - RODO

Reforma przepisów nie powinna być dla nikogo zaskoczeniem, bo przygotowywano się do niej już od dość dawna. Zaledwie po pięciu latach stosowania Dyrektywy 95/46/WE, w 2010 roku w Europie dostrzeżono potrzebę reformy przepisów o ochronie danych osobowych. Dwa lata później dostępne były już pierwsze projekty, które dawały pojęcie o tym, co może nas czekać… Kolejne cztery lata poświęcone były głównie negocjacjom z krajami członkowskimi tak, aby przyjęte przepisy były w miarę uniwersalne w całej Europie i dające się stosować w rozmaitych systemach prawnych. I ostatecznie 27 kwietnia 2016 r. uchwalono Rozporządzenie, przewidując jednocześnie że będzie stosowane po dwóch latach od przyjęcia.



Kalendarium zmian w przepisach

- **24 października 1995 r.** - przyjęcie dyrektywy 95/46/WE
- **28 sierpnia 1997 r.** - uchwalenie pierwszy raz polskiej ustawy o ochronie danych osobowych
- **4 listopada 2010 r.** - zainicjowanie kompleksowego podejścia do ochrony danych
- **25 stycznia 2012 r.** - propozycja reformy przepisów europejskich
- **7 listopada 2014 r.** - zmiany w polskiej ustawie, „torujące" drogę przyszłemu rozporządzeniu
- **1 stycznia 2015 r.** - rozpoczęcie obowiązywania zmian wprowadzonych 7/11/2014r.
- **27 kwietnia 2016 r.** - uchwalenie RODO
- **28 marca 2017 r.** - pierwsza propozycja polskich przepisów dostosowujących do wdrożenia RODO
- **14 września 2017 r. -** konsultacje społeczne
- **25 maja 2018 r.** - obowiązywanie RODO

Aby zrozumieć, jaki wpływ na obywateli mają zapisy Rozporządzenia, warto zapoznać się z konstrukcją przepisów prawa Unii Europejskiej.

Składają się na nie: rozporządzenia, dyrektywy, decyzje, opinie, zalecenia.

Dyrektywy europejskie mają moc wiążącą wyłącznie co do rezultatu, ich rolą jest harmonizacja prawa. Oznacza to, że państwa członkowskie mają obowiązek wdrożyć opisane w dyrektywie przepisy, ale posiadają przy tym swobodę sposobu ich implementacji. Przykładowo, Dyrektywa 95/46/WE weszła do polskiego porządku prawnego przez uchwalenie w 1997 r. ustawy o ochronie danych osobowych.

Rozporządzenia europejskie są bardzo podobne do polskich ustaw, mają charakter wiążący i — co najważniejsze — obowiązują bezpośrednio. Oznacza to, że do rozporządzenia UE w Polsce należy stosować się tak samo, jakby to była polska ustawa.

Hasłem przyświecającym idei stworzenia jednego unijnego rozporządzenia w zakresie ochrony danych osobowych była zasada: jeden kontynent – jedno prawo. Jednak wcale to nie jest takie łatwe, jakby mogło się wydawać. Aby Rozporządzenie można było stosować, władze muszą uchylić wszystkie przepisy niezgodne z treścią Rozporządzenia oraz przyjąć przepisy wdrażające Rozporządzenie. Przykładowo art. 33 Rozporządzenia określa, że przypadki naruszenia bezpieczeństwa należy zgłaszać organowi nadzorczemu – zatem aby móc ten zapis stosować w kraju należy przyjąć przepisy powołujące taki organ oraz opisujące w jaki sposób zgłaszać takie przypadki. Oprócz tego Rozporządzenie państwom członkowskim pozostawiło pewną swobodę w stosowaniu rozporządzenia – przykładowo art. 7 określa, że „państwa członkowskie mogą przewidzieć w swoim prawie niższą granicę wiekową, która musi wynosić co najmniej 13 lat".

Do rozporządzenia europejskiego należy stosować się tak, jakby to była polska ustawa

We wrześniu 2017 r. pojawiły się projekty przepisów zmieniających aż 133 akty prawa, aby wdrożyć Rozporządzenie. Pojawił się także projekt ustawy o ochronie danych osobowych,[3] w uzasadnieniach do którego podkreślono, że *„przepisy nowej ustawy o ochronie danych osobowych, mają zapewnić skuteczne stosowanie w polskim porządku prawnym rozporządzenia".*

Rozporządzenie będzie spójnym narzędziem do stosowania we wszystkich państwach członkowskich. We wszystkich państwach członkowskich trzeba będzie stosować się do tych samych zasad ochrony danych osobowych. Ułatwi to prowadzenie biznesu w Europie, co należy uznać za dobry kierunek zmian.

Rozporządzenie napisano też językiem znacznie bardziej przystępnym niż ten, który zwykle stosuje się do tworzenia polskiego prawa. Polskie tłumaczenie dokumentu dobrze się czyta. Właściwie znaczenie zrozumiałego języka podkreśla samo Rozporządzenie przykładowo nakazując, aby informacje osobom były udzielane *„w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem"* (art. 12).

Bardzo korzystną zmianą jaką wprowadza Rozporządzenie jest prawo szyte na miarę. Do tej pory każdy, kto przetwarzał dane, musiał stosować te same zabezpieczenia, niezależnie od skali przetwarzania, rozmiaru działalności, użytej technologii czy ilości pracowników. Nowe przepisy stosowanie zabezpieczeń uzależniają od poziomu ryzyka.

[3] https://www.gov.pl/cyfryzacja/konsultacje-spoleczne-projektu-przepisow-wdrazajacych-ogolne-rozporzadzenie-o-ochronie-danych-rodo-

PODSTAWOWE ZAGADNIENIA

Bez znajomości podstawowych zagadnień może być niezmiernie trudno rozumieć nowe przepisy, dlatego warto poświęcić im odrobinę miejsca.

Dane osobowe

RODO nie zmienia definicji danych osobowych, pozostaje ona taka sama, jak była w polskiej ustawie o ochronie danych osobowych. Za dane osobowe uważa się więc informacje o zidentyfkowanej lub możliwej do zidentyfkowania osobie fzycznej. Kodeks cywilny stanowi, że osobą fizyczną jest każdy człowiek od momentu narodzin aż do śmierci. W efekcie przepisy o ochronie danych osobowych nie dotyczą osób nieżyjących.

Osobą zidentyfikowaną jest osoba znana z imienia i nazwiska, a możliwą do zidentyfikowania np. Jan Nowak, zamieszkały na ul. Rozporządzenia Europejskiego 17 m. 4 w Krakowie. Informacje takie jak *„obecnie urzędujący Prezydent Polski”*, *„Prezes Zarządu Fellowes Polska S.A.”* bądź numer PESEL umożliwiają identyfikację osoby, a więc stanowią dane osobowe.

Oczywiście nie każde informacje. Rozporządzenie w motywie 26 podkreśla, że należy wziąć pod uwagę takie czynniki jak koszt i czas potrzebny do identyfikacji osoby, uwzględniając aktualnie dostępną technologię. Nasza ustawa określała to tak: *”informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań”*.

Trzeba pamiętać też jeszcze o tym, że informacje, które samodzielnie nie stanowią danych osobowych (*„kupił niszczarkę AutoMax™ 300CL”*) staną się nimi automatycznie w momencie zestawienia z danymi osobowymi (*„Grażyna Niewiadomska, al. Papierowa 11, Poznań”*).

Dane osobowe wrażliwe

Rozporządzenie wyróżnia tzw. szczególne kategorie danych osobowych, które zwykliśmy określać mianem danych wrażliwych. Są to takie kategorie danych, których co do zasady nie można przetwarzać, bo mają szczególne znaczenie dla prywatności osoby.

Zalicza do nich dane osobowe ujawniające: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne i dane biometryczne, dane dotyczące zdrowia, dane dotyczące seksualności lub orientacji seksualnej.

Te kategorie są podobne do dawnych danych wrażliwych, ale... nie są identyczne. Przykładowo nie znajdują się wśród nich dane dotyczące skazań, gdyż Rozporządzenie, w przeciwieństwie do wcześniejszych przepisów, określa, że „przetwarzania danych osobowych dotyczących wyroków skazujących (...) wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego”. Kolejną istotną zmianą jest uznanie danych biometrycznych za dane wrażliwe. Rozporządzenie określa, że są to „dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne”. Takimi danymi będą też więc m.in. odcisk palca, skan tęczówki oka i cechy charakterystyczne głosu.

Administrator

Za „administratora" uważa się podmiot „który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych". Upraszczając można by powiedzieć, że jest to „właściciel" zebranych danych. W polskiej terminologii posługiwano się określeniem „administrator danych osobowych" (ABI) i wydaje się, że ten termin jeszcze będzie w obiegu przez pewnej czas.

Podmiot przetwarzający

Za podmiot przetwarzający uznaje się „podmiot, który przetwarza dane osobowe w imieniu administratora. W języku potocznym przyjął się termin „procesor", pochodzący od angielskiego określenia podmiotu przetwarzającego. Przykładem procesora będzie zewnętrzne call center lub zewnętrzne biuro księgowe prowadzące księgi rachunkowe.

Inspektor Ochrony Danych

Dawny Administrator bezpieczeństwa informacji (ABI) zostaje zastąpiony Inspektorem Ochrony Danych. W niektórych przypadkach organizacje będą musiały go powołać (np. organy publiczne) i jego zadaniem będzie przede wszystkim monitorowanie przestrzegania przepisów o ochronie danych osobowych, współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla osób, których dane się przetwarza.

Urząd Ochrony Danych Osobowych

Projekt ustawy o ochronie danych osobowych przewiduje, że obecny organ nadzorczy – Generalny Inspektor Ochrony Danych Osobowych (GIODO) – stanie się Prezesem Urzędu Ochrony Danych Osobowych. I analogicznie Biuro GIODO zamieni się w Urząd Ochrony Danych Osobowych. Wszystkie postępowania wszczęte przed GIODO później toczą się przez Prezesem Urzędu i prowadzi się je na podstawie przepisów nowej ustawy o ochronie danych osobowych. Zarejestrowane zbiory danych oraz rejestry administratorów bezpieczeństwa informacji Prezes Urzędu będzie jeszcze przechowywać przez 3 lata. Ilość jego zastępców zwiększy się do trzech.

Grupa robocza art. 29

Grupa robocza art. 29 to europejski zespół roboczy ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych (Working Party on the Protection of Individuals with regard to the Processing of Personal Data) powołany na na mocy art. 29 Dyrektywy 95/46/WE (stąd właśnie nazwa grupy). Wydaje ona często różne opinie, co zawsze miało znaczący wpływ na praktykę stosowania prawa ochrony danych osobowych, a teraz ma wpływ szczególny, kiedy to wytyczne do stosowania Rozporządzenia są wyjątkowo potrzebne[4]. Grupa stanowi niezależne ciało o charakterze doradczym, złożone m.in. z przedstawicieli organów nadzorczych państw Unii oraz przedstawiciela Komisji Europejskiej[5]. Niektóre z ostatnich publikacji grupy roboczej to: Wytyczne dotyczące inspektorów ochrony danych („DPO") - WP243[6], Wytyczne dotyczące prawa do przenoszenia danych – WP242[7], Wytyczne zgłaszania naruszeń bezpieczeństwa informacji - WP250[8]

[4] Informacje prasowe grupy roboczej publikowane są na stronie http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

[5] http://ec.europa.eu/justice/data-protection/article-29/structure/members/index_en.htm

[6] Nieoficjalne tłumaczenie dokumentu WP243 na język polski – http://www.giodo.gov.pl/pl/file/11716

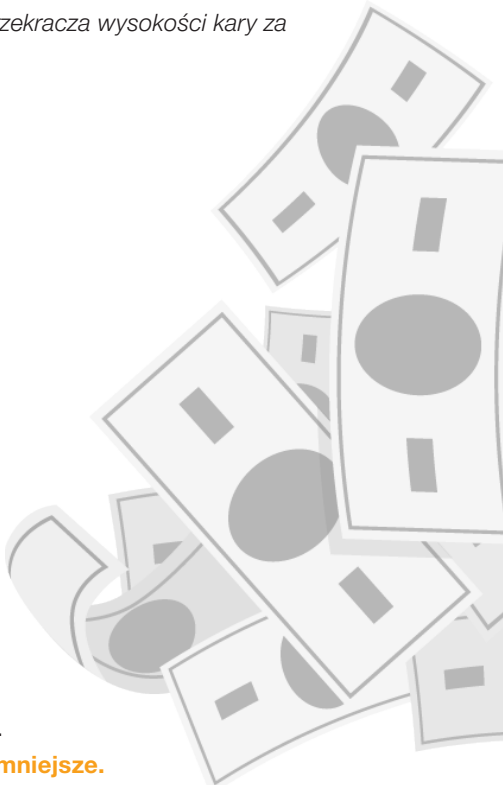
[7] Nieoficjalne tłumaczenie dokumentu WP242 na język polski – http://www.giodo.gov.pl/pl/file/11716

[8] http://ec.europa.eu/newsroom/document.cfm?doc_id=47741 (wersja angielska)

WYSOKIE SANKCJE – SIŁA NOWEGO PRAWA

Wysokie sankcje za nieprzestrzeganie przepisów są motorem napędowym Rozporządzenia. Przeszłoby by ono zapewne bez większego rozgłosu, gdyby nie to, że wprowadza wyjątkowo wysokie kary, które rzeczywiście przemawiają do wyobraźni. Górna granica w wysokości ponad 85 milionów złotych (20 milionów euro) lub 4% rocznego światowego obrotu (w zależności od tego co będzie wyższe) są bez wątpienia dobrym czynnikiem motywującym do ciężkiej pracy nad zapewnieniem zgodności. Niewielkim pocieszeniem jest to, że w ramach jednego postępowania kary nie sumują się: *„jeżeli administrator lub podmiot przetwarzający narusza umyślnie lub nieumyślnie w ramach tych samych lub powiązanych operacji przetwarzania kilka przepisów niniejszego rozporządzenia, całkowita wysokość administracyjnej kary pieniężnej nie przekracza wysokości kary za najpoważniejsze naruszenie”* (art. 83 ust. 3)

Nowe rozporządzenie wprowadza bardzo surowe kary.



W przypadku nakładania kar każdy przypadek będzie indywidualnie rozpatrywany i pod uwagę będą brane m. in. następujące elementy:

- skala naruszenia,
- umyślność działań,
- co zrobiono, żeby zminimalizować szkody poniesione przez osoby, których dane dotyczą,
- *„recydywa”*, czyli czy jest to pierwsze, czy kolejne przewinienie,
- kategorie przetwarzanych danych osobowych,
- stopień współpracy z organem nadzorczym.

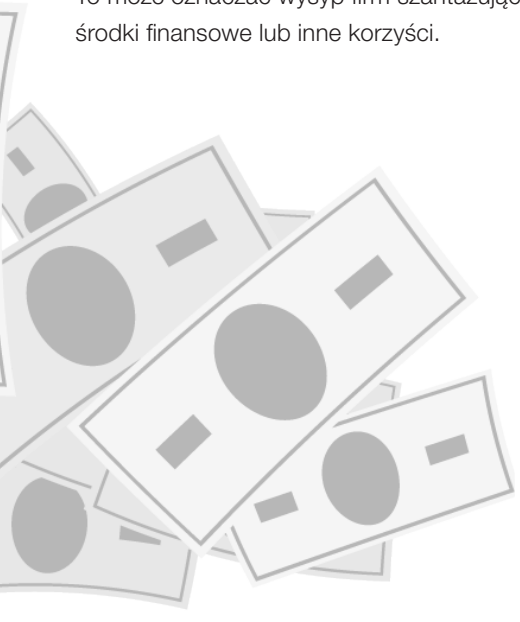
Organ nadzorczy może uwzględniać wszelkie okoliczności obciążające lub łagodzące. Jeśli działanie było celowe, nie zdarzyło się pierwszy raz, a winny nie będzie chciał współpracować, to można zakładać wyższe kary. Przy czym trzeba pamiętać, że **kary dla administracji publicznej będą mniejsze.**

W projekcie ustawy projektodawca ograniczył krąg podmiotów publicznych, wobec których możliwe jest nakładanie administracyjnych kar pieniężnych za naruszenia przepisów o ochronie danych osobowych, a tam gdzie one pozostały, maksymalna granica możliwej do nałożenia kary wynosi 100 tysięcy złotych (art. 50). Co ciekawe – w projekcie ustawy pojawiają się kary dla niesolidnych świadków i biegłych: *„Kto, będąc obowiązany do osobistego stawienia się mimo prawidłowego wezwania nie stawił się bez uzasadnionej przyczyny jako świadek lub biegły albo bezzasadnie odmówił złożenia zeznania, wydania opinii, okazania przedmiotu oględzin albo udziału w innej czynności urzędowej, może być ukarany karą grzywny do 500 zł. Na postanowienie o ukaraniu służy skarga do sądu administracyjnego”.*

Trzeba pamiętać, że w obecnym stanie prawnym GIODO nie może nakładać kar za niezgodność z przepisami, a może jedynie nakazać zapewnienie z nimi zgodności. Dopiero za uparte niestosowanie się (nieprzywracanie tzw. *„stanu zgodnego z prawem”*) organ nadzorczy może zastosować „środki egzekucyjne przewidziane w ustawie z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji”

Przedsiębiorcy, którzy wcześniej mieli większy *„apetyt na ryzyko”*, zmuszeni zostaną do ponownej kalkulacji ryzyka. Warto to zrobić, bo może okazać się, że zapewnienie zgodności z przepisami będzie tańszą strategią niż nieinwestowanie w ochronę danych osobowych.

Bardzo ciekawą sprawą jest możliwe *„uprawnienie organizacji społecznej do wystąpienia z żądaniem wszczęcia postępowania bądź udziału w postępowaniu, nie tylko w przypadku gdy przemawia za tym interes społeczny, o czym stanowi art. 31 § 1 KPA, ale również gdy przemawia za tym interes osoby, której prawa zostały naruszone”*. To może oznaczać wysyp firm szantażujących mniej przygotowane organizacje i wyłudzających w ten sposób środki finansowe lub inne korzyści.



Wysokie kary to nie wszystko – art. 82 Rozporządzenia określa, iż osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia przepisów Rozporządzenia ma prawo do uzyskania od administratora lub procesora odszkodowania za poniesioną szkodę. W efekcie oprócz kary, organizacja może ucierpieć wypłacając osobom odszkodowania. Co do zasady, administrator odpowiada za szkody spowodowane przetwarzaniem naruszającym przepisy, a procesor tylko wtedy, gdy nie dopełnił obowiązków, które Rozporządzenie nakłada bezpośrednio na niego lub gdy działał *„poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom”*. Oczywiście obaj zostają zwolnieni z odpowiedzialności odszkodowawczej, jeżeli są w stanie udowodnić, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.

Na koniec warto pamiętać, że proponuje się pozostawić karę grzywny za utrudnianie kontroli oraz wprowadzić dodatkowe przepisy karne za bezprawne przetwarzanie danych wrażliwych – co pozwala domyślać się, że dla polskiego ustawodawcy te zagadnienia są szczególnie istotne.

CO TRZEBA ZMIENIĆ

25 maja 2018 r.
należy być w pełnej zgodzie z przepisami o ochronie danych osobowych

Obecne przetwarzanie danych osobowych należy dostosować w ciągu dwóch lat od wejścia w życie nowych przepisów. Proces dostosowywania jest długotrwały, dlatego przygotowania należy zacząć jak najszybciej.

Aby być dobrze przygotowanym należy m. in.:

- zapewnić zgodność przetwarzania z obecnie obowiązującymi przepisami, tj. ustawą o ochronie danych osobowych – ułatwi to przygotowania do zapewnienia zgodności z Rozporządzeniem,
- poznać dobrze wymagania Rozporządzenia, by wiedzieć do czego należy się przygotować,
- przeszkolić zespół, który będzie koordynował przygotowania,
- zrozumieć gdzie i jakie dane są przetwarzane, przeanalizować obecne procesy zbierania danych,
- dokonać przeglądu własnych zleceniobiorców (tzw. procesorów) i współpracować z nimi, aby także dostosowali swoje procesy do Rozporządzenia,
- przejrzeć istniejące procedury i dokumentację,
- przeanalizować kto i za co jest odpowiedzialny w procesach przetwarzania,
- wdrożyć procesy analizy i szacowania ryzyka, w szczególności szacowania ryzyka dla osób, których dane są przetwarzane
- wzmocnić zabezpieczenia (tam gdzie to potrzebne, bazując na ocenie ryzyka) i zapewnić, że bezpieczeństwo będzie wbudowane we wszystkie nowe procesy,
- dokumentować naruszenia bezpieczeństwa i prowadzić rejestr incydentów,
- przygotować procesy zarządzania incydentami bezpieczeństwa.

Chyba każdy już wie, że dostosowanie się do Rozporządzenia nie jest kwestią wyłącznie działu prawnego czy IT. Zapewnienie zgodności wymaga skoordynowanej współpracy w całej organizacji.

Przygotować muszą się administratorzy danych oraz współpracownicy czyli tzw. *„procesorzy”*.

Podkreślenia wymaga to, że **przygotować muszą się zarówno administratorzy danych jak i podmioty, które przetwarzają dane na zlecenie**, szczególnie że w stosunku do tych ostatnich Rozporządzenie definiuje bardzo dużo nowych obowiązków.

Zgodność z Rozporządzeniem, to nie tylko uniknięcie wysokich kar. Coraz więcej uczestników rynku zdaje sobie sprawę z tego, jaka jest ekonomiczna wartość danych, które dzięki nowym technologiom pozyskiwane i przetwarzane są z każdym rokiem coraz szybciej i w coraz większych ilościach. Rośnie też świadomość osób, których dane są przetwarzane (klientów), którzy zdają sobie sprawę z zagrożeń wynikających z udostępniania danych. W związku z tym, coraz ważniejszym staje się zapewnienie ochrony ich prywatności, a tym samym zdobycie ich zaufania.

Każda organizacja, która chce spełnić oczekiwania swoich klientów, powinna zapoznać się z nowymi regulacjami, w odpowiedni sposób przygotować się, a następnie wdrożyć przepisy Rozporządzenia.

OCENA SKUTKÓW DLA OCHRONY DANYCH – SERCE SYSTEMU

Ocena skutków dla ochrony danych

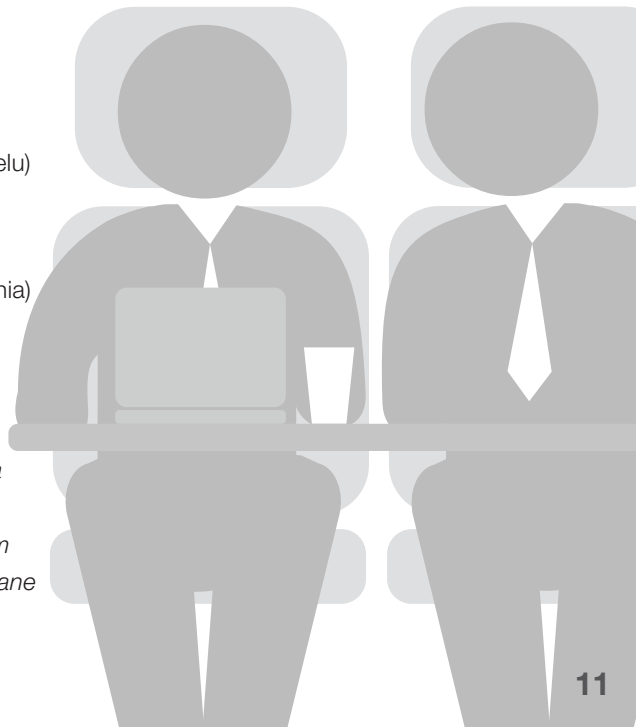
Art. 35 ust. 1 Rozporządzenia określa, że jeżeli dany rodzaj przetwarzania danych – zwłaszcza z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Ocenę skutków często określa się skrótowo DPIA od angielskiego terminu *„data privacy impact assessment”.*[9]

Zgodnie z „*Wytycznymi w sprawie oceny skutków dla ochrony danych...*” (WP248), przygotowanymi przez grupę roboczą art. 29[10] *„DPIA to proces który pozwala budować i wykazywać zgodność z przepisami”*.

Ocena skutków dla ochrony danych to jeden z najważniejszych elementów zapewnienia zgodności

Czytając zapisy art. 35 ustępu ma się wrażenie, że ocena skutków jest opcjonalna (bo tylko w niektórych przypadkach musi zostać wykonana) i nie odczuwa się wcale, że to bardzo ważny proces. A jednak okazuje się, że ocena (a raczej oceny) są sercem całego systemu przetwarzania danych osobowych – bo to od nich wszystko się zaczyna. Zanim zacznie się przetwarzać jakiekolwiek dane, należy najpierw określić czy jest „duże prawdopodobieństwo powodowania wysokiego ryzyka” dla prywatności, a jeśli jest – należy dokonać oceny skutków dla ochrony danych. Ocena taka powinna zawierać następujące informacje (art. 35. ust. 7):

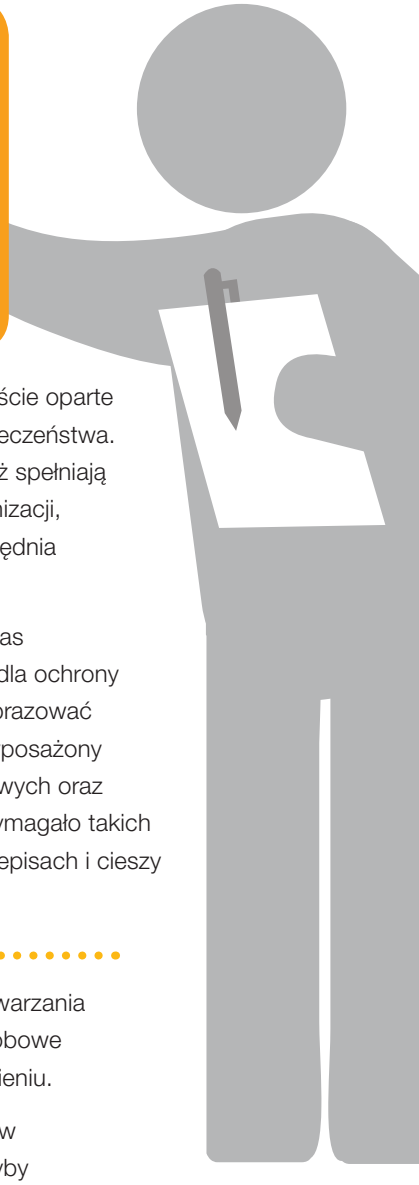
- *„systematyczny opis planowanych operacji przetwarzania i celów przetwarzania”* (udokumentowanie jakie dane osobowe będą przetwarzane, w jaki sposób oraz w jakim celu)
- *„ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów”*; (samoocena czy dane są niezbędne oraz adekwatne do celu przetwarzania)
- *„ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą”*
- *„środki planowane w celu zaradzenia ryzyku, w tym: 1) zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem 2) praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy”.*



DPIA można porównać do obowiązującego jeszcze modelu rejestrowania zbiorów – jego zawartość jest zasadniczo podobna do tego, co powinno znajdować się we wniosku zgłoszenia zbioru do rejestracji. I podobnie działa mechanizm momentu, od kiedy dane można przetwarzać – w przypadku zbiorów można było po wysłaniu zgłoszenia do rejestracji, a teraz – po dokonaniu oceny skutków. Różnica polega jedynie na tym, że kiedyś GIODO oceniał m.in., czy operacje są niezbędne i proporcjonalne, i czy ryzyko nie jest wysokie. Jeśli uznawał on, że istnieje zagrożenie dla praw i wolności osób, których dane dotyczą, odmawiał rejestracji zbioru. Teraz ten obowiązek ciążyć będzie na administratorze danych.

Kolejnym podobieństwem **DPIA** do dawnych zbiorów danych jest konieczność okresowych przeglądów. Jeśli coś się zmieniło, trzeba było wysłać zgłoszenie aktualizacyjne zbioru. **DPIA** też trzeba będzie aktualizować - art. 35. ust. 11 określa, że *„gdy zmienia się ryzyko wynikające z operacji przetwarzania, administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych”.*

Jeśli ocena skutków przetwarzania potwierdzi wysokie ryzyko trzeba będzie konsultować się z organem nadzorczym.



Bardzo ważną i szczególnie akcentowaną koncepcją w Rozporządzeniu jest podejście oparte na ryzyku – tylko po oszacowaniu ryzyka można dobrać odpowiednie środki bezpieczeństwa. A gdy ryzyko zmienia się, trzeba przeanalizować, czy obecne zabezpieczenia wciąż spełniają swoją rolę. Jest to prawdziwa rewolucja nie tylko w przepisach, ale także dla organizacji, bo rzadko która organizacja szacuje ryzyko, a jeśli już, to niezmiernie rzadko uwzględnia w nim ryzyko dla ochrony danych osobowych.

Szacowania ryzyka nie trzeba się bać. To bardzo praktyczne podejście, aby podczas przetwarzania danych osobowych brać pod uwagę istniejące i potencjalne ryzyka dla ochrony po to, aby zastosować odpowiednie do nich środki bezpieczeństwa. Można to zobrazować przykładem domu – jeśli znajduje się w nim wartościowe wyposażenie – będzie wyposażony w drzwi i okna ze zwiększoną odpornością na włamanie, system kamer przemysłowych oraz służby ochrony, natomiast niewielkie i słabo wyposażone mieszkanie nie będzie wymagało takich zabezpieczeń. Takiego racjonalnego podejścia brakowało w dotychczasowych przepisach i cieszy fakt, że pojawia się ono w Rozporządzeniu.

Podmiotem zobowiązanym do dokonania oceny ryzyka przed rozpoczęciem przetwarzania jest administrator danych, niezależnie od tego, czy zamierza przetwarzać dane osobowe samodzielnie, czy w przetwarzaniu będzie brał udział podmiot działający w jego imieniu.

Organizacje i przedsiębiorcy powinni konsultować się z UODO, jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka (…) (art. 36 ust. 1).

Dokonanie oceny skutków wymagać będzie zaangażowania inspektora ochrony danych, jeśli został powołany, a jeśli nie, to można założyć, że do przygotowania się w tym obszarze niezbędne będzie profesjonalne wsparcie, gdyż jest mało prawdopodobne, żeby przedsiębiorca, który nie posiada specjalistycznej wiedzy eksperckiej, sam był wstanie dokonać odpowiedniej analizy skutków przetwarzania danych.

Rejestr czynności przetwarzania

Zamiast rejestrowania zbiorów w GIODO, administrator danych osobowych będzie musiał prowadzić rejestr czynności przetwarzania danych osobowych. Obowiązek ten będzie także spoczywać na podmiotach przetwarzających (procesorach) – co jest absolutną nowością.

W preambule (motyw 98) podkreśla się: Dyrektywa 95/46/WE przewidywała ogólny obowiązek zawiadamiania organów nadzorczych o przetwarzaniu danych osobowych. Obowiązek ten powoduje jednak obciążenia administracyjne i finansowe, i nie zawsze przyczyniał się do poprawy ochrony danych osobowych. Dlatego należy znieść te powszechne, ogólne obowiązki zawiadamiania i zastąpić je skutecznymi procedurami i mechanizmami, koncentrującymi się w zamian na tych rodzajach operacji przetwarzania, które ze względu na swój charakter, zakres, kontekst i cele mogą nieść duże zagrożenie dla praw i wolności osób fizycznych. Likwiduje się rejestrację zbiorów, a wprowadza rejestr czynności przetwarzania. Rozporządzenie wskazuje, iż rejestr powinien być prowadzony w formie pisemnej, w tym w formie elektronicznej.

Rejestr przetwarzania ma zawierać m.in. następujące kategorie informacji:

- **informacje o administratorze i ew. współadministratorach,**
- **dane inspektora ochrony danych,**
- **opis celów przetwarzania,**
- **kategorie danych osobowych,**
- **kategorie osób, których dane się przetwarza,**
- **informacje o odbiorcach (także w państwach trzecich),**
- **planowane terminy usuwania poszczególnych kategorii danych,**
- **opis środków bezpieczeństwa.**

Procesorzy także będą musieli prowadzić rejestr czynności przetwarzania.

W rejestrze prowadzonym przez podmioty przetwarzające nie podaje się celu przetwarzania i kategorii odbiorców, którym dane osobowe zostały lub zostaną udostępnione oraz planowanych terminów usunięcia poszczególnych kategorii danych z uwagi na to, że o tych kwestiach decyduje administrator.

Rozporządzenie zwalnia z obowiązku prowadzenia rejestru w sytuacji, gdy dana organizacja zatrudnia mniej niż 250 osób. Jest jednak od tego wyjątek: taki rejestr musi być prowadzony, jeśli przetwarzanie danych w organizacji może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, przetwarzanie nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa.

Podkreślenia wymaga to, że rejestr czynności przetwarzania będzie musiał być udostępniony UODO, kiedy tylko tego zażąda.

Zgodnie z (jeszcze obowiązującą) ustawą oraz przepisami wykonawczymi na dokumentację przetwarzania składają się m.in. polityka bezpieczeństwa, instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, imienne upoważnienia, ewidencja upoważnień, etc. Od 25 maja 2018 r. prowadzenie takiej dokumentacji nie będzie obowiązkowe. Nie zmienia to jednak faktu, że administrator będzie musiał wykazać w jaki sposób przestrzega przepisy. W tym celu na pewno będzie wymagana odpowiednia dokumentacja.

[9] Zaskakujące jest przetłumaczenie „data privacy" jako ochronę danych – prywatność i ochrona danych to nie są w zasadzie tożsame pojęcia. Ocena skutków dla prywatności pewnie byłaby lepszym określeniem niż ocena skutków dla ochrony danych.
[10] http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

PRIVACY BY DESIGN – OCHRONA NA ETAPIE PROJEKTOWANIA

Architekt projektując nowy dom musi pamiętać także o zabezpieczeniach takich jak przykładowo instalacja przeciwpożarowa, wyjścia ewakuacyjne, bezpieczniki i wyłączniki różnicowe w instalacji elektrycznej, uziemienie, piorunochrony, wentylacja, etc. Komponuje je tak, aby dom był ładny, funkcjonalny i jednocześnie bezpieczny. W ten sam sposób teraz trzeba będzie podchodzić do procesów w których będą przetwarzane dane osobowe uwzględniając na etapie projektowania ochronę prywatności. Taka koncepcja nazywa się *privacy by design*.[11] Pomysłodawczynią tej idei była Ann Cavoukian, kanadyjska rzecznik ochrony danych. Promowane przez nią 7 podstawowych zasad prywatności warto stosować niezależnie od tego, czy wymaga ich Rozporządzenie czy też nie.[12]

Te zasady to:

- **pro-aktywność zamiast reakcji, lepiej zapobiegać niż leczyć;**
- **prywatność jako domyślne *„ustawienie”*;**
- **prywatność wbudowana w projekt ustawy o ochronie danych osobowych;**
- **pełna funkcjonalność jako suma dodatnia, niezerowa;**
- **ochrona od początku do końca trwania przetwarzania;**
- **otwartość – transparentność i widoczność;**
- **poszanowanie prywatności – osoba w centrum uwagi.**

Podczas prac nad regulacją dostrzeżono korzyści ze stosowania tych zasad i zaimplementowano je w treści Rozporządzenia.

Ochrona na etapie projektowania

Ochrona danych ma być wbudowywana w politykę przedsiębiorstwa już na etapie projektowania systemu ochrony danych osobowych (by design), a także ma być aktywna domyślnie (by default), czyli bez konieczności podejmowania działań przez osoby, których dane dotyczą.

Uwzględnianie ochrony w fazie projektowania jest niczym innym jak dobrą praktyką, którą można by zobrazować stwierdzeniem, że *„lepiej zapobiegać niż leczyć”,* gdyż w procesie wprowadzania produktu, usługi lub systemu informatycznego późniejsze wdrażanie mechanizmów gwarantujących ochronę danych osobowych jest na pewno dużo droższe i trudniejsze. Od maja 2018 r. ta praktyka stanie się obowiązkiem.

W preambule (motyw 78) czytamy, że: administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Procedury opisane w przedmiotowym dokumencie powinny obejmować m.in. sytuację, w której organizacja projektuje nową aplikację dla klientów oraz precyzować, aby w jej wdrażanie zaangażowane były odpowiednie osoby, które ocenią zgodność procesu z Rozporządzeniem, a także które zweryfikują techniczne i organizacyjne zabezpieczenia danych.

Rozporządzenie stanowi, że wywiązywanie się z tych obowiązków można wykazać między innymi poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji, określonego w art. 42 Rozporządzenia.

Co ciekawe, już wcześniej mówiło się o koncepcie privacy by design, ale skoro prawo dotyczy ochrony danych osobowych, a prywatność to szersze pojęcie, przemianowano go później na data protection by design and by default – w polskiej wersji przetłumaczone jako uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych (art. 25).

Domyślna ochrona danych

Funkcjonuje już gdzieniegdzie w praktyce. Przykładowo, producenci domowych routerów sieci bezprzewodowej nie ustalają już takich samych haseł dla każdego urządzenia, ponieważ użytkownicy często korzystali z ustawień domyślnych. Ułatwiało to dostęp do sieci, a przez to też do informacji prywatnych, osobom nieupoważnionym. Teraz przyszedł czas na dane osobowe.

Domyślnie powinny być przetwarzane tylko te dane, które są **niezbędne**

Pierwotnie ta koncepcja dotyczyła korzystania z usług świadczonych drogą elektroniczną, szczególnie portali społecznościowych, takich jak Facebook. Miała ona chronić użytkowników przed nieświadomym upublicznianiem swoich danych, bowiem często okazywało się, że nie byli oni świadomi zastosowanych domyślnie ustawień prywatności. Rozporządzenie ostatecznie rozszerzyło tę koncepcję i w myśl Rozporządzenia (art. 25 ust. 2) domyślnie mogą być przetwarzane wyłącznie te dane, które są niezbędne. [13]

Domyślną ochronę danych osobowych można łatwo zobrazować przykładem z serwisów społecznościowych. Każdy nowy post, który tam umieszczamy, powinien być z założenia niewidoczny. Dopiero sam użytkownik powinien móc każdorazowo zmieniać ustawienia prywatności, decydując się np. na widoczność tylko dla znajomych, czy dla wszystkich osób.

Przygotowując się należy przeanalizować jak przebiegają obecne procesy tworzenia nowych produktów czy usług, w których przetwarza się dane osobowe. Na pewno jednym z pomysłów może być zapewnienie, że wymagania i realizację wymagań w zakresie prywatności będzie nadzorował np. inspektor ochrony danych (o ile go powołano). Bez wątpienia ostrożniej trzeba będzie projektować nowe produkty czy usługi, a w każdym przypadku szacować potencjalne ryzyko. Niekiedy pewne rozwiązania mogą wymagać konsultacji z UODO, co może okazać się czasochłonne. Bardzo ważnym elementem jest technologia komputerowa – zwłaszcza architekci rozwiązań informatycznych oraz programiści powinni być świadomi nowych regulacji. Mimo, że w wielu organizacjach bezpieczeństwo informacji traktuje się bardzo poważnie i stosuje się zasadę *„security by design”*, to należy pamiętać, że nie jest ono tożsame z „privacy by design” i będzie wymagać dostosowania do Rozporządzenia.

Pseudonimizacja

Pseudoanonimizacja była już wcześniej powszechnie stosowana, jednak nie mieliśmy na taki proces żadnego określenia. Przykładowo oceny w szkole publikowano w ten sposób, że zamiast imienia i nazwiska na wykazie znajdował się numer legitymacji lub indeksu. I w taki sposób informacja o tym, że z *„uczeń o numerze legitymacji 134/17 z języka polskiego otrzymał ocenę 4+”* stanowiła właśnie pseudoanonimizację.

Rozporządzenie tłumaczy to pojęcie następująco – jest to *„przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej”.* W preambule (motyw 26) wskazano, iż spseudonimizowane dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje o możliwej do zidentyfikowania osobie fizycznej. Czyli takie informacje to wciąż dane osobowe. Dodatkowo, ustawodawca wskazał w treści Rozporządzenia pseudonimizację jako przykład jednego z mechanizmów, mających za zadanie zapewnić taki stopień bezpieczeństwa danych, który odpowiada ryzyku ich naruszenia (art. 32 ust. 1 lit. a).

Pseudonimizacja danych jest jednym z mechanizmów ochrony danych.

Nawet jeśli doszłoby do wycieku takich informacji to osoba nieupoważniona niewiele by się dowiedziała. Cóż bowiem znaczyłaby dla niej informacja, że ktoś o numerze identyfikacyjnym 0178 wpłacił w dniu 30 lipca 2017 r. 450 zł? Nic. Ta wiedza pozostaje jedynie u administratora i osób upoważnionych, mających dostęp do danych. Jak widać, jest to tania i wydajna metoda zmniejszania ryzyka. Okazuje się więc, że zastosowanie danych pseudonimizowanych zmniejsza możliwość naruszenia bezpieczeństwa informacji. Warto podkreślić, że to, jakie narzędzia stosować (pseudonimizację, anonimizację, szyfrowanie, haszowanie lub inne) wynikać będzie z analizy ryzyka.

Nr klienta	Data wpłaty	Kwota	Podpis zbierającego
14386	5/3/2017	450zł	Jan Kowalski
07462	14/4/2017	413zł	Jan Kowalski
16584	25/4/2017	520zł	Jan Kowalski

Przykład zastosowania anonimizacji

[11] W języku polskim nie ma tak ładnie brzmiącego odpowiednika i koncepcję tę należałoby tłumaczyć jako ochrona na etapie projektowania, co już tak wiernie nie oddaje znaczenia określenia privacy by design.

[12] Privacy by Design, The 7 Foundational Principles, Ann Cavoukian, Canada 2011, https://www.ipc.on.ca/wp-content/uploads/ Resources/7foundationalprinciples.pdf oraz https://www.ipc.on.ca/wp-content/uploads/Resources/PbDReport.pdf

[13] Oczywiście o niezbędności danych należy mówić w kontekście domyślnego przetwarzania, nie należy uznawać, że jest to likwidacja obowiązującej wcześniej zasady adekwatności danych.

RAPORTOWANIE NARUSZEŃ BEZPIECZEŃSTWA

Od kilku lat przedsiębiorcy telekomunikacyjni w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych mają obowiązek powiadamiać o takim zdarzeniu GIODO, a także (w niektórych sytuacjach) abonenta lub użytkownika końcowego. Przepisy Rozporządzenia podobny obowiązek wprowadzają wobec każdego, kto przetwarza dane osobowe.

Przez naruszenie ochrony danych osobowych rozumie się *„naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych”.*

Naruszenie ochrony danych należy zgłosić do UODO w ciągu

72 godzin

W szczególnych przypadkach trzeba będzie też informować klientów.

W sytuacji, w której naruszenie ochrony danych osobowych prawdopodobnie będzie skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, zgłasza się je do Prezesa Urzędu Ochrony Danych Osobowych bez zbędnej zwłoki – ale nie później niż w ciągu 72 godzin. Motyw 75 Rozporządzenia opisuje stosunkowo wyczerpująco i dość dokładnie w jakich przypadkach takie ryzyko może występować:

Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności: jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną; jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa; jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych; lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci; jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

To, które naruszenia należy zgłaszać do organu nadzorczego należy oceniać przez pryzmat wpływu na prawa i wolności osób, których dane dotyczą. Utrata pamięci USB z dużą ilością danych klientów jest przypadkiem oczywistym. Zatrzymanie pracy systemów nie wydaje się być czymś, co mieściłoby się w definicji naruszenia

bezpieczeństwa. I zazwyczaj nie będzie, ale na pewno będą takie sytuacje, w których brak dostępu, nawet chwilowy, do danych będzie stanowić ryzyka dla prac i wolności osób, np. brak dostępu do elektronicznej dokumentacji medycznej z powodu ataku DDoS.

Warto przyjrzeć się Wytycznym WP250[14] przygotowanym przez grupę roboczą art. 29; stanowią one doskonałą podpowiedź jak postępować.

Przykłady sytuacji w których **trzeba będzie zgłaszać naruszenie do Prezesa Urzędu:**

- zgubienie nośnika USB lub płyty CD-ROM z danymi osobowymi,
- utrata lub kradzież laptopa, w którym nie zastosowano szyfrowania,
- kradzież komputera z biura,
- włamanie do sieci komputerowej,
- wysłanie danych osobowych pocztą elektroniczną osobie nieuprawnionej,
- przypadkowe udostępnienie danych osobowych na stronie internetowej.

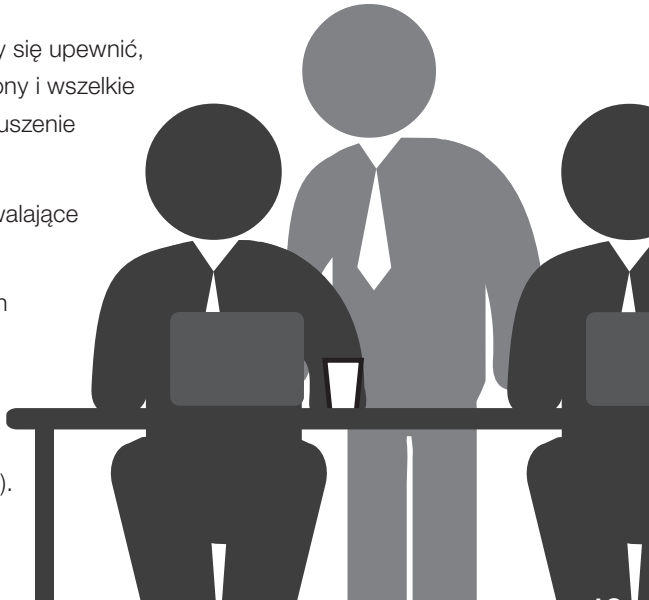
W takich sytuacjach naruszenia **nie będzie trzeba zgłaszać naruszenie do Prezesa Urzędu:**

- zgubienie lub kradzież nośnika na którym dane były zaszyfrowane.
- zgubienie lub kradzież laptopa z szyfrowanym dyskiem,
- zagubienie spseudoanonimizowanych wydruków,
- nieskuteczna próba ataku na sieć komputerową,
- wykrycie i usunięcie wirusa komputerowego.

Wykrywanie naruszeń

Aby móc informować o naruszeniach, trzeba mieć możliwości ich wykrywania – art. 33 ust. 1 podkreśla, że trzeba je zgłaszać *„po stwierdzeniu naruszenia”* (ang. *„after having become aware”*). Administrator musi mieć uzasadnione przekonanie co do tego, czy naruszenie wystąpiło, czy nie.

W preambule Rozporządzenia (motyw 87) czytamy, że należy się upewnić, czy wdrożono wszelkie odpowiednie techniczne środki ochrony i wszelkie odpowiednie środki organizacyjne, by od razu stwierdzić naruszenie ochrony danych osobowych.



Bez wątpienia potrzebne będą techniczne mechanizmy pozwalające wykrywać naruszenia takie jak:

- systemy monitorowania i korelowania zdarzeń w systemach komputerowych (SIEM),
- rozwiązania do wykrywania i zatrzymywania zagrożeń w sieciach komputerowych (IDS/IPS),
- programy wykrywające potencjalne wycieki informacji (DLP).

Wszyscy pracownicy muszą wiedzieć komu zgłaszać incydenty bezpieczeństwa

Każdy z nas zna pewnie numer alarmowy 112, pod który należy dzwonić w przypadkach, gdy niezbędna jest pomoc podmiotów i służb, do których zadań należy ochrona życia, zdrowia, bezpieczeństwa i porządku publicznego. Dlatego w przypadku naruszenia ochrony danych bardzo ważne jest, aby posiadać wewnętrzny odpowiednik numeru alarmowego. Każdy pracownik i każdy podmiot współpracujący (zleceniobiorca przetwarzający dane osobowe) powinien wiedzieć, do kogo i jak zgłaszać takie sytuacje. Nie ma bowiem nic gorszego, niż niepewność komunikacyjna, komu przekazać informację, bo przy incydentach czas ma duże znaczenie i im szybciej ktoś zajmie się incydentem, tym mniej strat dla organizacji. W przypadku incydentu liczy się każda sekunda, dlatego procedury nie mogą być zbyt skomplikowane. **Bardzo ważne jest aby jasno określić, kto jest odpowiedzialny za zgłoszenie naruszenia do organu nadzorczego.** Może to być dowolna osoba, w tym także Inspektor ochrony danych, przy czym musi mieć ona do tego odpowiednie pełnomocnictwo.

Procedura postępowania

Program zarządzania incydentami dotyczącymi ochrony danych osobowych powinien składać się z trzech kluczowych elementów:

1. Ustalenie kanałów komunikacyjnych do zgłaszania zdarzeń lub słabości systemu
2. Ustalenie sposobów postępowania (procedur) zapewniających szybką reakcję na zdarzenia
3. Wyznaczenie osób, które będą brać udział w sprawie rozwiązywania incydentu

W zasadzie przygotowując procesy dotyczące naruszeń ochrony danych osobowych warto (a nawet trzeba) odnosić się do uznanych standardów. Przykładowo incydent wg normy PN/ISO 27001:2007 to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji. Norma przywołuje też termin zdarzenia związanego z bezpieczeństwem informacji za które uznaje określony stan systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem. Możemy użyć dokładnie tych samych definicji, zamieniając bezpieczeństwo informacji na termin: ochrona danych osobowych.

Różnica między zdarzeniem i incydentem polega na wpływie zdarzenia (bądź zdarzeń) na firmę. Najlepiej obrazuje to przykład zarażenia komputera wirusem. Jeśli wirus został w miarę szybko usunięty i nie poczynił

żadnych szkód – jest to zdarzenie. Jeśli jednak zarażone zostały wszystkie komputery w firmie (wiele zdarzeń) i istniało ryzyko wycieku danych (wpływ na biznes, zagraża bezpieczeństwu danych osobowych) lub dane zostały rzeczywiście udostępnione — to jest to incydent.

W art. 33 ust. 5 Rozporządzenia ustanowiono obowiązek prowadzenia dokumentacji dla wszelkich naruszeń ochrony danych osobowych. Oznacza to, że nawet jeśli administrator nie ma obowiązku poinformowania organu nadzorczego o konkretnym negatywnym zdarzeniu, musi i tak je odnotować we własnym rejestrze.

W sytuacji, w której naruszenie niesie ze sobą wysokie *„ryzyko naruszenia praw lub wolności osób fizycznych”*, administrator powinien również bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą o takim naruszeniu – jasnym i prostym językiem (art. 34 ust. 1 i 2 Rozporządzenia).

Trzeba pamiętać, że informowanie o naruszeniu bezpieczeństwa, szczególnie wszystkich klientów, może być bardzo kosztowne, zarówno operacyjnie, jak i wizerunkowo. Dlatego też warto dołożyć wszelkich starań, aby zminimalizować ryzyko wycieków danych.

Z tym zaś wiąże się konieczność wdrożenia rozmaitych zabezpieczeń technicznych i organizacyjnych. Można śmiało powiedzieć, iż w świetle nowych przepisów organizacje będą musiały uwzględnić większy budżet na wdrożenie mechanizmów zabezpieczenia danych osobowych niż dotychczas.

Pamiętajmy, że sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim stopniu administrator danych lub podmiot przetwarzający zgłosili naruszenie, będzie brany pod uwagę przez organ nadzorczy przy ustalaniu wysokości ewentualnej kary finansowej.

[14] http://ec.europa.eu/newsroom/document.cfm?doc_id=47741

ZMIANY W FIRMOWYCH DOKUMENTACH, FORMULARZACH I SYSTEMACH

Dane osobowe można zbierać dopiero po wykonaniu oceny skutków dla ochrony danych, chyba że taka ocena nie była wymagana.[15]

Zbieranie danych

Obowiązek informacyjny, narzucony na administratora podczas zbierania danych, zostanie znacznie poszerzony. Zbierając dane trzeba będzie przekazywać znacznie więcej informacji niż do tej pory, bo trzeba będzie więc informować o:

- kontakcie do inspektora ochrony danych (jeśli go powołano),
- nazwie i danych kontaktowych przedstawiciela, jeżeli istnieje,
- podstawie prawnej przetwarzania,
- prawnie uzasadnionym interesie administratora, jeżeli na tej podstawie odbywa się przetwarzanie,
- informacji o zamiarze przekazywania danych do państwa trzeciego,
- okresie, przez który dane osobowe będą przechowywane, bądź kryteria ustalania tego okresu,
- profilowaniu,
- o prawie wniesienia skargi do organu nadzorczego,
- w przypadku istnienia obowiązku podania danych osobowych: wskazaniu ewentualnych konsekwencji niepodania danych,
- prawach osoby, której dane dotyczą, tj. prawie do:
  - usunięcia danych,
  - ograniczenia przetwarzania,
  - prawie przenoszenia danych,
  - prawie do cofnięcia zgody (gdy osoba, której dane dotyczą wyraża zgodę na przetwarzanie danych).

Osobom trzeba będzie przekazywać więcej informacji w sposób przyjazny i zrozumiały.

Jeśli pozyskuje się dane osobowe nie bezpośrednio od osoby, której dane dotyczą, obowiązek informacyjny poszerza się jeszcze o informację o źródle pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych. Poszerza się również prawo do udzielenia informacji na żądanie. Trzeba będzie też przeformułować obecne komunikaty, bo Rozporządzenie narzuca obowiązek komunikowania się z osobami w sposób przyjazny, przystępnym i zrozumiałym językiem, tak aby przekaz do nich kierowany można było odebrać i zrozumieć bez wysiłku.

Preambuła Rozporządzenia (motyw 39) stanowi: 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. Zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania oraz podawania innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących.

W motywie 58 zaś czytamy: zasada przejrzystości wymaga, by wszelkie informacje kierowane do ogółu społeczeństwa lub osoby, której dane dotyczą, były zwięzłe, łatwo dostępne i zrozumiałe, by były formułowane jasnym i prostym językiem, a w stosownych przypadkach, dodatkowo wizualizowane.

Także art. 12 Rozporządzenia podkreśla to wyjątkowo dobitnie: *„aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji”.*

To wszystko oznaczać będzie będzie modyfikację wszelkich formularzy, zarówno tych papierowych, jak i elektronicznych, zawierających zgody na przetwarzanie danych osobowych oraz przekazujących informacje wymagane przez prawo.

Warunki wyrażenia i odwołania zgody

Art. 7 określa warunki wyrażania zgody. Bardzo interesujący jest zapis: *„wycofanie zgody musi być równie łatwe jak jej wyrażenie”.* Wbrew pozorom dzisiaj wielu administratorów pozwala na wyrażenie zgody nawet w formie elektronicznej, natomiast do jej odwołania konieczne jest wizyta w biurze firmy lub wysłanie pisma listem poleconym. Rozporządzenie to zmienia.

Odwołanie zgody musi być tak samo łatwe, jak jej udzielenie.

Kolejną kwestią wyróżniającą nową definicję zgody jest pewna kategoria zachowań, określona jako wyraźne działanie potwierdzające. Oznacza to, że zgodę można wyrazić także poprzez działanie, a nie jedynie oświadczenie.

Na pewno za takie działanie będzie uważać się *„zaznaczenie”* zgody w elektronicznym formularzu. W świetle nowych przepisów już samo przesłanie aplikacji do potencjalnego pracodawcy może stanowić wyrażenie zgody na przetwarzanie danych w celu rekrutacji. W świetle obecnie obowiązującego prawa takie czynności wymagały zgody, którą dołączano do życiorysu z poczuciem bezsensownego takiego działania. Bardzo ważne jest, że na administratorze będzie ciążył dowód uzyskania zgody.

Przykładowo podczas zbierania danych należy podać okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu. Do tej pory konieczność podawania takich informacji nie pojawiała się w przepisach.

Podczas zbierania danych trzeba poinformować osobę o tym, jak długo jej dane będą przechowywane.

Obowiązki informacyjne

Rozporządzenie kontynuuje dotychczasowe prawo do uzyskania informacji (art. 15). Każda osoba (nawet postronna) „jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące". Jeśli jej dane osobowe są przetwarzane, to trzeba jej umożliwić dostęp do tych danych oraz przekazać informacje, które pozwolą jej zorientować się m.in. w jakim celu dane są przetwarzane, jak długo, jakie prawa jej przysługują, i jakie jest źródło tych danych. Dalej Rozporządzenie określa, iż „administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu". Administrator danych musi udzielić informacji:

Na piśmie, elektronicznie lub ustnie, jeżeli podmiot danych tego zażąda

W terminie jednego miesiąca od otrzymania wniosku

Bezpłatnie

Prawo to może też być nieco uciążliwe dla firmy, ponieważ takich informacji może żądać każdy. I można jej żądać w zasadzie od każdego, kto przetwarza (lub mógłby przetwarzać) dane osobowe.

Trzeba pamiętać, że jeśli osoba żąda informacji i nie ma pewności co do jej tożsamości, to należy odmówić udzielenia odpowiedzi, bo nie można ryzykować ujawnienia danych osobowych osobie nieupoważnionej.

Prawo do przenoszenia danych

Zupełną nowością jest prawo do przenoszenia danych. Art. 20 Rozporządzenia wskazuje, że osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane innemu administratorowi bez przeszkód ze strony administratora, któremu dane te dostarczono.

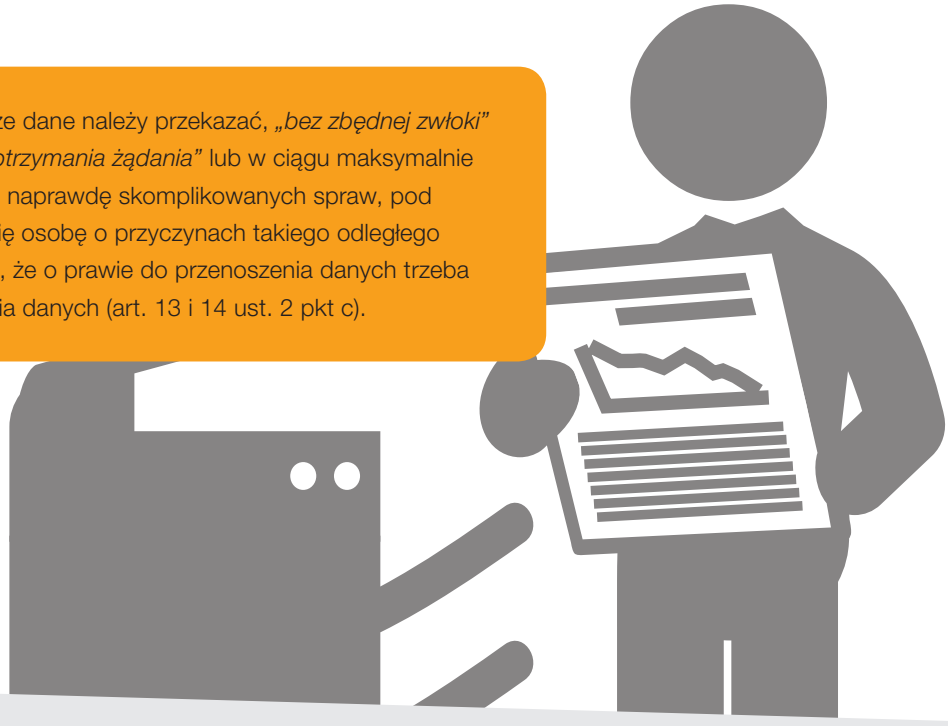
Celem przenoszenia danych jest ułatwienie zamiany jednego dostawcy usług na innego.

Będzie to możliwe wtedy, kiedy: przetwarzanie jest automatyczne (komputerowe) oraz dane przetwarza się w celu zawarcia bądź realizacji umowy (dane zwykłe), bądź na podstawie zgody (dane wrażliwe i dane zwykłe).

Można zastanawiać się, dlaczego takie prawo znalazło się w ustawie o ochronie danych osobowych. Z odpowiedzią przychodzi opracowanie Grupy Roboczej Art. 29 zatytułowane *„Wytyczne dotyczące prawa do przenoszenia danych”*.[16] I – jak się okazuje – celem przenoszenia danych jest nie ochrona danych, ale ułatwienie zamiany jednego dostawcy usług na innego, w ten sposób zwiększając konkurencję wśród dostawców usług (ułatwiając osobom zmianę dostawców usług). Umożliwia ono tworzenie nowych usług w kontekście strategii jednolitego rynku cyfrowego. Przenoszenie ma też na celu tworzenie „interoperacyjnych systemów, a nie kompatybilnych systemów”, w Wytycznych czytamy, że chodzi o możliwość łatwego przenoszenia, kopiowania lub przesyłania danych osobowych z jednego środowiska IT do innego.[17]

Wydawałoby się, że adresatem takich wymagań są głównie serwisy społecznościowe, przykładowo dzisiaj Facebook pozwala wykonać i ściągnąć kopię swoich danych, okazuje się jednak, że to wymaganie dotyczy bardzo wiele podmiotów, np. banki czy zakłady ubezpieczeń. W Wytycznych czytamy, że administratorzy danych powinni zacząć opracowywać środki, które przyczynią się do udzielania odpowiedzi na wnioski o przeniesienie danych, takie jak narzędzia do pobieraniai interfejsy programowania aplikacji (Application Programming Interfaces - API). Powinni oni zagwarantować, że dane osobowe będą przekazywane w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, oraz powinni być zachęcani do zapewnienia interoperacyjności formatu danych przekazywanych w ramach realizacji wniosku o przeniesienie danych.

Artykuł 12 ust. 3 podkreśla, że dane należy przekazać, *„bez zbędnej zwłoki”* lub *„w terminie miesiąca od otrzymania żądania”* lub w ciągu maksymalnie trzech miesięcy w przypadku naprawdę skomplikowanych spraw, pod warunkiem, że poinformuje się osobę o przyczynach takiego odległego terminu. Trzeba też pamiętać, że o prawie do przenoszenia danych trzeba informować podczas zbierania danych (art. 13 i 14 ust. 2 pkt c).



[15] Zdaniem autora ocenę skutków dla ochrony danych warto przeprowadzić dla każdego procesu przetwarzania, choćby po to, aby ocenić, czy przetwarzanie na pewno nie podowuje „z dużym prawdopodobieństwem” wysokiego ryzyka dla praw i wolności osób fizycznych. Ponadto trzeba będzie wykazać w jaki sposób doszło się do oceny – zatem ocena skutków zawsze będzie pozwalała wykazać w jaki sposób zapewniło się zgodność z przepisami.

[16] http://www.giodo.gov.pl/1520282/id_art/9741/j/pl/

[17] Wytyczne dotyczące prawa do przenoszenia na stronie 14.

INSPEKTOR OCHRONY DANYCH

Polskie przepisy od pewnego czasu przygotowywały nas do nowych obowiązków związanych z nadzorem administratora bezpieczeństwa informacji (ABI) nad przestrzeganiem przepisów o ochronie danych osobowych. Nie bez powodu projekt ustawy o ochronie danych osobowych zakłada, że obecni administratorzy bezpieczeństwa informacji, staną się automatycznie inspektorami ochrony danych, *„do tego czasu, każdy z inspektorów ochrony danych ma czas na podjęcie decyzji o dalszym pełnieniu takiej funkcji (i dokonaniu stosowanego zawiadomienia do Prezesa Urzędu). W razie braku do tego czasu jakiejkolwiek aktywności z ich strony, w dniu 1 września 2018 r. z mocy prawa przestaną pełnić funkcję inspektorów ochrony danych".*[18]

Polskie przepisy nie nakazywały powoływać ABI, była to rola całkowicie opcjonalna, a Rozporządzenie to zmienia, bo w niektórych przypadkach jego powołanie będzie obowiązkowe, np. gdy:

1	przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w ramach sprawowania przez nie wymiaru sprawiedliwości, albo
2	główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania podmiotów danych na dużą skalę, albo
3	główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę danych osobowych szczególnych kategorii, o których mowa w art. 9 ust. 1, oraz danych o wyrokach skazujących za przestępstwa i o przestępstwach, o których mowa w art. 9a.

Zmiana polega też na nowym „tytule" - zrezygnowano z administratora na rzecz inspektora ochrony danych. W literaturze angielskojęzycznej spotyka się jeszcze określenie „data privacy officer" (DPO). Należy zwrócić uwagę na to, że także zleceniobiorcy (podmioty przetwarzające) będą musieli wyznaczać inspektora ochrony danych, w przypadku zaistnienia jednego z powyższych czynników.

Inspektor ochrony danych zamiast administratora bezpieczeństwa informacji.

Grupa robocza art. 29 w połowie grudnia 2016 r. opublikowała *„Wytyczne dotyczące inspektorów ochrony danych (»DPO«)"* [19] Dokument ten rozwiewa wiele wątpliwości związanych z tym kiedy dokładnie należy powołać inspektora. Przykładowo trzeba go powołać, gdy główna działalność (…) polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych. W przypadku szpitala główną działalnością jest zapewnianie opieki medycznej, ale jej efektywne prowadzenie

„nie byłoby możliwe bez przetwarzania danych medycznych, jak np. historii choroby pacjenta. W związku z tym działalność polegająca na przetwarzaniu historii choroby pacjenta również powinna zostać zaklasyfikowana jako działalność główna. Oznacza to, że szpitale będą miały obowiązek powołania DPO."

Z tych wytycznych dowiadujemy się także m.in. że: jeśli z przepisów nie wynika, że trzeba powołać DPO, to **warto udokumentować tego rodzaju decyzję**, **można dobrowolnie powołać DPO**, nawet jeśli takiego obowiązku nie ma, **DPO powinien brać udział w spotkaniach przedstawicieli wyższego i średniego szczebla** organizacji, zaleca się inspektorowi „ustalanie priorytetów w swojej pracy i koncentrowania się na aspektach pociągających za sobą większe ryzyko".

Wytyczne podkreślają, że „administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów." Oznacza to, że inspektor nie może zajmować w organizacji stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych. W Wytycznych zauważa się, że „za powodujące konflikt interesów uważane będą stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT)". Oznaczałoby to, że większość dyrektorów, którzy mają coś wspólnego z przetwarzaniem danych - nie mogą być inspektorami ochrony danych.

W określonych przypadkach także procesorzy muszą powołać inspektora ochrony danych.

Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy, co w Polsce nie jest nowością, bo już dzisiaj administratora bezpieczeństwa trzeba zgłaszać do rejestracji w GIODO. Informacje o sposobie kontaktu z inspektorem trzeba będzie podawać podczas zbierania danych osobowych.

Rozporządzenie określa, że osoby, których dane się przetwarza, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych oraz z korzystaniem z praw przysługujących im na mocy niniejszego rozporządzenia.

Osoby będą mogły kontaktować się bezpośrednio z inspektorem ochrony danych.

Trzeba pamiętać, że tam, gdzie inspektor będzie powołany, osoby, których dane się przetwarza, będą mogły się z nim bezpośrednio kontaktować. Rozporządzenie nie określa, jakie dane kontaktowe inspektora trzeba będzie podać. Nie ma obowiązku podawania jego imienia i nazwiska, chociaż zaleca się, aby to były takie dane, które pozwolą na nawiązanie kontaktu w łatwy sposób. Bardzo możliwe, że wystarczy bezpośredni adres mailowy. Nie tylko jego dane będą musiały znaleźć się na formularzach zgody, będzie on musiał mieć odpowiednie zasoby do interakcji z klientami tak, aby móc odpisywać na ich pisma bądź udzielać telefonicznych wyjaśnień.

Inspektora ochrony danych należy zaangażować, dokonując oceny skutków przetwarzania danych, o której mowa w art. 35 ust. 1 Rozporządzenia (np. gdy przetwarza się szczególne kategorie danych na dużą skalę), oczywiście, jeżeli został on wyznaczony.

Pojawiają się też jednak ułatwienia. Grupa przedsiębiorstw będzie mogła powołać jednego inspektora ochrony danych pod warunkiem, że z każdej siedziby będzie można się z nim łatwo skontaktować. Inspektor może być pracownikiem lub wykonywać zadania na podstawie umowy o świadczenie usług. Trzeba jednak podkreślić, że w każdym przypadku należy zapewnić mu zasoby niezbędne do podtrzymania jego wiedzy fachowej. To bez wątpienia dobra nowina dla inspektorów (w końcu ktoś podkreślił wyraźnie, że muszą się rozwijać zawodowo), a mniej dobra dla administratorów – teraz będą musieli uwzględnić plany rozwoju inspektorów i znaleźć na nie środki finansowe.

Nic nie stoi na przeszkodzie, aby funkcję inspektora ochrony danych pełnił podmiot zewnętrzny, Rozporządzenie zezwala na taki outsourcing i prawdopodobnie będzie to najlepsze rozwiązanie szczególnie dla tych podmiotów, które nigdy wcześniej nie powoływały administratora bezpieczeństwa informacji.

[18] https://mc.gov.pl/aktualnosci/projekt-ustawy-o-ochronie-danych-osobowych

[19] http://www.giodo.gov.pl/456/id_art/9694/j/pl

NOWE OBOWIĄZKI I OGRANICZENIA DLA PODMIOTÓW WSPÓŁPRACUJĄCYCH

Rozporządzenie wprowadza wiele nowych obowiązków dla podmiotów przetwarzających dane w imieniu administratora. Rewolucyjnym obowiązkiem jest konieczność wybierania sobie godnych zaufania partnerów – art. 28 ust. 1 określa, że administrator „korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą".

Rozporządzenie dodaje też, że bez zgody nie wolno powierzać dalej przetwarzania danych osobowych – podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.

Podmiot przetwarzający (procesor) w razie stwierdzenia, iż doszło do naruszenia ochrony danych osobowych, zgłasza je administratorowi (art. 33 ust. 2 Rozporządzenia) i nie musi ich zgłaszać do UODO. Już wcześniej umowa z podmiotem przetwarzającym dane osobowe w imieniu administratora (procesorem) musiała być zawarta na piśmie (art. 31 ust. 1 ustawy o ochronie danych osobowych). Rozporządzenie dodaje, że może to być forma elektroniczna.

Obowiązkiem podmiotu przetwarzającego będzie prowadzenie rejestru wszelkich kategorii czynności przetwarzania, dokonywanych w imieniu administratora. Procesor będzie miał również obowiązek udostępnić taki rejestr na żądanie organu nadzorczego, a także powołać inspektora ochrony danych osobowych, jeśli zaistnieje przynajmniej jeden z czynników, o których stanowi art. 37 ust. 1 Rozporządzenia. Na plus warto zaliczyć fakt dokładnego sprecyzowania obowiązków wszystkich stron. Wcześniej takie zobowiązania trzeba było formułować samodzielnie i nie zawsze pamiętano o wszystkich kluczowych elementach, które powinny znaleźć się w prawidłowo skonstruowanej umowie powierzenia.

Administrator musi wyrażać zgodę na dalsze powierzanie przetwarzania.

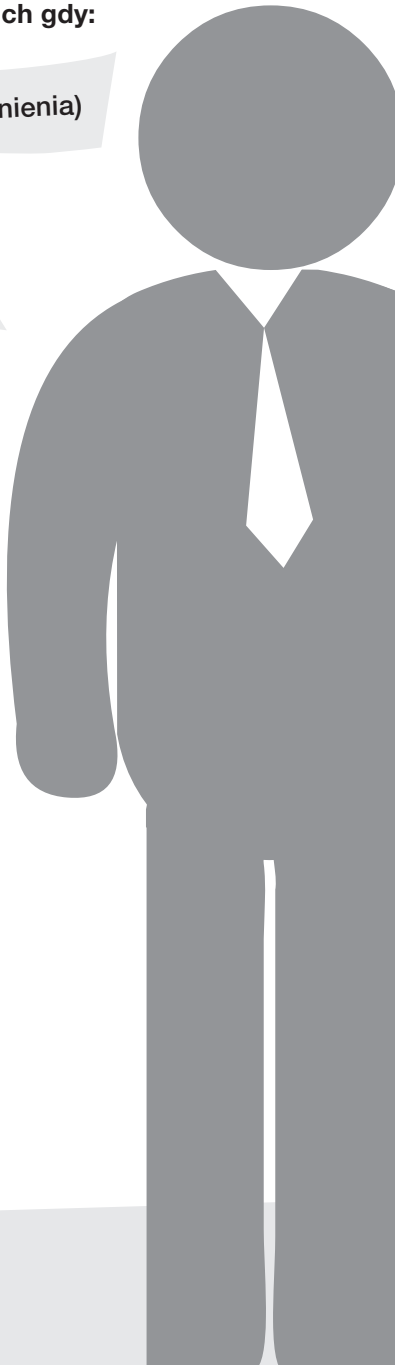
Rozporządzenie wyraźnie podkreśla, że jeżeli podmiot przetwarzający naruszy niniejsze rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania (ale to nie wyklucza stosowania przepisów art. 82, 83 i 84 – poświęconych sankcjom, karom, odszkodowaniom i odpowiedzialności). Oznacza to na przykład, że jeśli zakład ubezpieczeń powierzy dane agentowi oferującemu ubezpieczenia, a on zmieni pierwotny cel przetwarzania i wykorzysta te dane osobowe, żeby zaoferować konsumentom zupełnie inne produkty i usługi, niż te z oferty ubezpieczyciela, to agent automatycznie stanie się odrębnym administratorem tych danych. Taki stan obowiązywał już wcześniej, ale nie jako bezpośredni zapis prawny, a efekt interpretacji przepisów. To kolejny dowód na to, że Rozporządzenie zostało napisane przystępnym językiem oraz w taki sposób, aby wyjaśniać i regulować kwestie niejasne i wymagające wcześniej interpretacji. Przygotowując się do zapewnienia zgodności z Rozporządzeniem trzeba zinwentaryzować wszystkie przypadki powierzenia przetwarzania danych, zapewnić, że umowy są na piśmie oraz ocenić w jakim stopniu regulują kwestie zdefiniowane przez Rozporządzenie. Jeśli okaże się, że umowy nie zawierają wszystkich wymagany elementów, powinny zostać zmienione (aneksowane).

USUWANIE DANYCH

Rozporządzenie bardzo dobitnie podkreśla potrzebę usuwania danych, wzmacniając ją prawem do zapomnienia. Konieczność usuwania danych była już wcześniej obecna w polskich przepisach, ale nie była tak wyraźnie akcentowania i być może dlatego nie przykładano do niej specjalnej wagi. To zagadnienie często określa się mianem „retencji danych".[20]

Dane osobowe będą musiały być usuwane głównie w takich sytuacjach gdy:

- kiedy osoba zwróci się z wnioskiem o ich usunięcie (prawo do zapomnienia)
- dane miały charakter tymczasowy, doraźny
- cel przetwarzania zostanie osiągnięty



Osiągnięcie celu przetwarzania

Rozporządzenie w wielu miejscach akcentuje potrzebę usuwania danych. Motyw 39 Rozporządzenia podpowiada, że „aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu". Ponadto podczas zbierania danych osobowych „administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania: (…) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu". Można by żartobliwie powiedzieć, że dane osobowe będą mieć teraz swojego rodzaju datę przydatności do spożycia.

Oznacza to, że konieczne będzie ustalenie jak długo różne dane osobowe będą przechowywane. Niekiedy będzie to dość łatwe. Przykładowo dane przetwarzane na podstawie zgody osoby można przetwarzać, dopóki nie wygaśnie cel, dla którego dane zostały zebrane lub do czasu odwołania zgody, więc dane zebrane w celu wysyłki firmowego newslettera będą „ważne" do czasu odwołania udzielonej zgody lub do momentu zaprzestania wysyłki.

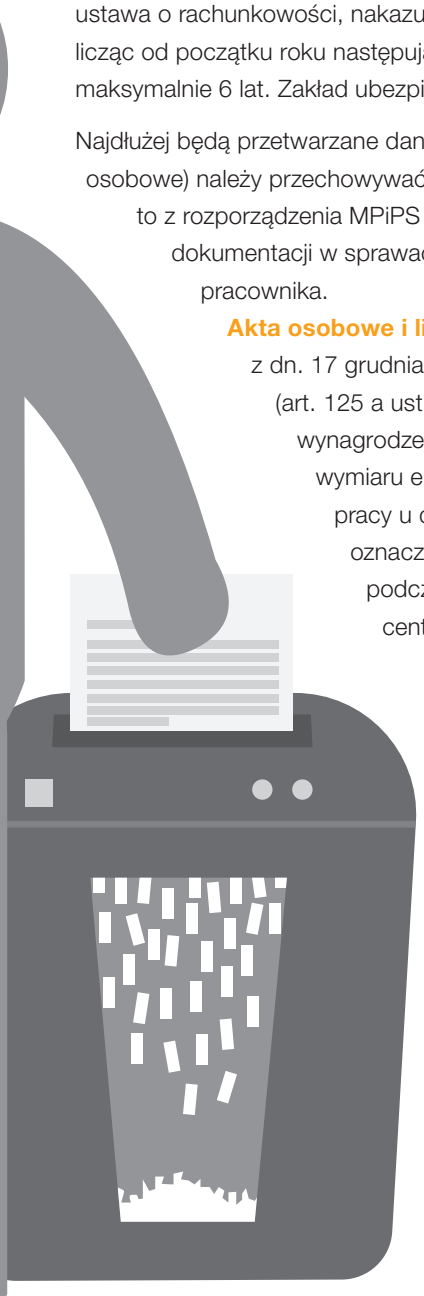
[20] Znaczenie polskiego słowa retencja jest ograniczone i posługując się nim należałoby wyjść od definicji angielskojęzycznej, w której *retention* oznacza ciągłe posiadanie i kontrolę nad czymś.

Ale może to być też dość skomplikowane. Przykładowo dane osobowe klienta w związku z zawartą z nim umową co prawda „wygasną" po rozwiązaniu tej umowy , ale będą musiały być przechowywane z powodów takich jak potencjalne roszczenia oraz przepisy podatkowe (ustawa o rachunkowości, ustawa o przeciwdziałaniu praniu brudnych pieniędzy, etc.) – czyli ok. do 6 lat po rozwiązaniu umowy.

W przypadku polisy ubezpieczeniowej okres ewentualnych roszczeń wynikających z prawnych uwarunkowań to 3 lata od wydania decyzji przez zakład ubezpieczeń w przedmiocie przyznania lub odmowy świadczenia, natomiast dla polisy ubezpieczeniowej OC wskazane jest przechowywanie danych przez możliwy dla zgłoszenia roszczenia (w związku z czynami niedozwolonymi) okres, tj. minimum 20 lat. Na ten okres nakłada się jeszcze ustawa o rachunkowości, nakazująca, aby większość dokumentów księgowych była przechowywana przez 5 lat, licząc od początku roku następującego po roku obrotowym, którego dane dotyczą, co w efekcie może stanowić maksymalnie 6 lat. Zakład ubezpieczeń niektóre dane osobowe będzie musiał więc przechowywać aż przez 26 lat!

Najdłużej będą przetwarzane dane osobowe pracowników. Dokumentację dotycząca zatrudnienia (m. in. akta osobowe) należy przechowywać 50 lat licząc od 1 stycznia roku następnego po dacie ich wytworzenia. Wynika to z rozporządzenia MPiPS z 28 maja 1996 r., określającego zakres prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposób prowadzenia akt osobowych pracownika.

Akta osobowe i listy płac trzeba przechowywać 50 lat. Dodatkowo, na mocy ustawy z dn. 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (art. 125 a ust. 4) „płatnik składek jest zobowiązany przechowywać listy płac, karty wynagrodzeń albo inne dowody, na podstawie których następuje ustalenie podstawy wymiaru emerytury lub renty, przez okres 50 lat od dnia zakończenia przez ubezpieczonego pracy u danego płatnika". Obowiązek informowania o terminach przechowywania danych oznacza też konieczność modyfikacji wszystkich komunikatów przekazywanych klientom podczas zbierania danych – będą to rozmaite formularze, umowy i – głównie w call center – komunikaty głosowe.



Prawo do bycia zapomnianym

Co do zasady „niepotrzebne" dane osobowe trzeba usunąć jak tylko ustaną przesłanki za tym, aby je przechowywać. Rozporządzenie idzie dalej i daje każdej osobie „prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe" w przypadkach gdy:

- dane osobowe już nie są niezbędne do osiągnięcia celu przetwarzania,
- odwołana została zgoda,
- osoba sprzeciwia się marketingowi własnych towarów i usług,
- dane osobowe były przetwarzane niezgodnie z prawem,
- dane osobowe przetwarzano (upraszczając) w serwisach społecznościowych takich jak np. Facebook.

Trzeba wspomnieć, że prawo do usunięcia danych nie jest niczym specjalnie nowym, podobne przepisy obowiązywały już wcześniej w polskim prawie (art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych), ale miało mniejszy zakres, no i – co już było wielokrotnie podkreślane – mało kto przykładał się do zapewnienia z nimi zgodności, z powodu niskich kar.

Bardzo ciekawe jest wymaganie by administrator, który „upublicznił dane osobowe, a na mocy ust. 1 ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje". Szczególnie uciążliwe może być stosowanie tego wymagania przez firmy zajmujące się obrotem danych osobowych, bo takie żądanie osoby będą musiały przekazać wszystkim podmiotom, które dane „kupiły".

Jeśli chodzi o roszczenia to Rozporządzenie wprost podpowiada, że prawo do usunięcia danych („prawo do bycia zapomnianym") nie ma zastosowania „w zakresie w jakim przetwarzanie jest niezbędne (…) do ustalenia, dochodzenia lub obrony roszczeń" (art. 17 ust. 3)

Dane w systemach informatycznych

W systemach informatycznych zamiast usuwania stosuje się anonimizowanie danych osobowych, określane też mianem zamazywania danych albo depersonalizacją danych osobowych. Polega to na tym, że modyfikuje się dane osobowe tak, aby nie pozwalały na identyfikację osoby lub kontakt z nią. A jak wiemy, dane osobowe pozbawione możliwości identyfikacji osoby, której dotyczą, przestają być danymi osobowymi, a to w efekcie z punktu widzenia prawa tożsame jest z usunięciem danych osobowych. Zatem jeśli mówi się o usuwaniu danych osobowych, to może w grę wchodzić prawdziwe usuwanie lub anonimizacja.

Anonimizować można na wiele sposobów. Dość popularne jest mieszanie danych – losuje się imię, nazwisko, ulicę, miejscowość.

Jeśli organizacja zdecyduje się na anonimizowanie danych, to trzeba pamiętać, aby rekord (zapis) dotyczący osoby (klienta) zawierał dodatkowo informację czy zawarte w nim dane są prawdziwe czy też zanonimizowane. W końcu "pomieszane" dane wyglądają tak samo jak prawdziwe.

Warto zwrócić uwagę, że Rozporządzenie zauważa też dane anonimowe już w samej preambule (motyw 26). Czytamy w niej, że: zasady ochrony danych nie powinny więc mieć zastosowania do informacji anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować. Niniejsze rozporządzenie nie dotyczy więc przetwarzania takich anonimowych informacji, w tym przetwarzania do celów statystycznych lub naukowych.

Anonimizacja jest obecna w polskich przepisach od pewnego czasu. Przykładowo zarządzeniem nr 12/2008 Pierwszego Prezesa Sądu Najwyższego z dn. 15 kwietnia 2008 r. w sprawie anonimizacji orzeczeń i zarządzeń wydawanych w Sądzie Najwyższym oraz wokand Sądu Najwyższego:

§ 1. Ustala się następujące zasady anonimizacji orzeczeń i zarządzeń wydanych w Sądzie Najwyższym:

1) Anonimizacja nazwisk, pseudonimów i nazw

a) nazwiska stron postępowania i innych uczestników postępowania, a także ich pseudonimy należy usunąć pozostawiając imię i pierwszą literę nazwiska, np. Jan Nowak - po anonimizacji: Jan N.;

b) zasady określone w punkcie a) stosuje się również, gdy imię i nazwisko stanowi część nazwy spółki, przedsiębiorstwa lub innych podmiotów obrotu prawnego, nie będących osobami fizycznymi;

c) w przypadku występowania w sprawie imion i nazwisk takich samych lub zaczynających się na takie same litery, np. Jan Nowak i Jan Nowak lub Joanna Niegocka i Janusz Nawrocki, wówczas pierwszą osobę oznaczamy jako J.N., a drugą jako X.Y.

Niszczenie nośników danych

Nie można pominąć niszczenia nośników danych. Gdy zapadały się budynki World Trade Center, 11 września 2001 roku, tysiące ton ciężaru sprasowały, połamały i pogniotły znajdujące się w środku komputery wraz z dyskami twardymi. Wysoka temperatura pożarów i woda, którą je gaszono dodatkowo poniszczyła talerze dysków. A jak się okazuje, mimo takich uszkodzeń dało coś się odzyskać z tych nośników. I to jeszcze kilkanaście lat temu, w 2001 roku![21] Sprzedając komputery czy serwery należy pamiętać, że usunięcie danych i sformatowanie, nawet kilkukrotne dysków, tak naprawdę nic nie usuwa. Formatowanie dysku, nie usuwa żadnych danych. Wynika to z tego, że usuwanie ze względów wydajnościowych uproszczono do zaznaczenia pliku jako usuniętego, poinformowanie systemu, że miejsce po nim można będzie wykorzystać. Formatowanie działa podobnie, przygotowuje dysk do pracy i usuwa jedynie tzw. znaczniki danych, nie naruszając samych danych. Aby pliki zostały usunięte, miejsce po nich musi zostać nadpisane. W starszych dyskach aby skutecznie usunąć pliki, należało miejsce po nich nadpisywać kilka razy, dzisiaj już to nie ma takiego znaczenia, jednokrotne nadpisanie wystarczy. Jak nadpisywać? Najlepiej użyć programu, który służy do zamazywania. Bardzo często jest on częścią pakietów oprogramowania do zabezpieczania komputera. Można też wykorzystać do tego darmowe oprogramowanie takie jak Eraser[22] czy Hard Disk Scrubber[23]. Można by powiedzieć, że takie programy są dla plików tym, czym niszczarki dla papieru. Nośniki takie jak płyty CD-ROM czy DVD oraz taśmy magnetyczne najlepiej niszczyć za pomocą specjalnych niszczarek. W ostateczności można je przeciąć nożyczkami, pamiętajmy jednak że im bardziej poufne dane, tym lepszej metody trzeba użyć.

Należy też pamiętać, że niektóre programy także nie kasują danych – wiele systemów finansowych czy też typu CRM zamiast usuwać dane „zaznacza" je jako usunięte. Podobnie ma się rzecz w przypadku baz danych – przykładowo w przypadku bazy Microsoft SQL dane z tabel można usuwać m.in. poleceniami **DELETE** oraz **TRUNCATE TABLE**. Pierwsze z nich usuwa dane przenosząc je do logu transakcyjnego, skąd można operację usunięcia cofnąć, drugie usuwa je nieodwołalnie.

[21] http://www.rediff.com/money/2001/dec/17wtc.htm
oraz http://www.foxnews.com/story/2001/12/17/german-firm-probes-final-world-trade-center-deals.html

[22] https://sourceforge.net/projects/eraser

[23] https://privacyroot.com/software/www/en/wipe-download.php

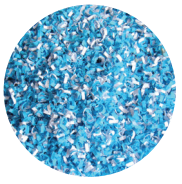
Niszczenie dokumentów papierowych

Dokumenty zawierające dane osobowe, które nie są już potrzebne powinny zostać przed wyrzuceniem skutecznie zniszczone. Nie wystarczy przedrzeć je na kilka części. Taki dokument można łatwo odzyskać i odczytać z niego dane. Najwygodniejszym sposobem jest skorzystanie z niszczarek dokumentów. Wybierając niszczarkę warto zwrócić uwagę na stopień zabezpieczenia zniszczonych dokumentów. Pomóc może w tym niemiecka norma przemysłowa DIN 66399 obowiązująca od października 2012 roku. Reguluje ona wielkość mechanicznie zniszczonych nośników danych. Im wyższy stopień tym trudniej odczytać zniszczone dokumenty.

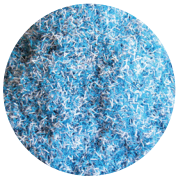
P-1 & P-2

P-3

P-4



P-5

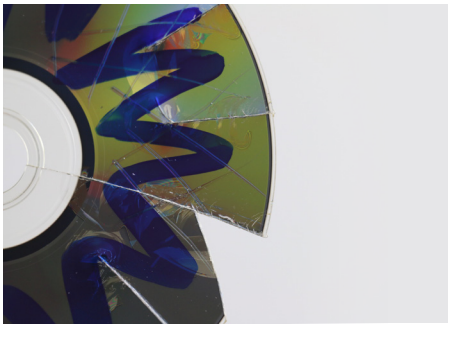


P-6

P-7

WYS. BEZPIECZEŃSTWO **POZIOM DIN P-7**	Dla dokumentów ściśle poufnych wymagających zabezpieczeń na najwyższym poziomie
CIĘCIE NA SUPERMICROŚCINKI **POZIOM DIN P-6**	Dla wymagań związanych z wysokim poziomem bezpieczeństwa, np. rządowych
CIĘCIE NA MICROŚCINKI **POZIOM DIN P-5**	Dla dokumentów o wysokim poziomie poufności. Praktycznie niemożliwe do zebrania i odczytania
CIĘCIE NA ŚCINKI **POZIOM DIN P-4**	Dla dokumentów poufnych. Trudne do zebrania i odczytania
CIĘCIE NA ŚCINKI **POZIOM DIN P-3**	Dla dokumentów poufnych. Trudne do zebrania i odczytania.
CIĘCIE NA PASKI **POZIOMY DIN P-1 i P-2**	Zapewnia podstawowe bezpieczeństwo dokumentów

* Powyższe poziomy zabezpieczeń są zgodne z normą DIN 66399 i odnoszą się wyłącznie do niszczenia papieru



Przykład płyty CD-ROM zniszczonej niszczarką oraz domowymi sposobami

Zapasowe kopie danych

W przypadku zapasowych kopii danych tylko teoretycznie powinno usuwać się z nich dane osobowe, gdyż uważa się przecież, że przechowywanie danych osobowych to także przetwarzanie. Należy jednak brać pod uwagę, że celem wykonywania zapasowych kopii danych nie jest przetwarzanie danych osobowych jako takie, ale zapewnienie sobie możliwości odtworzenia systemów informatycznych na wypadek ich awarii. Stanowią też spełnienie obowiązku wynikającego z prawa np. z ustawy o rachunkowości. Dlatego zapasowej kopii danych nie powinno się modyfikować, bo jeśli dane na niej zostaną zmienione, stracą swoją integralność i kopia stanie się bezużyteczna. Należy jednak koniecznie zadbać o to, aby wdrożyć procedury, zapobiegające ewentualnemu odtworzeniu tych danych osobowych z kopii zapasowej, które zostały kiedyś już usunięte.

PROGRAM BUDOWANIA ŚWIADOMOŚCI / EDUKACJA

To bardzo ważny element w organizacji ochrony danych osobowych. Najlepsze nawet zabezpieczenia będą nieskuteczne, jeśli pracownicy nie będą wiedzieć, jak z nimi postępować.

Ataki takie jak np. phishing czy stosowanie socjotechnik odnoszą sukces głównie z braku świadomości bezpieczeństwa. Przykładem phishingu może być mail, w którym znajduje się link kierujący na stronę internetową, która udaje np. rzeczywisty bank internetowy, a w rzeczywistości przechwytuje wpisywane tam przez ofiary ataku informacje. Najczęściej w mailu znajduje się informacja o rzekomej konieczności podania danych w celu ich weryfikacji, bo inaczej konto zostanie zablokowane. Socjotechniką będzie np. telefon do pracownika, rzekomo od prezesa firmy, który żąda podania hasła. Widać, że to są ataki, przed którymi można bronić się jedynie szkoląc użytkowników, pokazując im co wolno robić, jak dane przetwarzać i co jest zabronione.

Ponadto, jeśli dojdzie do naruszenia przepisów i przedsiębiorca zechce pociągnąć pracownika do odpowiedzialności, to nieprzeszkolony pracownik może argumentować, że nie wiedział jak ma postępować, gdyż nie miał szkolenia. Dlatego dla bezpieczeństwa warto chociażby w ramach szkolenia stanowiskowego przedstawić zasady bezpiecznego przetwarzania danych osobowych i udokumentować ten fakt stosownym oświadczeniem pracownika.

Szkolenie pracowników będzie obowiązkiem inspektora ochrony danych. Jeśli w organizacji powołano inspektora ochrony danych, ciężar działań zwiększających świadomość oraz „szkolenia personelu uczestniczącego w operacjach przetwarzania" będą ciążyć na nim (art. 39 ust. 1 lit b).

ZAKOŃCZENIE

Rozporządzenie obejmuje bardzo szeroką materię i na temat praktycznego jej stosowania można by napisać właściwie kilka książek. Celem tego poradnika było przedstawienie najbardziej interesujących i praktycznych aspektów stosowania nowych przepisów.

Więcej informacji na temat ochrony danych osobowych dostępnych jest na **www.ochronatozsamosci.pl**

oraz na naszym Facebooku **www.facebook.com/chronswojatozsamosc**