Istota i praktyka ochrony danych osobowych

Zmiany 2015, nowe przepisy wykonawcze, nowe obowiązki

Problemy organizacyjne, prawne i techniczne gromadzenia danych osobowych (obowiązki, uprawnienia, procedury, dokumenty, działania, zagrożenia, …)

Wybór treści szkoleniowych

Wszystkie części składowe tego skryptu są dostępne w wersji elektronicznej

Materiały szkoleniowe (w. 7.25 / 03.10.2015)

Krzysztof Sługocki

Krzysztof.Slugocki@gmail.com

Facebook.com/Krzysztof.Slugocki

sites.google.com/site/KrzysztofSlugocki
slideshare.net/eGocki
prezi.com/user/eGocki
art30a.ucoz.pl

Zawartość

Nota redakcyjna

Na potrzeby szkolenia treści zawarte w tej publikacji będą nazywane skryptem lub opracowaniem.

W przygotowaniu tego skryptu oparto się o opracowania własne oraz wykorzystano i dostosowano treści dostępne na stronach internetowych wybranych ministerstw, systemu ISAP Kancelarii Sejmu RP (http://www.sejm.gov.pl , http://isap.sejm.gov.pl) oraz GIODO (http://giodo.gov.pl) . **Udostępnione na stronach tego opracowania teksty aktów prawnych nie są źródłami prawa.** Jedynym takim źródłem są publikowane na podstawie ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych aktów prawnych (Dz. U. z 2010 r. Nr 17, poz. 95) akty prawne ogłaszane i wydawane w Dzienniku Ustaw i Monitorze Polskim. Ich wydawcą i dystrybutorem jest Kancelaria Prezesa Rady Ministrów (http://www.rcl.gov.pl) . Teksty aktów prawnych zawarte w tym skrypcie proszę traktować jedynie jako pomoc dydaktyczną i materiał szkoleniowy, informacyjny i pomocniczy wykorzystywany w czasie szkolenia. Opracowania własne zawarte w tym skrypcie (treści i opracowania inne niż teksty aktów prawnych) są udostępniane zgodnie z deklaracją autora co do zgodności z typem licencjowania: http://creativecommons.org/licenses/by/3.0/pl/ i mogą być rozpowszechniane po stosownym oznaczeniu ich informacją zawartą na tej karcie tytułowej (po znaku )

Ustawa o ochronie danych osobowych (+ zmiany od 01.01.2015)

Dz.U.2014.1182

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych **(tekst jednolity + zmiany od 01.01.2015)**

Rozdział 1 Przepisy ogólne

Art. 1. 1. Każdy ma prawo do ochrony dotyczących go danych osobowych.

2. Przetwarzanie danych osobowych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą, lub dobro osób trzecich w zakresie i trybie określonym ustawą.

Art. 2. 1. Ustawa określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych.

2. Ustawę stosuje się do przetwarzania danych osobowych:

1) w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych;

2) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych.

3. W odniesieniu do zbiorów danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji, mają zastosowanie jedynie przepisy rozdziału 5.

Art. 3. 1. Ustawę stosuje się do organów państwowych, organów samorządu terytorialnego oraz do państwowych i komunalnych jednostek organizacyjnych.

2. Ustawę stosuje się również do:

1) podmiotów niepublicznych realizujących zadania publiczne,

2) osób fizycznych i osób prawnych oraz jednostek organizacyjnych niebędących osobami prawnymi, jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych

- które mają siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, albo w państwie trzecim, o ile przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej.

Art. 3a. 1. Ustawy nie stosuje się do:

1) osób fizycznych, które przetwarzają dane wyłącznie w celach osobistych lub domowych;

2) podmiotów mających siedzibę lub miejsce zamieszkania w państwie trzecim, wykorzystujących środki techniczne znajdujące się na terytorium Rzeczypospolitej Polskiej wyłącznie do przekazywania danych.

2. Ustawy, z wyjątkiem przepisów art. 14-19 i art. 36 ust. 1, nie stosuje się również do prasowej działalności dziennikarskiej w rozumieniu ustawy z dnia 26 stycznia 1984 r. - Prawo prasowe (Dz. U. Nr 5, poz. 24, z późn. zm.) oraz do działalności literackiej lub artystycznej, chyba że wolność wyrażania swoich poglądów i rozpowszechniania informacji istotnie narusza prawa i wolności osoby, której dane dotyczą.

Art. 4 . Przepisów ustawy nie stosuje się, jeżeli umowa międzynarodowa, której stroną jest Rzeczpospolita Polska, stanowi inaczej.

Art. 5. Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z niniejszej ustawy, stosuje się przepisy tych ustaw.

Art. 6. 1. W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

2. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

3. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Art. 7. Ilekroć w ustawie jest mowa o:

1) zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

2) przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

2a) systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

2b) zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

3) usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

4) administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych;

5) zgodzie osoby, której dane dotyczą - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie;

6) odbiorcy danych - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

a) osoby, której dane dotyczą,

b) osoby upoważnionej do przetwarzania danych,

c) przedstawiciela, o którym mowa w art. 31a,

d) podmiotu, o którym mowa w art. 31,

e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;

7) państwie trzecim - rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego.

Rozdział 2 Organ ochrony danych osobowych

Art. 8. 1. Organem do spraw ochrony danych osobowych jest Generalny Inspektor Ochrony Danych Osobowych, zwany dalej "Generalnym Inspektorem".

2. Generalnego Inspektora powołuje i odwołuje Sejm Rzeczypospolitej Polskiej za zgodą Senatu.

3. Na stanowisko Generalnego Inspektora może być powołany ten, kto łącznie spełnia następujące warunki:

1) jest obywatelem polskim i stale zamieszkuje na terytorium Rzeczypospolitej Polskiej;

2) wyróżnia się wysokim autorytetem moralnym;

3) posiada wyższe wykształcenie prawnicze oraz odpowiednie doświadczenie zawodowe;

4) nie był karany za przestępstwo.

4. Generalny Inspektor w zakresie wykonywania swoich zadań podlega tylko ustawie.

5. Kadencja Generalnego Inspektora trwa 4 lata, licząc od dnia złożenia ślubowania. Po upływie kadencji Generalny Inspektor pełni swoje obowiązki do czasu objęcia stanowiska przez nowego Generalnego Inspektora.

6. Ta sama osoba nie może być Generalnym Inspektorem więcej niż przez dwie kadencje.

7. Kadencja Generalnego Inspektora wygasa z chwilą jego śmierci, odwołania lub utraty obywatelstwa polskiego.

8. Sejm, za zgodą Senatu, odwołuje Generalnego Inspektora, jeżeli:

1) zrzekł się stanowiska;

2) stał się trwale niezdolny do pełnienia obowiązków na skutek choroby;

3) sprzeniewierzył się złożonemu ślubowaniu;

4) został skazany prawomocnym wyrokiem sądu za popełnienie przestępstwa.

Art. 9. Przed przystąpieniem do wykonywania obowiązków Generalny Inspektor składa przed Sejmem następujące ślubowanie:

"Obejmując stanowisko Generalnego Inspektora Ochrony Danych Osobowych uroczyście ślubuję dochować wierności postanowieniom Konstytucji Rzeczypospolitej Polskiej, strzec prawa do ochrony danych osobowych, a powierzone mi obowiązki wypełniać sumiennie i bezstronnie."

Ślubowanie może być złożone z dodaniem słów "Tak mi dopomóż Bóg".

Art. 10. 1. Generalny Inspektor nie może zajmować innego stanowiska, z wyjątkiem stanowiska profesora szkoły wyższej, ani wykonywać innych zajęć zawodowych.

2. Generalny Inspektor nie może należeć do partii politycznej, związku zawodowego ani prowadzić działalności publicznej niedającej się pogodzić z godnością jego urzędu.

Art. 11. Generalny Inspektor nie może być bez uprzedniej zgody Sejmu pociągnięty do odpowiedzialności karnej ani pozbawiony wolności. Generalny Inspektor nie może być zatrzymany lub aresztowany, z wyjątkiem ujęcia go na gorącym uczynku przestępstwa i jeżeli jego zatrzymanie jest niezbędne do zapewnienia prawidłowego toku postępowania. O zatrzymaniu niezwłocznie powiadamia się Marszałka Sejmu, który może nakazać natychmiastowe zwolnienie zatrzymanego.

Art. 12. Do zadań Generalnego Inspektora w szczególności należy:

1) kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych;

2) wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych;

3) zapewnienie wykonania przez zobowiązanych obowiązków o charakterze niepieniężnym wynikających z decyzji, o których mowa w pkt 2, przez stosowanie środków egzekucyjnych przewidzianych w ustawie z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2012 r. poz. 1015, z późn. zm.);

4) prowadzenie rejestru zbiorów danych oraz udzielanie informacji o zarejestrowanych zbiorach;

1) w art. 12 pkt 4 otrzymuje brzmienie:

„4) prowadzenie rejestru zbiorów danych oraz rejestru administratorów bezpieczeństwa informacji, a także udzielanie informacji o zarejestrowanych zbiorach danych i zarejestrowanych administratorach bezpieczeństwa informacji;”;

5) opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych;

6) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,

7) uczestniczenie w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

Art. 12a. 1. Na wniosek Generalnego Inspektora Marszałek Sejmu może powołać zastępcę Generalnego Inspektora. Odwołanie zastępcy Generalnego Inspektora następuje w tym samym trybie.

2. Generalny Inspektor określa zakres zadań swojego zastępcy.

3. Zastępca Generalnego Inspektora powinien spełniać wymogi określone w art. 8 ust. 3 pkt 1, 2 i 4 oraz posiadać wyższe wykształcenie i odpowiednie doświadczenie zawodowe.

Art. 13. 1. Generalny Inspektor wykonuje swoje zadania przy pomocy Biura Generalnego Inspektora Ochrony Danych Osobowych, zwanego dalej Biurem.

1a. Generalny Inspektor w przypadkach uzasadnionych charakterem i liczbą spraw z zakresu ochrony danych osobowych na danym terenie może wykonywać swoje zadania przy pomocy jednostek zamiejscowych Biura.

2. (uchylony).

3. Prezydent Rzeczypospolitej Polskiej, po zasięgnięciu opinii Generalnego Inspektora, w drodze rozporządzenia, nadaje statut Biuru, określając jego organizację, zasady działania oraz siedziby jednostek zamiejscowych i zakres ich właściwości terytorialnej, mając na uwadze stworzenie optymalnych warunków organizacyjnych do prawidłowej realizacji zadań Biura.

Art. 14. W celu wykonania zadań, o których mowa w art. 12 pkt 1 i 2, Generalny Inspektor, zastępca Generalnego Inspektora lub upoważnieni przez niego pracownicy Biura, zwani dalej "inspektorami", mają prawo:

1) wstępu, w godzinach od 6^{00}do 22^{00}, za okazaniem imiennego upoważnienia i legitymacji służbowej, do pomieszczenia, w którym zlokalizowany jest zbiór danych, oraz pomieszczenia, w którym przetwarzane są dane poza zbiorem danych, i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą;

2) żądać złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przesłuchiwać osoby w zakresie niezbędnym do ustalenia stanu faktycznego;

3) wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii;

4) przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych;

5) zlecać sporządzanie ekspertyz i opinii.

Art. 15. 1. Kierownik kontrolowanej jednostki organizacyjnej oraz kontrolowana osoba fizyczna będąca administratorem danych osobowych są obowiązani umożliwić inspektorowi przeprowadzenie kontroli, a w szczególności umożliwić przeprowadzenie czynności oraz spełnić żądania, o których mowa w art. 14 pkt 1-4.

2. W toku kontroli zbiorów, o których mowa w art. 43 ust. 1 pkt 1a, inspektor przeprowadzający kontrolę ma prawo wglądu do zbioru zawierającego dane osobowe jedynie za pośrednictwem upoważnionego przedstawiciela kontrolowanej jednostki organizacyjnej.

3. Kontrolę przeprowadza się po okazaniu imiennego upoważnienia wraz z legitymacją służbową.

4. Imienne upoważnienie powinno zawierać:

1) wskazanie podstawy prawnej przeprowadzenia kontroli;

2) oznaczenie organu kontroli;

3) imię i nazwisko, stanowisko służbowe osoby upoważnionej do przeprowadzenia kontroli oraz numer jej legitymacji służbowej;

4) określenie zakresu przedmiotowego kontroli;

5) oznaczenie podmiotu objętego kontrolą albo zbioru danych, albo miejsca poddawanego kontroli;

6) wskazanie daty rozpoczęcia i przewidywanego terminu zakończenia kontroli;

7) podpis Generalnego Inspektora;

8) pouczenie kontrolowanego podmiotu o jego prawach i obowiązkach;

9) datę i miejsce wystawienia imiennego upoważnienia.

Art. 16. 1. Z czynności kontrolnych inspektor sporządza protokół, którego jeden egzemplarz doręcza kontrolowanemu administratorowi danych.

1a. Protokół kontroli powinien zawierać:

1) nazwę podmiotu kontrolowanego w pełnym brzmieniu i jego adres;

2) imię i nazwisko, stanowisko służbowe, numer legitymacji służbowej oraz numer upoważnienia inspektora;

3) imię i nazwisko osoby reprezentującej podmiot kontrolowany oraz nazwę organu reprezentującego ten podmiot;

4) datę rozpoczęcia i zakończenia czynności kontrolnych, z wymienieniem dni przerw w kontroli;

5) określenie przedmiotu i zakresu kontroli;

6) opis stanu faktycznego stwierdzonego w toku kontroli oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;

7) wyszczególnienie załączników stanowiących składową część protokołu;

8) omówienie dokonanych w protokole poprawek, skreśleń i uzupełnień;

9) parafy inspektora i osoby reprezentującej podmiot kontrolowany na każdej stronie protokołu;

10) wzmiankę o doręczeniu egzemplarza protokołu osobie reprezentującej podmiot kontrolowany;

11) wzmiankę o wniesieniu lub niewniesieniu zastrzeżeń i uwag do protokołu;

12) datę i miejsce podpisania protokołu przez inspektora oraz przez osobę lub organ reprezentujący podmiot kontrolowany.

2. Protokół podpisują inspektor i kontrolowany administrator danych, który może wnieść do protokołu umotywowane zastrzeżenia i uwagi.

3. W razie odmowy podpisania protokołu przez kontrolowanego administratora danych, inspektor czyni o tym wzmiankę w protokole, a odmawiający podpisu może, w terminie 7 dni, przedstawić swoje stanowisko na piśmie Generalnemu Inspektorowi.

Art. 17. 1. Jeżeli na podstawie wyników kontroli inspektor stwierdzi naruszenie przepisów o ochronie danych osobowych, występuje do Generalnego Inspektora o zastosowanie środków, o których mowa w art. 18.

2. Na podstawie ustaleń kontroli inspektor może żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym dopuszczenia do uchybień i poinformowania go, w określonym terminie, o wynikach tego postępowania i podjętych działaniach.

Art. 18. 1. W przypadku naruszenia przepisów o ochronie danych osobowych Generalny Inspektor z urzędu lub na wniosek osoby zainteresowanej, w drodze decyzji administracyjnej, nakazuje przywrócenie stanu zgodnego z prawem, a w szczególności:

1) usunięcie uchybień;

2) uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych;

3) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe;

4) wstrzymanie przekazywania danych osobowych do państwa trzeciego;

5) zabezpieczenie danych lub przekazanie ich innym podmiotom;

6) usunięcie danych osobowych.

2. Decyzje Generalnego Inspektora, o których mowa w ust. 1, nie mogą ograniczać swobody działania podmiotów zgłaszających kandydatów lub listy kandydatów w wyborach na urząd Prezydenta Rzeczypospolitej Polskiej, do Sejmu, do Senatu i do organów samorządu terytorialnego, a także w wyborach do Parlamentu Europejskiego, pomiędzy dniem zarządzenia wyborów a dniem głosowania.

2a. Decyzje Generalnego Inspektora, o których mowa w ust. 1, w odniesieniu do zbiorów określonych w art. 43 ust. 1 pkt 1a, nie mogą nakazywać usunięcia danych osobowych zebranych w toku czynności operacyjno-rozpoznawczych prowadzonych na podstawie przepisów prawa.

3. W przypadku gdy przepisy innych ustaw regulują odrębnie wykonywanie czynności, o których mowa w ust. 1, stosuje się przepisy tych ustaw.

Art. 19. W razie stwierdzenia, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby fizycznej będącej administratorem danych wyczerpuje znamiona przestępstwa określonego w ustawie, Generalny Inspektor kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.

Art. 19a. 1. W celu realizacji zadań, o których mowa w art. 12 pkt 6, Generalny Inspektor może kierować do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych.

2. Generalny Inspektor może również występować do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie bądź zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych.

3. Podmiot, do którego zostało skierowane wystąpienie lub wniosek, o których mowa w ust. 1 i 2, jest obowiązany ustosunkować się do tego wystąpienia lub wniosku na piśmie w terminie 30 dni od daty jego otrzymania.

2) po art. 19a dodaje się art. 19b w brzmieniu:

„Art. 19b. 1. Generalny Inspektor może zwrócić się do administratora bezpieczeństwa informacji wpisanego do rejestru, o którym mowa w art. 46c, o dokonanie sprawdzenia, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, u administratora danych, który go powołał, wskazując zakres i termin sprawdzenia.

2. Po dokonaniu sprawdzenia, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, administrator bezpieczeństwa informacji, za pośrednictwem administratora danych, przedstawia Generalnemu Inspektorowi sprawozdanie, o którym mowa w art. 36a ust. 2 pkt 1 lit. a.

3. Dokonanie przez administratora bezpieczeństwa informacji sprawdzenia w przypadku, o którym mowa w ust. 1, nie wyłącza prawa Generalnego Inspektora do przeprowadzenia kontroli, o której mowa w art. 12 pkt 1.”;

Art. 20. Generalny Inspektor składa Sejmowi, raz w roku, sprawozdanie ze swojej działalności wraz z wnioskami wynikającymi ze stanu przestrzegania przepisów o ochronie danych osobowych.

Art. 21. 1. Strona może zwrócić się do Generalnego Inspektora z wnioskiem o ponowne rozpatrzenie sprawy.

2. Na decyzję Generalnego Inspektora w przedmiocie wniosku o ponowne rozpatrzenie sprawy stronie przysługuje skarga do sądu administracyjnego.

Art. 22. Postępowanie w sprawach uregulowanych w niniejszej ustawie prowadzi się według przepisów Kodeksu postępowania administracyjnego, o ile przepisy ustawy nie stanowią inaczej.

Art. 22a. Minister właściwy do spraw administracji publicznej określi, w drodze rozporządzenia, wzór upoważnienia i legitymacji służbowej, o których mowa w art. 14 pkt 1, uwzględniając konieczność imiennego wskazania inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych.

Rozdział 3 Zasady przetwarzania danych osobowych

Art. 23. 1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych;

2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;

3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;

4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;

5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

2. Zgoda, o której mowa w ust. 1 pkt 1, może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania.

3. Jeżeli przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a spełnienie warunku określonego w ust. 1 pkt 1 jest niemożliwe, można przetwarzać dane bez zgody tej osoby, do czasu, gdy uzyskanie zgody będzie możliwe.

4. Za prawnie usprawiedliwiony cel, o którym mowa w ust. 1 pkt 5, uważa się w szczególności:

1) marketing bezpośredni własnych produktów lub usług administratora danych;

2) dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

Art. 24. 1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:

1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku;

2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;

3) prawie dostępu do treści swoich danych oraz ich poprawiania;

4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

2. Przepisu ust. 1 nie stosuje się, jeżeli:

1) przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania;

2) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.

Art. 25. 1. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:

1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku;

2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych;

3) źródle danych;

4) prawie dostępu do treści swoich danych oraz ich poprawiania;

5) o uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8.

2. Przepisu ust. 1 nie stosuje się, jeżeli:

1) przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą;

2) (uchylony);

3) dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie wymagań określonych w ust. 1 wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania;

4) (uchylony);

5) dane są przetwarzane przez administratora, o którym mowa w art. 3 ust. 1 i ust. 2 pkt 1, na podstawie przepisów prawa;

6) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.

Art. 26. 1. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były:

1) przetwarzane zgodnie z prawem;

2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2;

3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;

4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

2. Przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje:

1) w celach badań naukowych, dydaktycznych, historycznych lub statystycznych;

2) z zachowaniem przepisów art. 23 i 25.

Art. 26a. 1. Niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym.

2. Przepisu ust. 1 nie stosuje się, jeżeli rozstrzygnięcie zostało podjęte podczas zawierania lub wykonywania umowy i uwzględnia wniosek osoby, której dane dotyczą, albo jeżeli zezwalają na to przepisy prawa, które przewidują również środki ochrony uzasadnionych interesów osoby, której dane dotyczą.

Art. 27. 1. Zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

2. Przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli:

1) osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych;

2) przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony;

3) przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora;

4) jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych;

5) przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem;

6) przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie;

7) przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych;

8) przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą;

9) jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone;

10) przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

Art. 28. 1. (uchylony).

2. Numery porządkowe stosowane w ewidencji ludności mogą zawierać tylko oznaczenie płci, daty urodzenia, numer nadania oraz liczbę kontrolną.

3. Zabronione jest nadawanie ukrytych znaczeń elementom numerów porządkowych w systemach ewidencjonujących osoby fizyczne.

Art. 29. (uchylony).

Art. 30. (uchylony).

Art. 31. 1. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.

2. Podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

3. Podmiot, o którym mowa w ust. 1, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych.

4. W przypadkach, o których mowa w ust. 1-3, odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

5. Do kontroli zgodności przetwarzania danych przez podmiot, o którym mowa w ust. 1, z przepisami o ochronie danych osobowych stosuje się odpowiednio przepisy art. 14-19.

Art. 31a. W przypadku przetwarzania danych osobowych przez podmioty mające siedzibę albo miejsce zamieszkania w państwie trzecim, administrator danych jest obowiązany wyznaczyć swojego przedstawiciela w Rzeczypospolitej Polskiej.

Rozdział 4 Prawa osoby, której dane dotyczą

Art. 32. 1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:

1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy, a w przypadku gdy administratorem danych jest osoba fizyczna - jej miejsca zamieszkania oraz imienia i nazwiska;

2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze;

3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych;

4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej;

5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane;

5a) uzyskania informacji o przesłankach podjęcia rozstrzygnięcia, o którym mowa w art. 26a ust. 2;

6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane;

7) wniesienia, w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację;

8) wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, wymienionych w art. 23 ust. 1 pkt 4 i 5, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych;

9) wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem art. 26a ust. 1.

2. W przypadku wniesienia żądania, o którym mowa w ust. 1 pkt 7, administrator danych zaprzestaje przetwarzania kwestionowanych danych osobowych albo bez zbędnej zwłoki przekazuje żądanie Generalnemu Inspektorowi, który wydaje stosowną decyzję.

3. W razie wniesienia sprzeciwu, o którym mowa ust. 1 pkt 8, dalsze przetwarzanie kwestionowanych danych jest niedopuszczalne. Administrator danych może jednak pozostawić w zbiorze imię lub imiona i nazwisko osoby oraz numer PESEL lub adres wyłącznie w celu uniknięcia ponownego wykorzystania danych tej osoby w celach objętych sprzeciwem.

3a. W razie wniesienia żądania, o którym mowa w art. 32 ust. 1 pkt 9, administrator danych bez zbędnej zwłoki rozpatruje sprawę albo przekazuje ją wraz z uzasadnieniem swojego stanowiska Generalnemu Inspektorowi, który wydaje stosowną decyzję.

4. Jeżeli dane są przetwarzane dla celów naukowych, dydaktycznych, historycznych, statystycznych lub archiwalnych, administrator danych może odstąpić od informowania osób o przetwarzaniu ich danych w przypadkach, gdy pociągałoby to za sobą nakłady niewspółmierne z zamierzonym celem.

5. Osoba zainteresowana może skorzystać z prawa do informacji, o których mowa w ust. 1 pkt 1-5, nie częściej niż raz na 6 miesięcy.

Art. 33. 1. Na wniosek osoby, której dane dotyczą, administrator danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji, o których mowa w art. 32 ust. 1 pkt 1-5a.

2. Na wniosek osoby, której dane dotyczą, informacji, o których mowa w ust. 1, udziela się na piśmie.

Art. 34. Administrator danych odmawia osobie, której dane dotyczą, udzielenia informacji, o których mowa w art. 32 ust. 1 pkt 1-5a, jeżeli spowodowałoby to:

1) ujawnienie wiadomości zawierających informacje niejawne;

2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego;

3) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa;

4) istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.

Art. 35. 1. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy.

2. W razie niedopełnienia przez administratora danych obowiązku, o którym mowa w ust. 1, osoba, której dane dotyczą, może się zwrócić do Generalnego Inspektora z wnioskiem o nakazanie dopełnienia tego obowiązku.

3. Administrator danych jest obowiązany poinformować bez zbędnej zwłoki innych administratorów, którym udostępnił zbiór danych, o dokonanym uaktualnieniu lub sprostowaniu danych.

Rozdział 5 Zabezpieczenie danych osobowych

Art. 36. 1. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.

3. Administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba że sam wykonuje te czynności.

3) w art. 36 uchyla się ust. 3;

4) po art. 36 dodaje się art. 36a–36c w brzmieniu:

„Art. 36a. 1. Administrator danych może powołać administratora bezpieczeństwa informacji.
2. Do zadań administratora bezpieczeństwa informacji należy:
1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,
c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2–4a i 7.
3. Rejestr, o którym mowa w ust. 2 pkt 2, jest jawny. Przepis art. 42 ust. 2 stosuje się odpowiednio.
4. Administrator danych może powierzyć administratorowi bezpieczeństwa informacji wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań, o których mowa w ust. 2.
5. Administratorem bezpieczeństwa informacji może być osoba, która:
1) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;
2) posiada odpowiednią wiedzę w zakresie ochrony danych osobowych;
3) nie była karana za umyślne przestępstwo.
6. Administrator danych może powołać zastępców administratora bezpieczeństwa informacji, którzy spełniają warunki określone w ust. 5.

7. Administrator bezpieczeństwa informacji podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych.
8. Administrator danych zapewnia środki i organizacyjną odrębność administratora bezpieczeństwa informacji niezbędne do niezależnego wykonywania przez niego zadań, o których mowa w ust. 2.
9. Minister właściwy do spraw administracji publicznej określi, w drodze rozporządzenia:
1) tryb i sposób realizacji zadań, o których mowa w ust. 2 pkt 1 lit. a i b,
2) sposób prowadzenia rejestru zbiorów danych, o którym mowa w ust. 2 pkt 2
– uwzględniając konieczność zapewnienia prawidłowości realizacji zadań administratora bezpieczeństwa informacji oraz niezależności i organizacyjnej odrębności w wykonywaniu przez niego zadań.
Art. 36b. W przypadku niepowołania administratora bezpieczeństwa informacji zadania określone w art. 36a ust. 2 pkt 1, z wyłączeniem obowiązku sporządzania sprawozdania, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, wykonuje administrator danych.
Art. 36c. Sprawozdanie, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, powinno zawierać:
1) oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania;
2) imię i nazwisko administratora bezpieczeństwa informacji;
3) wykaz czynności podjętych przez administratora bezpieczeństwa informacji w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach;
4) datę rozpoczęcia i zakończenia sprawdzenia;
5) określenie przedmiotu i zakresu sprawdzenia;
6) opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
7) stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem;
8) wyszczególnienie załączników stanowiących składową część sprawozdania;
9) podpis administratora bezpieczeństwa informacji, a w przypadku sprawozdania w postaci papierowej – dodatkowo parafy administratora bezpieczeństwa informacji na każdej stronie sprawozdania;
10) datę i miejsce podpisania sprawozdania przez administratora bezpieczeństwa informacji.";

Art. 35.
Administrator bezpieczeństwa informacji wyznaczony na podstawie art. 36 ust. 3 ustawy zmienianej w art. 9, w brzmieniu dotychczasowym, pełni funkcję administratora bezpieczeństwa informacji w rozumieniu art. 36a ust. 1 ustawy zmienianej w art. 9, w brzmieniu nadanym niniejszą ustawą, do czasu zgłoszenia go do rejestru, o którym mowa w art. 46c ustawy zmienianej w art. 9, w brzmieniu nadanym niniejszą ustawą, nie dłużej jednak niż do dnia 30 czerwca 2015 r.

Art. 37. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

Art. 38. Administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Art. 39. 1. Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:

1) imię i nazwisko osoby upoważnionej;

2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;

3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

2. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

Art. 39a. Minister właściwy do spraw administracji publicznej w porozumieniu z ministrem właściwym do spraw informatyzacji określi, w drodze rozporządzenia, sposób prowadzenia i zakres dokumentacji, o której mowa w art. 36 ust. 2, oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, uwzględniając zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną, a także wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzanych danych.

Rozdział 6 Rejestracja zbiorów danych osobowych

5) tytuł rozdziału 6 otrzymuje brzmienie:
„Rejestracja zbiorów danych osobowych oraz administratorów bezpieczeństwa informacji";

Art. 40. Administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1.

6) art. 40 otrzymuje brzmienie:
„Art. 40. Administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 i 1a.";

Art. 41. 1. Zgłoszenie zbioru danych do rejestracji powinno zawierać:

1) wniosek o wpisanie zbioru do rejestru zbiorów danych osobowych;

2) oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany, oraz podstawę prawną upoważniającą do prowadzenia zbioru, a w przypadku powierzenia przetwarzania danych podmiotowi, o którym mowa w art. 31, lub wyznaczenia podmiotu, o którym mowa w art. 31a; oznaczenie tego podmiotu i adres jego siedziby lub miejsca zamieszkania,

3) cel przetwarzania danych;

3a) opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych;

4) sposób zbierania oraz udostępniania danych;

4a) informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane;

5) opis środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36-39,

6) informację o sposobie wypełnienia warunków technicznych i organizacyjnych, określonych w przepisach, o których mowa w art. 39a;

7) informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego.

2. Administrator danych jest obowiązany zgłaszać Generalnemu Inspektorowi każdą zmianę informacji, o której mowa w ust. 1, w terminie 30 dni od dnia dokonania zmiany w zbiorze danych, z zastrzeżeniem ust. 3.

3. Jeżeli zmiana informacji, o której mowa w ust. 1 pkt 3a, dotyczy rozszerzenia zakresu przetwarzanych danych o dane, o których mowa w art. 27 ust. 1, administrator danych jest obowiązany do jej zgłoszenia przed dokonaniem zmiany w zbiorze.

4. Do zgłaszania zmian stosuje się odpowiednio przepisy o rejestracji zbiorów danych.

Art. 36. Do postępowań rejestracyjnych prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych na podstawie zgłoszeń, o których mowa w art. 41 ust. 1 i 2 ustawy zmienianej w art. 9, wszczętych i niezakończonych przed dniem wejścia w życie niniejszej ustawy stosuje się przepisy dotychczasowe.

Art. 42. 1. Generalny Inspektor prowadzi ogólnokrajowy, jawny rejestr zbiorów danych osobowych. Rejestr powinien zawierać informacje, o których mowa w art. 41 ust. 1 pkt 1-4a i 7.

2. Każdy ma prawo przeglądać rejestr, o którym mowa w ust. 1.

3. Na żądanie administratora danych może być wydane zaświadczenie o zarejestrowaniu zgłoszonego przez niego zbioru danych, z zastrzeżeniem ust. 4.

4. Generalny Inspektor wydaje administratorowi danych, o których mowa w art. 27 ust. 1, zaświadczenie o zarejestrowaniu zbioru danych niezwłocznie po dokonaniu rejestracji.

Art. 43. 1. Z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych:

1) zawierających informacje niejawne;

1a) które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności;

2) przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym;

2a) przetwarzanych przez Generalnego Inspektora Informacji Finansowej;

2b) przetwarzanych przez właściwe organy na potrzeby udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym;

2c) przetwarzanych przez właściwie organy na podstawie przepisów o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej;

3) dotyczących osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego;

4) przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się;

5) dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta;

6) tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województw, wyborów na urząd Prezydenta Rzeczypospolitej Polskiej, na wójta, burmistrza, prezydenta miasta oraz dotyczących referendum ogólnokrajowego i referendum lokalnego;

7) dotyczących osób pozbawionych wolności na podstawie ustawy, w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności;

8) przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej;

9) powszechnie dostępnych;

10) przetwarzanych w celu przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego;

11) przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.

2. W odniesieniu do zbiorów, o których mowa w ust. 1 pkt 1 i 3, oraz zbiorów, o których mowa w ust. 1 pkt 1a, przetwarzanych przez Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego, Służbę

Wywiadu Wojskowego oraz Centralne Biuro Antykorupcyjne, Generalnemu Inspektorowi nie przysługują uprawnienia określone w art. 12 pkt 2, art. 14 pkt 1 i 3-5 oraz art. 15-18.

7) w art. 43:

a) w ust. 1 w pkt 11 kropkę zastępuje się średnikiem i dodaje się pkt 12 w brzmieniu:

„12) przetwarzanych w zbiorach, które nie są prowadzone z wykorzystaniem systemów informatycznych, z wyjątkiem zbiorów zawierających dane, o których mowa w art. 27 ust. 1.”,

7) w art. 43:

b) po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. Obowiązkowi rejestracji zbiorów danych osobowych, z wyjątkiem zbiorów zawierających dane, o których mowa w art. 27 ust. 1, nie podlega administrator danych, który powołał administratora bezpieczeństwa informacji i zgłosił go Generalnemu Inspektorowi do rejestracji, z zastrzeżeniem art. 46e ust. 2.”;

Art. 44. 1. Generalny Inspektor wydaje decyzję o odmowie rejestracji zbioru danych, jeżeli:

1) nie zostały spełnione wymogi określone w art. 41 ust. 1;

2) przetwarzanie danych naruszałoby zasady określone w art. 23-28;

3) urządzenia i systemy informatyczne służące do przetwarzania zbioru danych zgłoszonego do rejestracji nie spełniają podstawowych warunków technicznych i organizacyjnych, określonych w przepisach, o których mowa w art. 39a.

2. Odmawiając rejestracji zbioru danych, Generalny Inspektor, w drodze decyzji administracyjnej, nakazuje:

1) ograniczenie przetwarzania wszystkich albo niektórych kategorii danych wyłącznie do ich przechowywania lub

2) zastosowanie innych środków, o których mowa w art. 18 ust. 1.

3. (uchylony).

4. Administrator danych może zgłosić ponownie zbiór danych do rejestracji po usunięciu wad, które były powodem odmowy rejestracji zbioru.

5. W razie ponownego zgłoszenia zbioru do rejestracji administrator danych może rozpocząć ich przetwarzanie po zarejestrowaniu zbioru.

Art. 44a. Wykreślenie z rejestru zbiorów danych osobowych jest dokonywane, w drodze decyzji administracyjnej, jeżeli:

1) zaprzestano przetwarzania danych w zarejestrowanym zbiorze;

2) rejestracji dokonano z naruszeniem prawa.

Art. 45. (uchylony).

Art. 46. 1. Administrator danych może, z zastrzeżeniem ust. 2, rozpocząć ich przetwarzanie w zbiorze danych po zgłoszeniu tego zbioru Generalnemu Inspektorowi, chyba że ustawa zwalnia go z tego obowiązku.

2. Administrator danych, o których mowa w art. 27 ust. 1, może rozpocząć ich przetwarzanie w zbiorze danych po zarejestrowaniu zbioru, chyba że ustawa zwalnia go z obowiązku zgłoszenia zbioru do rejestracji.

Art. 46a. Minister właściwy do spraw administracji publicznej określi, w drodze rozporządzenia, wzór zgłoszenia, o którym mowa w art. 41 ust. 1, uwzględniając obowiązek zamieszczenia informacji niezbędnych do stwierdzenia zgodności przetwarzania danych z wymogami ustawy.

8) po art. 46a dodaje się art. 46b–46f w brzmieniu:

„Art. 46b. 1. Administrator danych jest obowiązany zgłosić do rejestracji Generalnemu Inspektorowi powołanie i odwołanie administratora bezpieczeństwa informacji w terminie 30 dni od dnia jego powołania lub odwołania.

2. Zgłoszenie powołania administratora bezpieczeństwa informacji do rejestracji powinno zawierać:
1) oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany;
2) dane administratora bezpieczeństwa informacji:
a) imię i nazwisko,
b) numer PESEL lub, gdy ten numer nie został nadany, nazwę i numer dokumentu stwierdzającego tożsamość,
c) adres do korespondencji, jeżeli jest inny niż adres, o którym mowa w pkt 1;
3) datę powołania;
4) oświadczenie administratora danych o spełnianiu przez administratora bezpieczeństwa informacji warunków określonych w art. 36a ust. 5 i 7.
3. Zgłoszenie odwołania administratora bezpieczeństwa informacji powinno zawierać:
1) dane, o których mowa w ust. 2 pkt 1 i pkt 2 lit. a i b;
2) datę i przyczynę odwołania.
4. Na żądanie administratora danych lub administratora bezpieczeństwa informacji Generalny Inspektor wydaje zaświadczenie o zarejestrowaniu administratora bezpieczeństwa informacji.
5. Administrator danych jest obowiązany zgłosić Generalnemu Inspektorowi zmianę informacji objętych zgłoszeniem, o którym mowa w ust. 2, w terminie 14 dni od dnia zmiany. Do zgłaszania zmian stosuje się odpowiednio przepisy o zgłoszeniu powołania administratora bezpieczeństwa informacji.
Art. 46c. Generalny Inspektor prowadzi ogólnokrajowy, jawny rejestr administratorów bezpieczeństwa informacji, zawierający informacje, o których mowa w art. 46b ust. 2 pkt 1 i pkt 2 lit. a i c.
Art. 46d. 1. Wykreślenie administratora bezpieczeństwa informacji z rejestru administratorów bezpieczeństwa informacji następuje po powiadomieniu o jego odwołaniu albo w przypadku jego śmierci.
2. Generalny Inspektor z urzędu wydaje administratorowi danych decyzję o wykreśleniu administratora bezpieczeństwa informacji z rejestru administratorów bezpieczeństwa informacji, jeżeli:
1) administrator bezpieczeństwa informacji nie spełnia warunków określonych w art. 36a ust. 5 lub 7;
2) administrator bezpieczeństwa informacji nie wykonuje zadań określonych w art. 36a ust. 2;
3) administrator danych nie powiadomił o odwołaniu administratora bezpieczeństwa informacji.
3. Do administratora danych będącego adresatem decyzji, o której mowa w ust. 2, nie stosuje się zwolnienia, o którym mowa w art. 43 ust. 1a.
Art. 46e. 1. W przypadku ponownego zgłoszenia przez administratora danych do rejestracji Generalnemu Inspektorowi powołania administratora bezpieczeństwa informacji wykreślonego z rejestru administratorów bezpieczeństwa informacji na podstawie art. 46d ust. 2, Generalny Inspektor, w drodze decyzji administracyjnej:
1) wpisuje administratora bezpieczeństwa informacji do rejestru administratorów bezpieczeństwa informacji po stwierdzeniu, że nie zachodzą przyczyny wykreślenia z rejestru, o których mowa w art. 46d ust. 2 pkt 1 i 2;
2) odmawia wpisania administratora bezpieczeństwa informacji do rejestru administratorów bezpieczeństwa informacji, jeżeli nie zostały usunięte przyczyny wykreślenia z rejestru, o których mowa w art. 46d ust. 2 pkt 1 i 2.
2. Do administratora danych, który ponownie zgłosił do rejestracji administratora bezpieczeństwa informacji wykreślonego na podstawie art. 46d ust. 2, zwolnienie z obowiązku rejestracji zbioru określone w art. 43 ust. 1a stosuje się po wpisaniu zgłoszonego administratora bezpieczeństwa informacji do rejestru administratorów bezpieczeństwa informacji.

Art. 46f. Minister właściwy do spraw administracji publicznej określi, w drodze rozporządzenia, wzory zgłoszeń administratora bezpieczeństwa informacji, o których mowa w art. 46b ust. 2 i 3, uwzględniając konieczność zapewnienia Generalnemu Inspektorowi informacji niezbędnych do prawidłowego realizowania jego zadań.";

Rozdział 7 Przekazywanie danych osobowych do państwa trzeciego

Art. 47. 1. Przekazanie danych osobowych do państwa trzeciego może nastąpić, jeżeli państwo docelowe zapewnia na swoim terytorium odpowiedni poziom ochrony danych osobowych.

1a. Odpowiedni poziom ochrony danych osobowych, o którym mowa w ust. 1, jest oceniany z uwzględnieniem wszystkich okoliczności dotyczących operacji przekazania danych, w szczególności biorąc pod uwagę charakter danych, cel i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego przeznaczenia danych oraz przepisy prawa obowiązujące w danym państwie trzecim oraz stosowane w tym państwie środki bezpieczeństwa i zasady zawodowe.

2. Przepisu ust. 1 nie stosuje się, gdy przesłanie danych osobowych wynika z obowiązku nałożonego na administratora danych przepisami prawa lub postanowieniami ratyfikowanej umowy międzynarodowej, gwarantującymi odpowiedni poziom ochrony tych danych.

3. Administrator danych może jednak przekazać dane osobowe do państwa trzeciego, jeżeli:

1) osoba, której dane dotyczą, udzieliła na to zgody na piśmie;

2) przekazanie jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, lub jest podejmowane na jej życzenie;

3) przekazanie jest niezbędne do wykonania umowy zawartej w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem;

4) przekazanie jest niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych;

5) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą,

6) dane są ogólnie dostępne.

Art. 48. W przypadkach innych niż wymienione w art. 47 ust. 2 i 3 przekazanie danych osobowych do państwa trzeciego, które nie daje gwarancji ochrony danych osobowych przynajmniej takich, jakie obowiązują na terytorium Rzeczypospolitej Polskiej, może nastąpić po uzyskaniu zgody Generalnego Inspektora, pod warunkiem że administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą.

9) art. 48 otrzymuje brzmienie:
„Art. 48. 1. W przypadkach innych niż wymienione w art. 47 ust. 2 i 3 przekazanie danych osobowych do państwa trzeciego, które nie zapewnia na swoim terytorium odpowiedniego poziomu ochrony danych osobowych, może nastąpić po uzyskaniu zgody Generalnego Inspektora, wydanej w drodze decyzji administracyjnej, pod warunkiem że administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą.
2. Zgoda Generalnego Inspektora nie jest wymagana, jeżeli administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą, przez:
1) standardowe klauzule umowne ochrony danych osobowych, zatwierdzone przez Komisję Europejską zgodnie z art. 26 ust. 4 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995, str. 31, z późn. zm.; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, str. 355, z późn. zm.) lub

2) prawnie wiążące reguły lub polityki ochrony danych osobowych, zwane dalej „wiążącymi regułami korporacyjnymi", które zostały zatwierdzone przez Generalnego Inspektora zgodnie z ust. 3–5.

3. Generalny Inspektor zatwierdza, w drodze decyzji administracyjnej, wiążące reguły korporacyjne przyjęte w ramach grupy przedsiębiorców do celów przekazania danych osobowych przez administratora danych lub podmiot, o którym mowa w art. 31 ust. 1, do należącego do tej samej grupy innego administratora danych lub podmiotu, o którym mowa w art. 31 ust. 1, w państwie trzecim.

4. Generalny Inspektor przed zatwierdzeniem wiążących reguł korporacyjnych może przeprowadzić konsultacje z właściwymi organami ochrony danych osobowych państw należących do Europejskiego Obszaru Gospodarczego, na których terytorium mają siedziby przedsiębiorcy należący do grupy, o której mowa w ust. 3, przekazując im niezbędne informacje w tym celu.

5. Generalny Inspektor, wydając decyzję, o której mowa w ust. 3, uwzględnia wyniki przeprowadzonych konsultacji, o których mowa w ust. 4, a jeżeli wiążące reguły korporacyjne były przedmiotem rozstrzygnięcia organu ochrony danych osobowych innego państwa należącego do Europejskiego Obszaru Gospodarczego – może uwzględnić to rozstrzygnięcie.".

Rozdział 8 Przepisy karne

Art. 49. 1. Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

Art. 50. (uchylony).

Art. 51. 1. Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 52. Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 53. Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 54. Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 54a. Kto inspektorowi udaremnia lub utrudnia wykonanie czynności kontrolnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Rozdział 9 Zmiany w przepisach obowiązujących, przepisy przejściowe i końcowe

Art. 55. W ustawie z dnia 31 lipca 1981 r. o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz. U. Nr 20, poz. 101, z 1982 r. Nr 31, poz. 214, z 1985 r. Nr 22, poz. 98 i Nr 50, poz. 262, z 1987 r. Nr 21, poz. 123, z 1989 r. Nr 34, poz. 178, z 1991 r. Nr 100, poz. 443, z 1993 r. Nr 1, poz. 1, z 1995 r. Nr 34, poz. 163 i Nr 142, poz. 701, z 1996 r. Nr 73, poz. 350, Nr 89, poz. 402, Nr 106, poz. 496 i Nr 139, poz. 647 oraz z 1997 r. Nr 75, poz. 469) w art. 2 w pkt 2 po wyrazach "Rzecznika Praw Obywatelskich," dodaje się wyrazy "Generalnego Inspektora Ochrony Danych Osobowych,".

Art. 56. W ustawie z dnia 16 września 1982 r. o pracownikach urzędów państwowych (Dz. U. Nr 31, poz. 214, z 1984 r. Nr 35, poz. 187, z 1988 r. Nr 19, poz. 132, z 1989 r. Nr 4, poz. 24, Nr 34, poz. 178 i 182, z 1990 r. Nr 20, poz. 121, z 1991 r. Nr 55, poz. 234, Nr 88, poz. 400 i Nr 95, poz. 425, z 1992 r. Nr 54, poz. 254 i Nr 90, poz. 451, z 1994 r. Nr 136, poz. 704, z 1995 r. Nr 132, poz. 640, z 1996 r. Nr 89, poz. 402 i Nr 106, poz. 496 oraz z 1997 r. Nr 98, poz. 604) wprowadza się następujące zmiany: (zmiany pominięte).

Art. 57. W ustawie z dnia 5 stycznia 1991 r. - Prawo budżetowe (Dz. U. z 1993 r. Nr 72, poz. 344, z 1994 r. Nr 76, poz. 344, Nr 121, poz. 591 i Nr 133, poz. 685, z 1995 r. Nr 78, poz. 390, Nr 124, poz. 601 i Nr 132, poz. 640, z 1996 r. Nr 89, poz. 402, Nr 106, poz. 496, Nr 132, poz. 621 i Nr 139, poz. 647 oraz z 1997 r. Nr 54, poz. 348, Nr 79, poz. 484, Nr 121, poz. 770 i Nr 123, poz. 775 i 778) w art. 31 w ust. 3 w pkt 2 po wyrazach "Najwyższej Izby Kontroli" dodaje się wyrazy ", Generalnego Inspektora Ochrony Danych Osobowych".

Art. 58. W ustawie z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 1995 r. Nr 13, poz. 59, z 1996 r. Nr 64, poz. 315 i Nr 89, poz. 402 oraz z 1997 r. Nr 28, poz. 153, Nr 79, poz. 484, Nr 96, poz. 589 i Nr 121, poz. 770) w art. 4 wprowadza się następujące zmiany:

1)w ust. 1 po wyrazach "Krajowej Rady Radiofonii i Telewizji," dodaje się wyrazy "Generalnego Inspektora Ochrony Danych Osobowych,";

2)w ust. 2 po wyrazach "Krajowej Rady Radiofonii i Telewizji" dodaje się przecinek oraz wyrazy "Generalnego Inspektora Ochrony Danych Osobowych".

Art. 59. W ustawie z dnia 23 grudnia 1994 r. o kształtowaniu środków na wynagrodzenia w państwowej sferze budżetowej oraz o zmianie niektórych ustaw (Dz. U. z 1995 r. Nr 34, poz. 163 oraz z 1996 r. Nr 106, poz. 496 i Nr 139, poz. 647) w art. 2 w ust. 2 w pkt 1 po wyrazach "Krajowym Biurze Wyborczym" dodaje się wyrazy ", Biurze Generalnego Inspektora Ochrony Danych Osobowych."

Art. 60. W ustawie z dnia 26 kwietnia 1996 r. o Służbie Więziennej (Dz. U. Nr 61, poz. 283 i Nr 106, poz. 496 oraz z 1997 r. Nr 28, poz. 153 i Nr 88, poz. 554) dodaje się art. 23a w brzmieniu:

"Art. 23a.Służba Więzienna może gromadzić i przetwarzać informacje i dane osobowe, w tym także bez zgody osób, których dotyczą, niezbędne do realizacji zadań, o których mowa w art. 1 ust. 3 ustawy.".

Art. 61. 1. Podmioty określone w art. 3, prowadzące w dniu wejścia w życie ustawy zbiory danych osobowych w systemach informatycznych, mają obowiązek złożenia wniosków o zarejestrowanie tych zbiorów w trybie określonym w art. 41, w terminie 18 miesięcy od dnia jej wejścia w życie, chyba że ustawa zwalnia ich z tego obowiązku.

2. Do czasu rejestracji zbioru danych osobowych w trybie określonym w art. 41, podmioty, o których mowa w ust. 1, mogą prowadzić te zbiory bez rejestracji.

Art. 62. Ustawa wchodzi w życie po upływie 6 miesięcy od dnia ogłoszenia, z tym że:

1) art. 8-11, art. 13 i 45 wchodzą w życie po upływie 2 miesięcy od dnia ogłoszenia;

2) art. 55-59 wchodzą w życie po upływie 14 dni od dnia ogłoszenia.

Rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych

Dz.U. z 2004 nr 100 poz. 1024; 01.05.2004

ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI [1)]

z dnia 29 kwietnia 2004 r.

w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

Na podstawie art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285) zarządza się, co następuje:

§ 1. Rozporządzenie określa:

1) sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;

2) podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;

3) wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

§ 2. Ilekroć w rozporządzeniu jest mowa o:

1) ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwaną dalej „ustawą";

2) identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

3) haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

4) sieci telekomunikacyjnej – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm. [2)])

5) sieci publicznej – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne;

6) teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

7) rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

8) integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

9) raporcie – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;

10) poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

11) uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 3. 1. Na dokumentację, o której mowa w § 1 pkt 1, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „instrukcją".

2. Dokumentację, o której mowa w § 1 pkt 1, prowadzi się w formie pisemnej.

3. Dokumentację, o której mowa w § 1 pkt 1, wdraża administrator danych.

§ 4. Polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;

2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;

4) sposób przepływu danych pomiędzy poszczególnymi systemami;

5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

§ 5. Instrukcja, o której mowa w § 3 ust. 1, zawiera w szczególności:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;

2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;

3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;

4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

5) sposób, miejsce i okres przechowywania:

a) elektronicznych nośników informacji zawierających dane osobowe,

b) kopii zapasowych, o których mowa w pkt 4,

6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia;

7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4;

8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

§ 6. 1. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia wprowadza się poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym:

1) podstawowy;

2) podwyższony;

3) wysoki.

2. Poziom co najmniej podstawowy stosuje się, gdy:

1) w systemie informatycznym nie są przetwarzane dane, o których mowa w art. 27 ustawy, oraz

2) żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

3. Poziom co najmniej podwyższony stosuje się, gdy:

1) w systemie informatycznym przetwarzane są dane osobowe, o których mowa w art. 27 ustawy, oraz

2) żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

4. Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.

5. Opis środków bezpieczeństwa stosowany na poziomach, o których mowa w ust. 1, określa załącznik do rozporządzenia.

§ 7. 1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym – z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie – system ten zapewnia odnotowanie:

1) daty pierwszego wprowadzenia danych do systemu;

2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;

3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;

4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;

5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§ 8. System informatyczny służący do przetwarzania danych, który został dopuszczony przez właściwą służbę ochrony państwa do przetwarzania informacji niejawnych, po uzyskaniu certyfikatu wydanego na podstawie przepisów ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm. [3)]) spełnia wymogi niniejszego rozporządzenia pod względem bezpieczeństwa na poziomie wysokim.

§ 9. Administrator przetwarzanych w dniu wejścia w życie niniejszego rozporządzenia danych osobowych jest obowiązany dostosować systemy informatyczne służące do przetwarzania tych danych do wymogów określonych w § 7 oraz w załączniku do rozporządzenia w terminie 6 miesięcy od dnia wejścia w życie niniejszego rozporządzenia.

§ 10. Rozporządzenie wchodzi w życie z dniem uzyskania przez Rzeczpospolitą Polską członkostwa w Unii Europejskiej [4)] .

Minister Spraw Wewnętrznych i Administracji: w z. *T. Matusiak*

Załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (poz. 1024)

Załącznik 1

Załącznik do rozporządzenia

Dz.U. z 2004 nr 100 poz. 1024; 01.05.2004

A. Środki bezpieczeństwa na poziomie podstawowym

I

1. Obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

2. Przebywanie osób nieuprawnionych w obszarze, o którym mowa w § 4 pkt 1 rozporządzenia, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

II

1. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.

2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;

b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;

2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

IV

1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 6 znaków.

3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.

4. Kopie zapasowe:

a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;

b) usuwa się niezwłocznie po ustaniu ich użyteczności.

V

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w § 4 pkt 1 rozporządzenia, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

VI

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

1) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

3) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

VII

Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego.

B. Środki bezpieczeństwa na poziomie podwyższonym

VIII

W przypadku gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

IX

Urządzenia i nośniki zawierające dane osobowe, o których mowa w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przekazywane poza obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

X

Instrukcja zarządzania systemem informatycznym, o której mowa w § 5 rozporządzenia, rozszerza się o sposób stosowania środków, o których mowa w pkt IX załącznika.

XI

Administrator danych stosuje na poziomie podwyższonym środki bezpieczeństwa określone w części A załącznika, o ile zasady zawarte w części B nie stanowią inaczej.

C. Środki bezpieczeństwa na poziomie wysokim

XII

1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:

a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;

b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

XIII

Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

XIV

Administrator danych stosuje na poziomie wysokim środki bezpieczeństwa, określone w części A i B załącznika, o ile zasady zawarte w części C nie stanowią inaczej.

Rozporządzenie w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji

ROZPORZĄDZENIE
MINISTRA ADMINISTRACJI I CYFRYZACJI[1)]

z dnia 10 grudnia 2014 r.

w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji

Na podstawie art. 46f ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 i 1662) zarządza się, co następuje:

§ 1. [Wzory zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji] Określa się wzory zgłoszeń:

1) powołania administratora bezpieczeństwa informacji do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, stanowiący załącznik nr 1 do rozporządzenia;

2) odwołania administratora bezpieczeństwa informacji do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, stanowiący załącznik nr 2 do rozporządzenia.

§ 2. [Wejście w życie] Rozporządzenie wchodzi w życie z dniem 1 stycznia 2015 r.

Minister Administracji i Cyfryzacji: A. Halicki

[1)] Minister Administracji i Cyfryzacji kieruje działem administracji rządowej - administracja publiczna, na podstawie § 1 ust. 2 pkt 1 rozporządzenia Prezesa Rady Ministrów z dnia 22 września 2014 r. w sprawie szczegółowego zakresu działania Ministra Administracji i Cyfryzacji (Dz. U. poz. 1254).

Załącznik 1. [WZÓR – ZGŁOSZENIE POWOŁANIA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI DO REJESTRACJI GENERALNEMU INSPEKTOROWI OCHRONY DANYCH OSOBOWYCH]

Załączniki do rozporządzenia Ministra Administracji i Cyfryzacji
z dnia 10 grudnia 2014 r. (poz. 1934)

Załącznik nr 1

WZÓR – ZGŁOSZENIE POWOŁANIA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI DO REJESTRACJI GENERALNEMU INSPEKTOROWI OCHRONY DANYCH OSOBOWYCH

ZGŁOSZENIE
POWOŁANIA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI DO REJESTRACJI GENERALNEMU INSPEKTOROWI OCHRONY DANYCH OSOBOWYCH

Data wpłynięcia zgłoszenia: ……
(wypełnia Generalny Inspektor Ochrony Danych Osobowych)*

Część A. Oznaczenie administratora danych

Nazwa administratora danych i adres jego siedziby albo nazwisko, imię i adres miejsca zamieszkania administratora danych oraz nr REGON – jeżeli został nadany.

1. Administrator:
2. REGON:
3. Adres:
   ulica:
   nr domu: nr lokalu:
   kod pocztowy:
   miejscowość:

Część B. Dane osobowe administratora bezpieczeństwa informacji i data jego powołania

1. Imię i nazwisko:
2. Numer PESEL lub, gdy ten numer nie został nadany, nazwa i seria/nr dokumentu stwierdzającego tożsamość:
   PESEL:
   nazwa dokumentu tożsamości: seria/nr dokumentu tożsamości:
3. Adres do korespondencji, jeżeli jest inny niż wskazany w części A zgłoszenia:
   ulica:
   nr domu: nr lokalu:
   kod pocztowy:
   miejscowość:
4. Data powołania administratora bezpieczeństwa informacji:

Część C. Oświadczenie administratora danych o spełnieniu przez administratora bezpieczeństwa informacji warunków określonych w ustawie

Oświadczam, że administrator bezpieczeństwa informacji wskazany w części B zgłoszenia**:

- ☐ ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych,
- ☐ posiada odpowiednią wiedzę w zakresie ochrony danych osobowych,
- ☐ nie był karany za umyślne przestępstwo,
- ☐ podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych.

(data, podpis i pieczęć administratora danych)*

Objaśnienia:

* Pola nie należy wypełniać, jeżeli zgłoszenie doręczone jest za pomocą środków komunikacji elektronicznej.
** W przypadku odpowiedzi twierdzącej należy zakreślić kwadrat literą „X".

Załącznik 2. [WZÓR – ZGŁOSZENIE ODWOŁANIA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI DO REJESTRACJI GENERALNEMU INSPEKTOROWI OCHRONY DANYCH OSOBOWYCH]

Załącznik nr 2

WZÓR – ZGŁOSZENIE ODWOŁANIA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI DO REJESTRACJI GENERALNEMU INSPEKTOROWI OCHRONY DANYCH OSOBOWYCH

ZGŁOSZENIE
ODWOŁANIA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI DO REJESTRACJI GENERALNEMU INSPEKTOROWI OCHRONY DANYCH OSOBOWYCH

Data wpłynięcia zgłoszenia: .....
(wypełnia Generalny Inspektor Ochrony Danych Osobowych)*

Część A. Oznaczenie administratora danych

Nazwa administratora danych i adres jego siedziby albo nazwisko, imię i adres zamieszkania administratora danych oraz nr REGON – jeśli został nadany.

1. Administrator:
2. REGON:
3. Adres:
   ulica:
   nr domu: nr lokalu:
   kod pocztowy:
   miejscowość:

Część B. Dane osobowe administratora bezpieczeństwa informacji

1. Imię i nazwisko:
2. Numer PESEL lub, gdy ten numer nie został nadany, nazwa i seria nr dokumentu stwierdzającego tożsamość:
   PESEL:
   nazwa dokumentu tożsamości: seria nr dokumentu tożsamości:

Część C. Data i przyczyna odwołania administratora bezpieczeństwa informacji

1. Data odwołania administratora bezpieczeństwa informacji:
2. Przyczyna odwołania administratora bezpieczeństwa informacji:

(data, podpis i pieczęć administratora danych)*

Objaśnienia:

* Pola nie należy wypełniać, jeżeli zgłoszenie doręczone jest za pomocą środków komunikacji elektronicznej.

Rozporządzenie w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych

ROZPORZĄDZENIE
MINISTRA ADMINISTRACJI I CYFRYZACJI[1)]

z dnia 11 maja 2015 r.

w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych

Na podstawie art. 36a ust. 9 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 i 1662) zarządza się, co następuje:

§ 1. [Zakres regulacji] Rozporządzenie określa sposób prowadzenia rejestru zbiorów danych, o którym mowa w art. 36a ust. 2 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwanej dalej „ustawą".

§ 2. [Forma prowadzenia rejestru zbiorów danych] 1. Rejestr zbiorów danych, o którym mowa w art. 36a ust. 2 pkt 2 ustawy, zwany dalej „rejestrem", składa się z wykazu zbiorów danych zawierającego informacje określone w § 3 odrębnie dla każdego zbioru danych.

2. Rejestr jest prowadzony w postaci papierowej lub w postaci elektronicznej.

§ 3. [Informacje zawarte w rejestrze] 1. W rejestrze znajdują się następujące informacje dotyczące każdego zbioru danych:

1) nazwa zbioru danych;

2) oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania oraz numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany;

3) oznaczenie przedstawiciela administratora danych, o którym mowa w art. 31a ustawy, i adres jego siedziby lub miejsca zamieszkania – w przypadku wyznaczenia takiego podmiotu;

4) oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru na podstawie art. 31 ustawy, i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi;

5) podstawa prawna upoważniająca do prowadzenia zbioru danych;

6) cel przetwarzania danych w zbiorze;

7) opis kategorii osób, których dane są przetwarzane w zbiorze;

8) zakres danych przetwarzanych w zbiorze;

9) sposób zbierania danych do zbioru, w szczególności informacja, czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą;

10) sposób udostępniania danych ze zbioru, w szczególności informacja, czy dane ze zbioru są udostępniane innym podmiotom niż upoważnione na podstawie przepisów prawa;

11) oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane;

12) informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego.

2. W rejestrze podaje się datę wpisu każdego zbioru danych do rejestru, a także datę ostatniej aktualizacji informacji dotyczących każdego zbioru danych.

3. W przypadku wykreślenia zbioru danych z rejestru w rejestrze pozostawia się nazwę zbioru danych, datę wpisania zbioru danych oraz datę ostatniej aktualizacji informacji dotyczących tego zbioru wraz z adnotacją, że jest to data wykreślenia zbioru z rejestru.

4. Informacje, o których mowa w ust. 1, są udostępniane w rejestrze do przeglądania w powszechnie zrozumiałej formie, według kolejności określonej w ust. 1.

§ 4. [Czynności dokonywane przez administratora bezpieczeństwa informacji] 1. Administrator bezpieczeństwa informacji w ramach prowadzenia rejestru:

1) wpisuje zbiór danych do rejestru przed rozpoczęciem przetwarzania w zbiorze danych;

2) aktualizuje informacje dotyczące zbioru danych w rejestrze – w przypadku zmiany informacji objętych wpisem;

3) wykreśla zbiór danych z rejestru – w przypadku zaprzestania przetwarzania w nim danych osobowych;

4) udostępnia rejestr do przeglądania.

2. Czynności, o których mowa w ust. 1 pkt 2 i 3, dokonuje się niezwłocznie po zaistnieniu zdarzenia powodującego obowiązek ich dokonania.

§ 5. [Udostępnienie rejestru do przeglądania] 1. W przypadku prowadzenia rejestru w postaci elektronicznej administrator bezpieczeństwa informacji udostępnia rejestr do przeglądania:

1) na stronie internetowej administratora danych, przy czym na stronie głównej umieszcza się odwołanie umożliwiające bezpośredni dostęp do rejestru, lub

2) na stanowisku dostępowym w systemie informatycznym administratora danych znajdującym się w siedzibie lub miejscu zamieszkania tego administratora, lub

3) przez sporządzenie wydruku rejestru z systemu informatycznego administratora danych.

2. W przypadku prowadzenia rejestru w postaci papierowej administrator bezpieczeństwa informacji udostępnia każdemu zainteresowanemu treść rejestru do przeglądania w siedzibie lub miejscu zamieszkania administratora danych.

3. W przypadku prowadzenia rejestru wyłącznie w postaci elektronicznej albo w postaci papierowej i postaci elektronicznej administrator bezpieczeństwa informacji może zdecydować, że w odniesieniu do informacji, o których mowa w § 3 ust. 1 pkt 4, w postaci elektronicznej udostępnia się do przeglądania wyłącznie informacje o powierzeniu przetwarzania danych innemu podmiotowi, a jego oznaczenie i adres siedziby lub miejsca zamieszkania są udostępniane do przeglądania jedynie w sposób określony w ust. 2.

§ 6. [Historia zmian w rejestrze] Administrator bezpieczeństwa informacji odnotowuje historię zmian w rejestrze zawierającą:

1) informację o rodzaju zmiany (nowy wpis, aktualizacja, wykreślenie);

2) datę dokonania zmiany;

3) informację o zakresie zmiany.

§ 7. [Wejście w życie] Rozporządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

Minister Administracji i Cyfryzacji: A. Halicki

[1)] Minister Administracji i Cyfryzacji kieruje działem administracji rządowej - administracja publiczna, na podstawie § 1 ust. 2 pkt 1 rozporządzenia Prezesa Rady Ministrów z dnia 22 września 2014 r. w sprawie szczegółowego zakresu działania Ministra Administracji i Cyfryzacji (Dz. U. poz. 1254).

Rozporządzenie w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji

ROZPORZĄDZENIE
MINISTRA ADMINISTRACJI I CYFRYZACJI[1)]

z dnia 11 maja 2015 r.

w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji

Na podstawie art. 36a ust. 9 pkt 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 i 1662) zarządza się, co następuje:

Rozdział 1

Przepisy ogólne

§ 1. [Zakres regulacji] Rozporządzenie określa tryb i sposób:

1) sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania sprawozdania w tym zakresie;

2) nadzorowania:

a) opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną,

b) przestrzegania zasad określonych w dokumentacji, o której mowa w lit. a.

§ 2. [Definicje] Ilekroć w rozporządzeniu jest mowa o:

1) ustawie – należy przez to rozumieć ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;

2) dokumentacji przetwarzania danych – należy przez to rozumieć dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, określoną w przepisach wydanych na podstawie art. 39a ustawy;

3) sprawdzeniu – należy przez to rozumieć czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

4) sprawozdaniu – należy przez to rozumieć dokument, o którym mowa w art. 36c ustawy, opracowany przez administratora bezpieczeństwa informacji po dokonaniu sprawdzenia.

Rozdział 2

Tryb i sposób sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania sprawozdania

§ 3. [Sprawdzenie] 1. Sprawdzenie jest dokonywane:

1) dla administratora danych;

2) dla Generalnego Inspektora Ochrony Danych Osobowych, zwanego dalej „Generalnym Inspektorem", w przypadku, o którym mowa w art. 19b ust. 1 ustawy.

2. Sprawdzenie jest przeprowadzane w trybie:

1) sprawdzenia planowego – według planu sprawdzeń, o którym mowa w ust. 3;

2) sprawdzenia doraźnego – w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia przez administratora bezpieczeństwa informacji wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia;

3) art. 19b ust. 1 ustawy – w przypadku zwrócenia się o dokonanie sprawdzenia przez Generalnego Inspektora.

3. Plan sprawdzeń określa przedmiot, zakres oraz termin przeprowadzenia poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania.

4. Administrator bezpieczeństwa informacji w planie sprawdzeń uwzględnia, w szczególności, zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych:

1) z zasadami, o których mowa w art. 23–27 i art. 31–35 ustawy;

2) z zasadami dotyczącymi zabezpieczenia danych osobowych, o których mowa w art. 36, art. 37–39 ustawy oraz przepisach wydanych na podstawie art. 39a ustawy;

3) z zasadami przekazywania danych osobowych, o których mowa w art. 47–48 ustawy;

4) z obowiązkiem zgłoszenia zbioru danych do rejestracji i jego aktualizacji, jeżeli zbiór zawiera dane, o których mowa w art. 27 ust. 1 ustawy.

5. Plan sprawdzeń jest przygotowywany przez administratora bezpieczeństwa informacji na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan sprawdzeń jest przedstawiany administratorowi danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem. Plan sprawdzeń obejmuje co najmniej jedno sprawdzenie.

6. Zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych powinny być objęte sprawdzeniem co najmniej raz na pięć lat.

7. Sprawdzenie doraźne jest przeprowadzane niezwłocznie po powzięciu wiadomości przez administratora bezpieczeństwa informacji o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.

8. Administrator bezpieczeństwa informacji zawiadamia administratora danych o rozpoczęciu sprawdzenia doraźnego lub sprawdzenia w trybie, o którym mowa w art. 19b ust. 1 ustawy, przed podjęciem pierwszej czynności w toku sprawdzenia.

§ 4. [Dokumentowanie czynności w toku sprawdzenia] 1. Administrator bezpieczeństwa informacji dokumentuje czynności przeprowadzone w toku sprawdzenia, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.

2. Dokumentowanie czynności w toku sprawdzenia może polegać, w szczególności, na utrwaleniu danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych na informatycznym nośniku danych lub dokonaniu wydruku tych danych oraz na:

1) sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;

2) odebraniu wyjaśnień osoby, której czynności objęto sprawdzeniem;

3) sporządzeniu kopii otrzymanego dokumentu;

4) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;

5) sporządzeniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

3. W systemie informatycznym służącym do przetwarzania lub zabezpieczania danych osobowych czynności administratora bezpieczeństwa informacji mogą być wykonywane przy udziale osób upoważnionych do przetwarzania danych osobowych, w szczególności osoby zarządzającej tym systemem.

4. Materiały są sporządzane w postaci papierowej lub w postaci elektronicznej.

§ 5. [Zawiadomienie kierownika jednostki organizacyjnej objętej sprawdzeniem o zakresie planowanych czynności] 1. Osoba odpowiedzialna za przetwarzanie danych osobowych, której dotyczy sprawdzenie, bierze udział w sprawdzeniu lub umożliwia administratorowi bezpieczeństwa informacji przeprowadzenie czynności w toku sprawdzenia.

2. Administrator bezpieczeństwa informacji zawiadamia kierownika jednostki organizacyjnej objętej sprawdzeniem o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności.

3. Zawiadomienia nie przekazuje się w przypadku:

1) sprawdzenia doraźnego, jeżeli niezwłoczne rozpoczęcie sprawdzenia jest niezbędne do przywrócenia stanu zgodnego z prawem lub weryfikacji, czy naruszenie miało miejsce;

2) sprawdzenia, o którego dokonanie zwrócił się Generalny Inspektor, jeżeli na zawiadomienie nie pozwala wyznaczony przez niego termin;

3) jeżeli kierownik jednostki organizacyjnej objętej sprawdzeniem posiada informacje, o których mowa w ust. 2.

§ 6. [Sprawozdanie po zakończeniu sprawdzenia] 1. Po zakończeniu sprawdzenia administrator bezpieczeństwa informacji przygotowuje sprawozdanie.

2. Sprawozdanie jest sporządzane w postaci elektronicznej albo w postaci papierowej.

3. Administrator bezpieczeństwa informacji przekazuje administratorowi danych sprawozdanie:

1) ze sprawdzenia planowego – nie później niż w terminie 30 dni od zakończenia sprawdzenia;

2) ze sprawdzenia doraźnego – niezwłocznie po zakończeniu sprawdzenia;

3) ze sprawdzenia, o którego dokonanie zwrócił się Generalny Inspektor – zachowując termin wskazany przez Generalnego Inspektora zgodnie z art. 19b ust. 1 ustawy.

Rozdział 3

Tryb i sposób nadzoru nad dokumentacją przetwarzania danych

§ 7. [Weryfikacja przeprowadzana przez administratora bezpieczeństwa informacji] 1. Sprawując nadzór, o którym mowa w § 1 pkt 2, administrator bezpieczeństwa informacji dokonuje weryfikacji:

1) opracowania i kompletności dokumentacji przetwarzania danych;

2) zgodności dokumentacji przetwarzania danych z obowiązującymi przepisami prawa;

3) stanu faktycznego w zakresie przetwarzania danych osobowych;

4) zgodności ze stanem faktycznym przewidzianych w dokumentacji przetwarzania danych środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych;

5) przestrzegania zasad i obowiązków określonych w dokumentacji przetwarzania danych.

2. Administrator bezpieczeństwa informacji przeprowadza weryfikację:

1) w sprawdzeniach, o których mowa w § 3;

2) poza sprawdzeniami, na podstawie zgłoszenia osoby wykonującej obowiązki określone w dokumentacji przetwarzania danych oraz własnego udziału administratora bezpieczeństwa informacji w procedurach w niej określonych.

3. Administrator bezpieczeństwa informacji może przeprowadzić weryfikację poza sprawdzeniami, na podstawie zgłoszenia osoby trzeciej.

§ 8. [Wykrycie nieprawidłowości podczas weryfikacji] 1. W przypadku wykrycia podczas weryfikacji nieprawidłowości administrator bezpieczeństwa informacji:

1) zawiadamia administratora danych o nieopracowaniu lub brakach w dokumentacji przetwarzania danych lub jej elementach oraz działaniach podjętych w celu doprowadzenia dokumentacji do wymaganego stanu, w szczególności może przedstawić mu do wdrożenia projekty dokumentów usuwające stan niezgodności;

2) zawiadamia administratora danych o nieaktualności dokumentacji przetwarzania danych oraz może przedstawić administratorowi danych do wdrożenia projekty dokumentów aktualizujących;

3) poucza lub instruuje osobę nieprzestrzegającą zasad określonych w dokumentacji przetwarzania danych o prawidłowym sposobie ich realizacji lub zawiadamia administratora danych, wskazując osobę odpowiedzialną za naruszenie tych zasad oraz jego zakres.

2. Zawiadomienia mogą być zawarte w sprawozdaniu albo w odrębnym dokumencie.

3. Pouczenia lub instrukcje są zawarte w odrębnym dokumencie skierowanym do osoby nieprzestrzegającej zasad określonych w dokumentacji przetwarzania danych.

4. Dokumenty, o których mowa w ust. 2 i 3, są sporządzane w postaci papierowej albo postaci elektronicznej.

Rozdział 4

Przepis końcowy

§ 9. [Wejście w życie] Rozporządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

Minister Administracji i Cyfryzacji: A. Halicki

[1)] Minister Administracji i Cyfryzacji kieruje działem administracji rządowej - administracja publiczna, na podstawie § 1 ust. 2 pkt 1 rozporządzenia Prezesa Rady Ministrów z dnia 22 września 2014 r. w sprawie szczegółowego zakresu działania Ministra Administracji i Cyfryzacji (Dz. U. poz. 1254).

Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa

Źródło: zasoby GIODO

Opracowanie omawia sposób przygotowania i zakresu dokumentacji opisującej politykę bezpieczeństwa w zakresie odnoszącym się do sposobu przetwarzania danych osobowych oraz środków ich ochrony określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024)

Uwagi ogólne

Zgodnie z § 3 i § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024), zwanego dalej rozporządzeniem, administrator danych obowiązany jest do opracowania w formie pisemnej i wdrożenia polityki bezpieczeństwa. Pojęcie „polityka bezpieczeństwa", użyte w rozporządzeniu należy rozumieć, jako zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej (tutaj danych osobowych) wewnątrz określonej organizacji [1]. Należy zaznaczyć, że zgodnie z art. 36 ust. 2 oraz art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm.), zwanej dalej ustawą, polityka bezpieczeństwa, o której mowa w rozporządzeniu powinna odnosić się całościowo do problemu zabezpieczenia danych osobowych u administratora danych tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie jak i danych przetwarzanych w systemach informatycznych. Celem polityki bezpieczeństwa, jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki administratora danych w zakresie zabezpieczenia danych osobowych, o których mowa w § 36 ustawy. Polska Norma PN-ISO/IEC 17799 [3] określająca praktyczne zasady zarządzania bezpieczeństwem informacji w obszarze technik informatycznych, jako cel polityki bezpieczeństwa wskazuje *„zapewnienie kierunków działania i wsparcie kierownictwa dla bezpieczeństwa informacji*". Zaznacza się, że dokument polityki bezpieczeństwa powinien deklarować zaangażowanie kierownictwa i wyznaczać podejście instytucji do zarządzania bezpieczeństwem informacji. Jako minimum w [3] wskazuje się, aby dokument określający politykę bezpieczeństwa zawierał:

a) *definicję bezpieczeństwa informacji, jego ogólne cele i zakres oraz znaczenie bezpieczeństwa jako mechanizmu umożliwiającego współużytkowanie informacji;*
b) *oświadczenie o intencjach kierownictwa, potwierdzające cele i zasady bezpieczeństwa informacji;*
c) *krótkie wyjaśnienie polityki bezpieczeństwa, zasad, standardów i wymagań zgodności mających szczególne znaczenie dla instytucji, np.:*
   1) *zgodność z prawem i wymaganiami wynikającymi z umów;*
   2) *wymagania dotyczące kształcenia w dziedzinie bezpieczeństwa;*
   3) *zapobieganie i wykrywanie wirusów oraz innego złośliwego oprogramowania;*
   4) *zarządzanie ciągłością działania biznesowego;*
   5) *konsekwencje naruszenia polityki bezpieczeństwa;*
d) *definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji, w tym zgłaszania przypadków naruszenia bezpieczeństwa;*
e) *odsyłacze do dokumentacji mogącej uzupełniać politykę, np. bardziej szczegółowych polityk bezpieczeństwa i procedur dla poszczególnych systemów informatycznych lub zasad bezpieczeństwa, których użytkownicy powinni przestrzegać.*

Wymienione wyżej, cytowane za [3], zalecenia w pełni można stosować do dokumentacji polityki bezpieczeństwa, o której mowa w § 4 rozporządzenia. Dokument określający politykę bezpieczeństwa nie powinien mieć charakteru zbyt abstrakcyjnego. Zasady postępowania określone w polityce bezpieczeństwa powinny zawierać uzasadnienie wyjaśniające przyjęte standardy i wymagania. Wyjaśnienia i uzasadnienia zalecanych metod sprawiają na ogół, że rzadziej dochodzi do ich naruszenia i nie przestrzegania [5].

Dokument, o którym mowa w § 4 rozporządzenia w zakresie przedmiotowym powinien koncentrować się na bezpieczeństwie przetwarzania danych osobowych, co wynika z art. 36 ustawy o ochronie danych osobowych[1]. Prawidłowe zarządzanie zasobami, w tym również zasobami informacyjnymi, zwłaszcza w aspekcie bezpieczeństwa informacji, wymaga właściwej identyfikacji tych zasobów [2] oraz określenia miejsca i sposobu ich przechowywania. Wybór zaś odpowiednich dla poszczególnych zasobów metod zarządzania ich ochroną i dystrybucją zależny jest od zastosowanych nośników informacji, rodzaju zastosowanych urządzeń, sprzętu komputerowego i oprogramowania. Stąd też w § 4 rozporządzenia ustawodawca wskazał, że polityka bezpieczeństwa powinna zawierać w szczególności:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
4) sposób przepływu danych pomiędzy poszczególnymi systemami;
5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

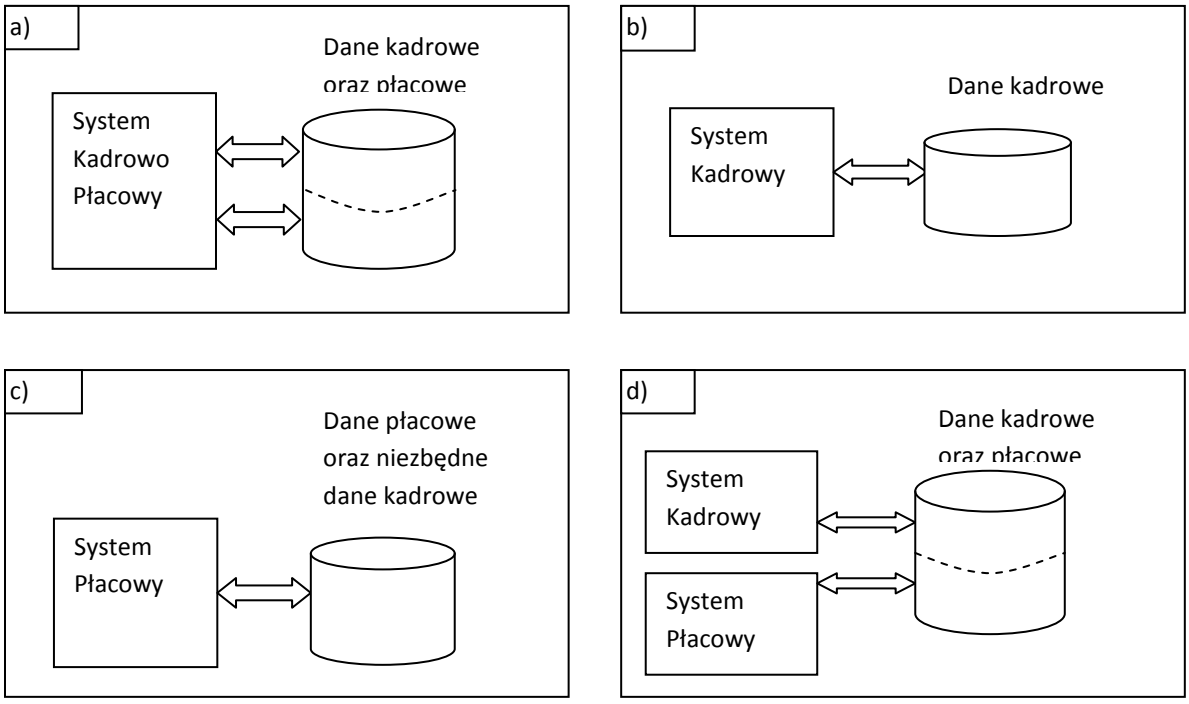
Określając obszar przetwarzania danych osobowych należy pamiętać, iż zgodnie z ustawą o ochronie danych osobowych, przetwarzaniem danych osobowych nazywamy jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. W związku z powyższym, określanie obszaru pomieszczeń, w którym przetwarzane są dane osobowe, powinno obejmować zarówno miejsca, w których wykonuje się operacje na danych osobowych (wpisuje, modyfikuje, kopiuje), jak również miejsca, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacja papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe, jak np. macierze dyskowe, na których dane osobowe są przetwarzane na bieżąco). Zgodnie z treścią §4 punkt 1, wskazanie miejsca przetwarzania danych osobowych powinno być określone poprzez określenie budynków, pomieszczeń lub części pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Do obszaru przetwarzania danych należy zaliczyć również pomieszczenia, gdzie składowane są uszkodzone komputerowe nośniki danych (taśmy, dyski, płyty CD, uszkodzone komputery i inne urządzenia z nośnikami zawierającymi dane osobowe). Do obszaru przetwarzania danych osobowych administrator danych powinien zaliczyć również miejsce w sejfie bankowym, archiwum, itp. jeśli wykorzystywane są one np. do przechowywania elektronicznych nośników informacji zawierających kopie zapasowe danych przetwarzanych w systemie informatycznym, czy też do składowania innych nośników danych, np. dokumentów źródłowych.

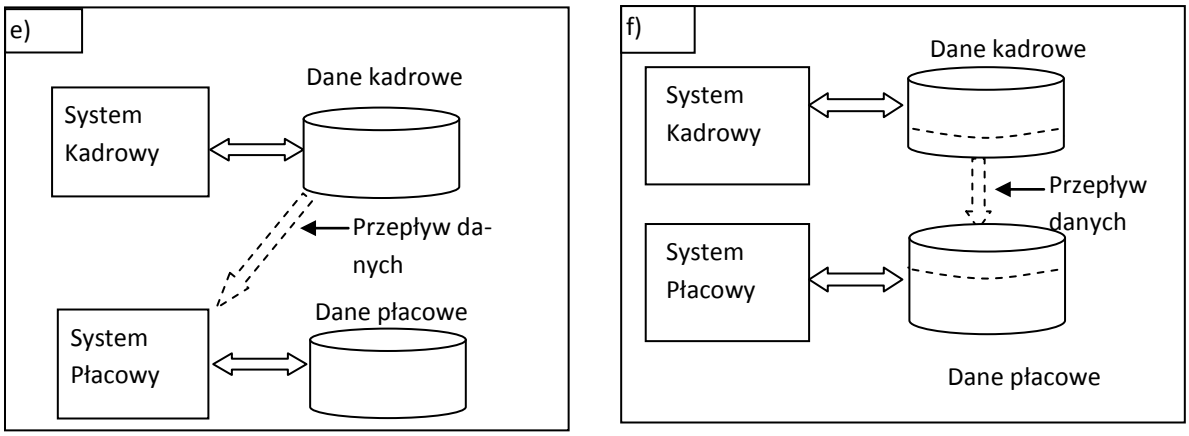
[1] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024), zwanego dalej rozporządzeniem, wydane zostało na podstawie delegacji ustawowej art. 39a ustawy o ochronie danych osobowych i jego zakres na podstawie art. 36 ust. 2 tejże ustawy ograniczony jest do przetwarzania danych osobowych.

W przypadku, gdy dane osobowe przetwarzane są w systemie informatycznym, do którego dostęp poprzez sieć telekomunikacyjną posiada wiele podmiotów, wówczas w polityce bezpieczeństwa informacje o tych podmiotach (nazwa podmiotu, siedziba, pomieszczenia, w których przetwarzane są dane), powinny być również wymienione jako obszar przetwarzania danych. Wymóg powyższy nie dotyczy sytuacji udostępniania danych osobowych użytkownikom, którzy dostęp do systemu uzyskują tylko z prawem wglądu w swoje własne dane po wprowadzeniu właściwego identyfikatora i hasła (np. systemów stosowanych w uczelniach wyższych do udostępniania studentom informacji o uzyskanych ocenach) oraz systemów, do których dostęp z założenia jest dostępem publicznym np. książka telefoniczna udostępniana w Internecie. W wyżej wymienionych sytuacjach wystarczające jest wskazanie budynków i pomieszczeń, w których dane są przetwarzane przez administratorów systemu informatycznego oraz budynki i pomieszczenia, w których dostęp do danych uzyskują osoby posiadające szerszy zakres uprawnień, niż tylko wgląd do swoich własnych danych lub danych udostępnianych publicznie.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Ważnym elementem identyfikacji przetwarzanych zasobów informacyjnych jest wskazanie nazw zbiorów danych oraz systemów informatycznych używanych do ich przetwarzania. Stąd też oprócz wskazania obszaru przetwarzania danych, polityka bezpieczeństwa powinna identyfikować zbiory danych osobowych oraz systemy informatyczne używane do ich przetwarzania. W przypadku, gdy system zbudowany jest z wielu modułów programowych i moduły te mogą pracować niezależnie np. mogą być instalowane na różnych stacjach komputerowych, wówczas wskazanie systemu powinno być wykonane z dokładnością do poszczególnych jego modułów. Należy zauważyć również, iż jeden program może przetwarzać dane zawarte w jednym zbiorze jak i wielu zbiorach danych osobowych. Sytuacja może być również odwrotna, kiedy to wiele różnych programów przetwarza dane, stanowiące jeden zbiór danych osobowych. Programy te to najczęściej moduły zintegrowanego systemu. Każdy taki moduł dedykowany jest do wykonywania określonych, wydzielonych funkcjonalnie zadań. Przykładem, może być system kadrowy oraz system płacowy, które często występują jako jeden zintegrowany system kadrowo - płacowy. Systemy informatyczne mogą przetwarzać dane osobowe stanowiące jeden wspólny zbiór danych, jak też wiele odrębnych zbiorów danych osobowych. Mogą być zintegrowane tworząc jeden system, z jednym lub wieloma zbiorami danych. Przykłady możliwych w tym zakresie konfiguracje przedstawiono na Rys. 1





Rys. 1. Różne modele współpracy systemów informatycznych ze zbiorami danych; a, b, c) -jeden zbiór danych przetwarzany przez jeden system; d) - dwa oddzielne systemy (moduły programowe) przetwarzają dane zawarte w jednym zbiorze; e, f) - dwa oddzielne systemy (moduły programowe) przetwarzają dane zawarte w dwóch zbiorach pomiędzy którymi występuje przepływ danych.

Stąd też, w części polityki bezpieczeństwa identyfikującej zbiory danych osobowych oraz stosowane do ich przetwarzania programy powinny być zamieszczone nazwy zbiorów danych osobowych oraz nazwy używanych do ich przetwarzania programów komputerowych.

Wykaz ten powinien zawierać informacje w zakresie precyzyjnej lokalizacji miejsca (budynek, pomieszczenie, nazwa komputera lub innego urządzenia np. macierzy dyskowej, biblioteki optycznej itp.), w których znajdują się zbiory danych osobowych przetwarzane na bieżąco oraz nazwy i lokalizacje programów (modułów programowych) używanych do ich przetwarzania.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Zgodnie z § 4 pkt 3 rozporządzenia, dla każdego zidentyfikowanego zbioru danych powinien być wskazany opis struktury zbioru i zakres informacji gromadzonych w danym zbiorze. Opisy poszczególnych pól informacyjnych w strukturze zbioru danych powinny jednoznacznie wskazywać jakie kategorie danych są w nich przechowywane. Opis pola danych, w przypadkach, gdy możliwa jest niejednoznaczna interpretacja jego zawartości, powinien wskazywać nie tylko kategorię danych, ale również format jej zapisu i/lub określone w danym kontekście znaczenie. Za niewystarczający należy uznać np. opis jednoznakowego pola w postaci „Zgoda na przetwarzanie danych osobowych dla celów marketingowych", jeśli nie dodamy, że w pole to należy wpisywać literę „T" w przypadku wyrażenia zgody lub literę „N" w przypadku nie wyrażenia zgody. Brak stosownego opisu może spowodować inne niż zakładano sposoby zapisu oraz interpretacji określonej informacji.

W odniesieniu do opisu struktury zbioru, w przypadku zbiorów danych przetwarzanych w systemie informatycznym, należy zauważyć, iż jest on niezbędny dla ustalenia bądź też weryfikacji zakresu danych. Zakres ten, w przypadku relacyjnych baz danych, nie wynika bezpośrednio z zakresu danych przypisanych poszczególnym obiektom zapisanym w zbiorze. Jest on zależny od relacji ustalonych pomiędzy poszczególnymi obiektami. Przykładowo, jeśli w zbiorze przetwarzane są informacje o danych adresowych klienta, zamówieniach klientów oraz sprzedawanych towarach w zakresie przedstawionym w tablicy 1, to z relacji ustanowionych za pośrednictwem pola o nazwie identyfikatora klienta pomiędzy obiektami: „*dane adresowe klienta*" i „*zamówienia klienta*" wynika, że w zbiorze tym przetwarzane są informacje o klientach w następującym zakresie:

<***Zakres 1***>: [imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/mieszkania), nazwa towaru, ilość towaru, wartość zamówienia, data zamówienia, data odbioru],

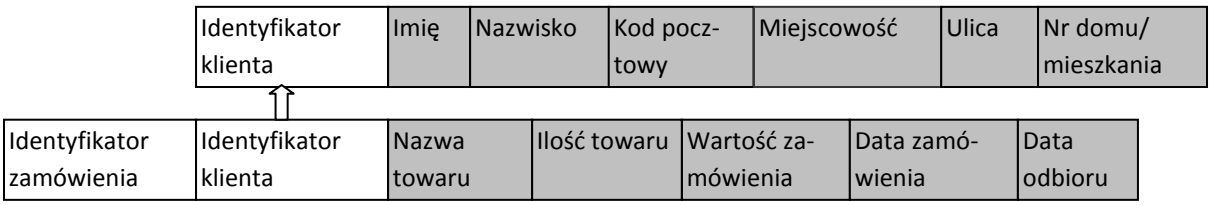
oraz informacje o towarach w zakresie:

<***Zakres 2***>: [identyfikator towaru, nazwa towaru, nazwa producenta, data produkcji].

Tablica 1. Struktura zbioru zawierającego informacje o klientach, zamówieniach i produktach.

dane adresowe klienta:	[**identyfikator klienta**, imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/mieszkania)]
zamówienia klienta:	[identyfikator zamówienia, **identyfikator klienta**, nazwa towaru, ilość towaru, wartość zamówienia, data zamówienia, data odbioru]
sprzedawane towary:	[identyfikator towaru, nazwa towaru, nazwa producenta, data produkcji]

Zakres danych przetwarzanych o kliencie oznaczony wyżej jako „*Zakres 1*", jak łatwo zauważyć, powstał na skutek relacji, jaka istnieje pomiędzy obiektami „*dane adresowe klienta*" i „*zamówienia klienta*". Relacja ta spowodowała, że zakres danych, zawarty w obiekcie „*dane adresowe klienta*", powiększony został o dane zawarte w obiektach „*zamówienia klienta*". Warto tutaj zauważyć, że w obiekcie oznaczonym „*zamówienia klienta*", zamawiany towar wskazany został bezpośrednio poprzez określenie jego nazwy, a nie relacji z obiektem, w którym opisane są wszystkie dane na jego temat. Zapis taki spowodował, że dane o sprzedawanych towarach zapisane w obiektach oznaczonych „*sprzedawane towary*", pomimo, że fizycznie zapisane są w tym samym zbiorze danych, nie poszerzają zakresu danych o kliencie oznaczony jako „*Zakres 1*".



Rys. 2. Zakres danych osobowych (pola oznaczone szarym tłem) przetwarzanych w zbiorze zawierającym informacje o danych adresowych klienta, zamówieniach oraz sprzedawanych towarach.

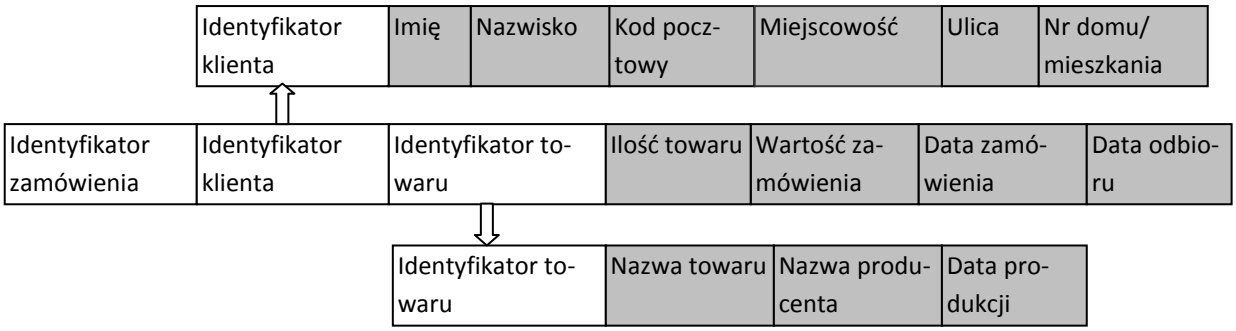
W przypadku relacyjnych baz danych praktycznie każdą informację można zapisać poprzez utworzenie odpowiedniej relacji. Dla struktury przedstawionej w tablicy 1, informacje o nazwie zamawianego towaru w zamówieniach klientów można zapisać alternatywnie w postaci relacji, co pokazano w tablicy 2.

Tablica 2. Struktura zbioru zawierającego informacje o klientach, zamówieniach i towarach z informacją o zamówionym towarze zapisaną w postaci relacji.

dane adresowe klienta:	[**identyfikator klienta**, imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/mieszkania)]
zamówienia klienta:	[identyfikator zamówienia, **identyfikator klienta**, ***identyfikator towaru***, ilość towaru, wartość zamówienia, data zamówienia, data odbioru]
sprzedawane towary:	[***identyfikator towaru***, nazwa towaru, nazwa producenta, data produkcji]

Przedstawiona powyżej, na pozór niewielka, zmiana w strukturze opisu obiektów w zbiorze danych powoduje, że na skutek wprowadzonej dodatkowo relacji pomiędzy zamówieniami klientów i sprzedawanymi produktami, zakres przetwarzanych informacji o klientach i wykonywanych przez nich zakupach powiększa się do zakresu:

<**Zakres 3**>: [imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/ mieszkania), nazwa towaru, nazwa producenta, data produkcji, ilość towaru, wartość zamówienia, data zamówienia, data odbioru].



Rys. 3. Zakres danych osobowych (pola oznaczone szarym tłem) przetwarzanych w zbiorze zawierającym informacje o danych adresowych klienta, zamówieniach oraz sprzedawanych towarach.

Analizując powyższy przykład można zauważyć, że istniejące w strukturze zbioru danych relacje, pomiędzy opisem poszczególnych obiektów, w istotny sposób wpływają na rzeczywisty zakres przetwarzanych informacji o wskazanym obiekcie.

Skróty i oznaczenia poszczególnych kategorii danych oraz wprowadzane ze względów technicznych indeksy i klucze, w celu podwyższenia efektywności przetwarzania, sprawiają często, że techniczny opis struktury zbioru danych, a zwłaszcza postać, w jakiej ta struktura jest zapisana w systemie informatycznym, nie zawsze są wystarczająco przejrzyste.

Stąd też, stosując się do § 4 pkt 3 rozporządzenia, należy w polityce bezpieczeństwa wskazać poszczególne grupy informacji oraz istniejące między nimi relacje identyfikując w ten sposób pełny zakres danych osobowych, jakie przetwarzane są w określonym zbiorze. Opisując struktury zbiorów danych nie jest konieczne przedstawianie pełnej dokumentacji struktury bazy danych z wyszczególnieniem oryginalnych nazw poszczególnych pól informacyjnych, stosowanych kluczy, czy też definicji wbudowanych obiektów funkcyjnych takich jak: procedury, funkcje, pakiety, i wyzwalacze[2] [4].

Wymóg wskazania powiązań pomiędzy polami informacyjnymi w strukturze zbiorów danych, określony w § 4 pkt 3 rozporządzenia, należy rozumieć jako wymóg wskazania wszystkich tych danych, występujących w strukturze zbioru, które poprzez występujące relacje można skojarzyć z określoną osobą. Tak, np. ze struktury zbioru pokazanej w tablicy 1, wynika, iż do danych, które można skojarzyć z osobą o podanym imieniu i nazwisku, należą nie tylko dane zawarte w tym obiekcie, ale również dane zawarte w obiekcie o nazwie „zamówienia klienta". Połączenie to, zgodnie z definicją danych osobowych, powoduje poszerzenie zakresu tych danych osobowych klienta, o dane zawarte w obiekcie „zamówienia klienta".

W § 4 pkt 3 rozporządzenia wyraźnie wskazano, że w polityce bezpieczeństwa ma być zawarty **opis struktury zbiorów** wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi. Opis ten może być przedstawiony w postaci formalnej (tak jak np. w tablicach 1, 2), w postaci graficznej pokazującej istniejące powiązania pomiędzy obiektami (rys. 1,2), jak również opisu tekstowego. Opis tekstowy, dla przypadku wskazanego w tablicy 1, może być następujący:

„*W zbiorze danych przetwarzane są dane osobowe klientów w zakresie:*

[2] Procedury, funkcje, pakiety, wyzwalacze – są to obiekty zapisane w bazie danych, tak jak inne dane. Obiektami tymi mogą być procedury i funkcje, które mogą być później używane przez aplikacje służąca do przetwarzania danych. Procedury, które uruchamiane są przy zajściu określonego zdarzenia nazywane są wyzwalaczami (ang. Trigger)

a) *dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu), oraz*

b) *wszystkich składanych przez danego klienta zamówieniach (nazwa towaru, ilość towaru, wartość zamówienia, data zamówienia i data odbioru).”*

W przytoczonym przykładzie opisu tekstowego, informacja o powiązaniach pomiędzy poszczególnymi polami informacyjnymi występującymi w strukturze zbioru, została przedstawiona w tekście, poprzez wskazanie w punkcie b), że w strukturze zbioru są też informacje o *wszystkich składanych przez **danego** klienta zamówieniach* (powiązanie zamówienia z danymi klienta, które należy rozumieć jako dane adresowe wymienione w punkcie a).

Należy pamiętać, że opis struktury zbiorów, o którym mowa w § 4 pkt 3 rozporządzenia, powinien być przedstawiony w sposób czytelny i zrozumiały.

Sposób przepływu danych pomiędzy systemami

W punkcie tym należy przedstawić sposób współpracy pomiędzy różnymi systemami informatycznymi oraz relacje, jakie istnieją pomiędzy danymi zgromadzonymi w zbiorach, do przetwarzania których systemy te są wykorzystywane. Przedstawiając przepływ danych można posłużyć się np. schematami, jak na rys. 1, które wskazują, z jakimi zbiorami danych system lub moduł systemu współpracuje, czy przepływ informacji pomiędzy zbiorem danych a systemem informatycznym jest jednokierunkowy np. informacje pobierane są tylko do odczytu, czy dwukierunkowy (do odczytu i do zapisu). W sposobie przepływu danych pomiędzy poszczególnymi systemami należy zamieścić również informacje o danych, które przenoszone są pomiędzy systemami w sposób manualny (przy wykorzystaniu zewnętrznych nośników danych) lub półautomatycznie – za pomocą teletransmisji (przy wykorzystaniu specjalnych funkcji eksportu/importu danych), wykonywanych w określonych odstępach czasu. Taki przepływ danych występuje np. często pomiędzy systemami Kadrowym i Płacowym (Rys. 1f) oraz pomiędzy systemami Kadrowym, Płacowym a systemem Płatnik służącym do rozliczeń pracowników z ZUS. Dla identyfikacji procesów przetwarzania danych osobowych szczególne znaczenie ma specyfikacja przepływu danych w systemach z rozproszonymi bazami danych.
W rozproszonej bazie danych, dane zlokalizowane są w różnych miejscach oddalonych od siebie terytorialnie i mogą zawierać, w zależności od lokalizacji, różne zakresy danych (tzw. niejednorodne oraz federacyjne, rozproszone bazy danych) [5]. Dla systemów korporacyjnych o zasięgu międzynarodowym, informacja o przepływie danych pomiędzy oddziałami korporacji znajdującymi się w państwach nie należących do Europejskiego Obszaru Gospodarczego musi być traktowana jako przepływ danych do państwa trzeciego[3] z wynikającymi z tego tytułu konsekwencjami[4].
W polityce bezpieczeństwa, w punkcie określającym sposób przepływu danych pomiędzy systemami nie jest wymagane szczegółowe omawianie rozwiązań technologicznych. Najistotniejsze jest wskazanie zakresu przesyłanych danych, podmiotu lub kategorii podmiotów, do których dane są przekazywane oraz ogólnych informacji na temat sposobu przesyłania danych (Internet, poczta elektroniczna, inne rozwiązania), które mogą decydować o rodzaju narzędzi niezbędnych do zapewnienia ich bezpieczeństwa podczas teletransmisji.

Przepływ danych pomiędzy poszczególnymi systemami informatycznymi, z punktu widzenia analizy zakresu przetwarzanych danych, można z punktu widzenia uzyskiwanego wyniku porównać do opisu relacji pomiędzy poszczególnymi polami informacyjnymi w strukturach zbiorów danych, co przedstawiono w punkcie 3. W przypadku przepływu danych pomiędzy systemami informatycznymi relacje, jakie powstają pomiędzy danymi przetwarzanymi w zbiorach poszczególnych systemów, nie wynikają z ich struktury. W przypadku przepływu danych pomiędzy systemami, dane z poszczególnych zbiorów łączone są dynamicznie poprzez wykonanie określonych funkcji systemu lub odpowiednio zdefiniowanych procedur zewnętrznych.

---

[3] Przez państwo trzecie – rozumie się zgodnie z art. 7 pkt 7 ustawy o ochronie danych osobowych państwo nie należące do Europejskiego Obszaru Gospodarczego

[4] Wymogi związane z przekazywaniem danych osobowych do państwa trzeciego określone zostały w art. 18 ust. 1 pkt 4, 41 ust. 1 pkt 7, 47 oraz 48 ustawy o ochronie danych osobowych.

Poprawne wykonanie zadań wymienionych w punktach 2 i 3 polityki bezpieczeństwa oraz przeprowadzona analiza przepływu danych powinna dać odpowiedź w zakresie klasyfikacji poszczególnych systemów informatycznych z punktu widzenia kategorii przetwarzanych danych osobowych. Klasyfikacja ta powinna w szczególności wskazywać, czy w danym systemie informatycznym są przetwarzane dane osobowe podlegające szczególnej ochronie, o których mowa w § 27 ustawy, czy też nie. Informacje te uzupełnione o dane dotyczące środowiska pracy poszczególnych systemów z punktu widzenia ich połączenia z publiczną siecią telekomunikacyjną powinny dać odpowiedź w zakresie wymaganych poziomów bezpieczeństwa, o których mowa w § 6 rozporządzenia. Stąd też podsumowaniem wykazów i opisów, o których mowa w punktach 2, 3 i 4 polityki bezpieczeństwa powinno być wskazanie w punkcie 4 wymaganych dla poszczególnych systemów informatycznych poziomów bezpieczeństwa.

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych

W tej części polityki bezpieczeństwa należy określić środki techniczne i organizacyjne niezbędne dla zapewnienia przetwarzanym danym poufności i integralności. Środki te powinny zapewnić jednocześnie rozliczalność wszelkich działań powodujących przetwarzanie danych osobowych. Należy pamiętać, iż środki, o których mowa wyżej, powinny być określone po uprzednim przeprowadzeniu wnikliwej analizy zagrożeń i ryzyka związanych z przetwarzaniem danych osobowych. Analiza zagrożeń i ryzyka powinna obejmować cały proces przetwarzania danych osobowych. Powinna uwzględniać podatność stosowanych systemów informatycznych na określone zagrożenia. Przy czym, podatność systemu należy tutaj rozumieć jako słabość w systemie, która może umożliwić zaistnienie zagrożenia np. włamania do systemu i utraty poufności danych. Podatnością taką jest np. brak mechanizmu kontroli dostępu do danych, który może spowodować zagrożenie przetwarzania danych przez nieupoważnione osoby. Analizując środowisko przetwarzania danych należy ocenić ryzyko zaistnienia określonych zagrożeń. Ryzyko to można określić jako prawdopodobieństwo wykorzystania określonej podatności systemu na istniejące w danym środowisku zagrożenia. Ważnym jest, aby zastosowane środki techniczne i organizacyjne niezbędne do zapewnienia poufności i integralności przetwarzanych danych były adekwatne do zagrożeń wynikających ze sposobu, jak również kategorii przetwarzanych danych osobowych. Środki te powinny zapewniać rozliczalność wszelkich działań (osób i systemów) podejmowanych w celu przetwarzania danych osobowych. Powinny one spełniać wymogi określone w art. 36 do 39 ustawy oraz być adekwatne do wymaganych poziomów bezpieczeństwa, o których mowa w § 6 rozporządzenia. W odniesieniu do rozliczalności działań podejmowanych przy przetwarzaniu danych osobowych zastosowane środki powinny w szczególności wspomagać kontrolę administratora nad tym, jakie dane osobowe i przez kogo zostały do zbioru wprowadzone (art. 38 ustawy).

Ryzykiem dla przetwarzania danych osobowych w systemie informatycznym podłączonym do sieci Internet jest np. możliwość przejęcia lub podglądu tych danych przez osoby nieupoważnione. Ryzyko to będzie tym większe im mniej skuteczne będą stosowane zabezpieczenia. Sygnalizacja istniejącego zagrożenia pozwala podjąć odpowiednie działania zapobiegawcze. Ważne jest często samo uświadomienie istnienia określonych zagrożeń np. wynikających z przetwarzania danych w systemie informatycznym podłączonym do sieci Internet czy też zagrożeń spowodowanych stosowaniem niesprawdzonych pod względem bezpieczeństwa technologii bezprzewodowej transmisji danych. Zidentyfikowane zagrożenia można minimalizować m.in. poprzez stosowanie systemów antywirusowych, mechanizmów szyfrowania, systemów izolacji i selekcji połączeń z siecią zewnętrzną (firewall), itp. Dla dużych systemów informatycznych (systemów połączonych z sieciami publicznymi, systemów z rozproszonymi bazami danych, itp.) wybór właściwych środków wymaga posiadania wiedzy specjalistycznej. Prawidłowe opracowanie polityki bezpieczeństwa przetwarzania danych osobowych w ww. zakresie jest procesem złożonym, wymagającym m.in. znajomości podstawowych pojęć i modeli używanych do opisywania sposobów zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele, o których mowa, jak również zagadnienia w zakresie zarządzania i planowania bezpieczeństwa systemów informatycznych, opisane zostały m.in. w Polskich Normach [2,3].

Podczas określania środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności i integralności przetwarzanych danych, jak również rozliczalności podejmowanych w tym celu działań, należy kierować się m.in. klasyfikacją poziomów bezpieczeństwa wprowadzoną w § 6 rozporządzenia. Dla każdego z wymienionych tam poziomów, które powinny być zidentyfikowane po wykonaniu zadań wymienionych w punktach 2, 3 i 4 polityki bezpieczeń-

stwa, niezbędne jest zapewnienie co najmniej takich środków bezpieczeństwa, które spełniają minimalne wymagania określone w załączniku do rozporządzenia.

Opis środków, o których mowa w § 4 pkt 5 rozporządzenia, powinien obejmować zarówno środki techniczne jak i organizacyjne. W odniesieniu np. do stosowanych mechanizmów uwierzytelniania powinny być wskazane i opisane zarówno zagadnienia dotyczące uwierzytelnienia użytkowników w systemach informatycznych jak i zagadnienia dotyczące uwierzytelnienia przy wejściu (wyjściu) do określonych pomieszczeń, a także sposób rejestracji wejść/wyjść itp. W przypadku stosowania narzędzi specjalistycznych (zapory ogniowe chroniące system informatyczny przed atakami z zewnątrz, systemy wykrywania intruzów (ang. Intrusion Detection System – IDS, itp.), należy wskazać w polityce bezpieczeństwa, że środki takie są stosowane, w jakim zakresie i w odniesieniu do jakich zasobów. W polityce bezpieczeństwa – dokumencie udostępnianym do wiadomości wszystkim pracownikom - nie należy opisywać szczegółów dotyczących charakterystyki technicznej i konfiguracji stosowanych narzędzi. Dokumenty opisujące szczegóły w tym zakresie powinny być objęte ochroną przed dostępem do nich osób nieupoważnionych.

Literatura

1. PN-I-02000: Zabezpieczenia w systemach informatycznych – Terminologia, PKN,1998
2. PN-I-13335-1: Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych, PKN, 1999
3. PN-ISO/IEC 17799 Technika Informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji, PKN, 2003
4. Tomasz Pełech, Gazeta IT nr 6(25) 20 czerwiec 2004
5. Andrzej Białas, Eugeniusz Januła i inni; (red. Andrzej Białas) Podstawy bezpieczeństwa systemów teleinformatycznych; Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2002
6. Paul Beynon-Davies, Systemy baz danych, Wydawnictwo Naukowo-Techniczne, Warszawa 1998.
7. Lech Banachowski, Bazy Danych – Tworzenie aplikacji, Akademicka Oficyna Wydawnicza PLJ, Warszawa 1998.

Przygotował: A. Kaczmarek

Wskazówki dotyczące sposobu opracowania instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji

Źródło: zasoby GIODO

Jednym z wymogów nałożonych na administratorów danych, zgodnie z §3 ust.1 przez rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024), jest opracowanie instrukcji, określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, zwanej dalej „instrukcją".

Opracowana instrukcja powinna być zatwierdzona przez administratora danych i przyjęta do stosowania, jako obowiązujący dokument. Zawarte w niej procedury i wytyczne powinny być przekazane osobom odpowiedzialnym w jednostce za ich realizację stosownie do przydzielonych uprawnień, zakresu obowiązków i odpowiedzialności. Np. zasady i procedury nadawania uprawnień do przetwarzania danych osobowych, czy też sposób prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych powinny być przekazane osobom zarządzającym organizacją przetwarzania danych, zaś sposób rozpoczęcia i zakończenia pracy, sposób użytkowania systemu, czy też zasady zmiany haseł - wszystkim osobom będącym jego użytkownikami, zasady ochrony antywirusowej, a także procedury wykonywania kopii zapasowych – osobom zajmującym się techniczną eksploatacją i utrzymaniem ciągłości pracy systemu.

W treści instrukcji powinny być zawarte ogólne informacje o systemie informatycznym i zbiorach danych osobowych, które są przy ich użyciu przetwarzane, zastosowane rozwiązania techniczne, jak również procedury eksploatacji i zasady użytkowania, jakie zastosowano w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. W przypadku, gdy administrator danych, do przetwarzania danych wykorzystuje nie jeden, lecz kilka systemów informatycznych, wówczas stosownie do podobieństwa zastosowanych rozwiązań powinien opracować jedną, ogólną instrukcję zarządzania lub opracować oddzielne instrukcje dla każdego z użytkowanych systemów. W zależności, zatem od przyjętego rozwiązania, inny będzie zakres opracowanych zagadnień w małych podmiotach, w których dane osobowe przetwarzane są przy pomocy jednego lub kilku komputerów i inny w dużych podmiotach, w których funkcjonują rozbudowane lokalne sieci komputerowe z dużą ilością serwerów i stacji roboczych przetwarzających dane przy użyciu wielu systemów informatycznych.

W instrukcji, o której mowa, powinny być wskazane systemy informatyczne, których ona dotyczy, ich lokalizacje, stosowane metody dostępu (bezpośrednio z komputera, na którym system jest zainstalowany, w lokalnej sieci komputerowej, czy też poprzez sieć telekomunikacyjną np. łącze dzierżawione, Internet). Instrukcja ta powinna obejmować zagadnienia dotyczące zapewnienia bezpieczeństwa informacji, a w szczególności elementy wymienione w §5 rozporządzenia, na które składają się:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem,
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu,
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
5) sposób, miejsce i okres przechowywania:
    a) elektronicznych nośników informacji zawierających dane osobowe,
    b) kopii zapasowych, o których mowa w pkt. 4,

6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia,
7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia,
8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

W celu zapewnienia ochrony przetwarzanych danych, w odniesieniu do każdego z wymienionych wyżej punktów, w treści instrukcji powinny być wskazane odpowiednie dla stosowanych systemów informatycznych zasady postępowania. Ogólne wskazówki dotyczące zagadnień, jakie powinny być zawarte w instrukcji w odniesieniu do wyżej wymienionych punktów przedstawiono poniżej.

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności (§ 5 pkt 1 rozporządzenia)

W punkcie tym powinny zostać opisane zasady przyznawania użytkownikowi identyfikatora w systemie informatycznym, jak również zasady nadawania lub modyfikacji uprawnień użytkownika do zasobów systemu informatycznego. Powyższe zasady powinny obejmować operacje związane z nadawaniem użytkownikom uprawnień do pracy w systemie informatycznym począwszy od utworzenia użytkownikowi konta, poprzez przydzielanie i modyfikację jego uprawnień aż do momentu usunięcia konta z systemu informatycznego. Procedura określająca zasady rejestracji użytkowników powinna w sposób jednoznaczny określać zasady postępowania z hasłami użytkowników uprzywilejowanych (tzn. użytkowników posiadających uprawnienia na poziomie administratorów systemów informatycznych), jak również zasady administrowania systemem informatycznym w przypadkach awaryjnych np. nieobecności administratora.

W instrukcji należy wskazać osoby odpowiedzialne za realizację procedur oraz rejestrowanie i wyrejestrowywanie użytkowników w systemie informatycznym.

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem (§ 5 pkt 2 rozporządzenia)

W punkcie tym powinien zostać opisany tryb przydzielania haseł, tj. wskazanie, czy hasła użytkowników przekazywane mają być w formie ustnej czy pisemnej oraz wskazanie zaleceń dotyczących stopnia ich złożoności. Powinny zostać również wskazane osoby odpowiedzialne za przydział haseł. Wskazanie to może być określone funkcjonalnie lub personalnie. Zaleca się, aby unikać przekazywania haseł przez osoby trzecie lub za pośrednictwem niechronionych wiadomości poczty elektronicznej. Użytkownik po otrzymaniu hasła powinien być zobowiązany do niezwłocznej jego zmiany, chyba, że system nie umożliwia wykonania takiej operacji. W zależności od stosowanych rozwiązań należy podać dodatkowe informacje dotyczące haseł, takie jak wymogi dotyczące ich powtarzalności czy też wymogi dotyczące zestawu tworzących je znaków. Powinna być również zawarta informacja o wymaganej częstotliwości i metodzie zmiany hasła np. czy zmiana hasła wymuszana jest po określonym czasie przez system informatyczny, czy też użytkownik sam musi o tym pamiętać. Przy określaniu częstotliwości zmiany haseł należy pamiętać, iż zgodnie z pkt IV ppk 2 załącznika do rozporządzenia, hasło użytkownika powinno być zmieniane nie rzadziej niż co 30 dni i składać się co najmniej z 6 znaków, jeżeli w systemie nie są przetwarzane dane, o których mowa w art. 27 ustawy lub 8 znaków, jeżeli takie dane są przetwarzane (pkt VII załącznika). Hasła w systemie informatycznym powinny być przechowywane w postaci zaszyfrowanej. Należy wskazać sposób przechowywania haseł użytkowników posiadających uprawnienia administratorów systemów informatycznych oraz sposób odnotowywania ich awaryjnego użycia. Dodatkowo, w przypadku zastosowania innych niż identyfikator i hasło metod weryfikacji tożsamości użytkownika, np. kart mikroprocesorowych czy też metod biometrycznych w instrukcji powinny być zawarte wytyczne w zakresie ich stosowania. Dla kart mikroprocesorowych np. należy wskazać sposób ich personalizacji, zaś dla metod biometrycznych sposób

pobierania danych biometrycznych w procesie rejestrowania użytkownika w systemie oraz sposób ich przechowywania.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu (§ 5 pkt 3 rozporządzenia)

W punkcie tym powinny być wskazane kolejne czynności, jakie należy wykonać w celu uruchamiania systemu informatycznego, a w szczególności zasady postępowania użytkowników podczas przeprowadzania procesu uwierzytelniania się (logowania się do systemu). Przestrzeganie określonych w instrukcji zasad powinno zapewniać zachowanie poufności haseł oraz uniemożliwiać nieuprawnione przetwarzanie danych. Należy również określić metody postępowania w sytuacji tymczasowego zaprzestania pracy na skutek opuszczenia stanowiska pracy lub w okolicznościach, kiedy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba. Użytkownik powinien być poinstruowany o konieczności wykonania operacji wyrejestrowania się z systemu informatycznego przed wyłączeniem stacji komputerowej oraz o czynnościach, jakie w tym celu powinien wykonać. Procedury przeznaczone dla użytkowników systemu powinny wskazywać sposób postępowania w sytuacji podejrzenia naruszenia bezpieczeństwa systemu np. w przypadku braku możliwości zalogowania się użytkownika na jego konto czy też w przypadku stwierdzenia fizycznej ingerencji w przetwarzane dane lub użytkowane narzędzia programowe lub sprzętowe.

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania (§ 5 pkt 4 rozporządzenia)

W punkcie tym należy wskazać metody i częstotliwość tworzenia kopii zapasowych danych oraz kopii zapasowych systemu informatycznego używanego do ich przetwarzania. Należy określić, dla jakich danych wykonywane będą kopie zapasowe, typ nośników, na których kopie będą wykonywane oraz narzędzia programowe i urządzenia, które mają być do tego celu wykorzystywane. W procedurze wykonywania kopii powinien być określony harmonogram wykonywania kopii zapasowych dla poszczególnych zbiorów danych wraz ze wskazaniem odpowiedniej metody sporządzania kopii (kopia przyrostowa, kopia całościowa). Fragment instrukcji dotyczący wykonywania kopii zapasowych w przypadku, gdy procedury wykonywania tych kopii są złożone, może się odwoływać do procedur szczegółowych dedykowanych poszczególnym zbiorom danych, czy też systemom informatycznym. Procedury takie powinny być wówczas załączone do instrukcji zarządzania. W procedurach określających zakres i sposób wykonywania kopii zapasowych powinny być wskazane okresy rotacji oraz całkowity czas użytkowania poszczególnych nośników danych. Powinny być określone procedury likwidacji nośników zawierających kopie zapasowe danych po ich wycofaniu na skutek utraty przydatności lub uszkodzenia. Procedura likwidacji nośników zawierających dane osobowe powinna uwzględniać wymogi zawarte w pkt VI ppkt 1 załącznika do rozporządzenia. Wymogi te nakazują, aby urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawiać zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadzać w sposób uniemożliwiający ich odczytanie.

Sposób, miejsce i okres przechowywania

a) **elektronicznych nośników informacji zawierających dane osobowe,**

b) **kopii zapasowych, o których mowa w §5 pkt. 4 rozporządzenia.**

W tym punkcie instrukcji należy określić sposób i czas przechowywania wszelkiego rodzaju nośników informacji (dyskietki, płyty CD, taśmy magnetyczne). Należy wskazać pomieszczenia, przeznaczone do przechowywania nośników informacji, jak również sposób zabezpieczenia tych nośników przed nieuprawnionym przejęciem, odczytem, skopiowaniem lub zniszczeniem.

Przy opracowywaniu zaleceń dotyczących sposobu i czasu przechowywania nośników informacji należy uwzględnić, iż zgodnie z wymogami pkt IV ppkt 4a załącznika do rozporządzenia, kopie zapasowe przechowuje się w miejscach za-

bezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem. Należy uwzględnić wymogi określone w pkt IV ppkt 4b załącznika do rozporządzenia nakazujące, aby kopie awaryjne bezzwłocznie usuwać po ustaniu ich użyteczności.

W przypadku przekazywania nośników informacji podmiotom zewnętrznym w celu bezpiecznego ich przechowywania, np. stosowane dość często deponowanie kopii zapasowych w skarbcach bankowych, należy określić procedury przekazywania nośników informacji tym podmiotom oraz wskazać metody zabezpieczania przekazywanych nośników informacji przed dostępem osób nieuprawnionych podczas ich transportu/przekazywania.

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia (§ 5 pkt 6 rozporządzenia)

W opisie zabezpieczeń systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia należy określić obszary systemu informatycznego narażone na ingerencję wirusów komputerowych oraz wszelkiego rodzaju innego szkodliwe oprogramowanie. Należy wskazać możliwe źródła przedostania się szkodliwego oprogramowania do systemu oraz działania, jakie należy podejmować, aby minimalizować możliwość zainstalowania się takiego oprogramowania. Niezależnie od wskazania czynności profilaktycznych przed przedostaniem się do systemu oprogramowania szkodliwego, w instrukcji należy wskazać zastosowane narzędzia programowe, których zadaniem jest przeciwdziałanie skutkom szkodliwego działania takiego oprogramowania. Należy wskazać oprogramowanie antywirusowe, które zostało zainstalowane, określić metody i częstotliwość aktualizacji definicji wirusów oraz osoby odpowiedzialne za zarządzanie tym oprogramowaniem. Powinny być przedstawione również procedury postępowania użytkowników na okoliczność zidentyfikowania określonego typu zagrożeń. Użytkownik powinien być poinformowany o czynnościach, które powinien wykonać w przypadku, gdy oprogramowanie zabezpieczające wskazuje zaistnienie zagrożenia. W przypadku, gdy stosowane są inne niż oprogramowanie antywirusowe metody ochrony przed szkodliwym oprogramowaniem należy je wskazać i przedstawić procedury związane z ich stosowaniem. Do metod takich mogą należeć m. in. fizyczne odłączenie urządzeń umożliwiających odczyt danych z wymiennych nośników informatycznych poszczególnych stacji komputerowych (np. odłączenie stacji CD, stacji dyskietek, itp.) i wyznaczenie wydzielonego stanowiska w sieci komputerowej do wymiany danych za pomocą nośników zewnętrznych.

Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4

Zgodnie z § 7 ust. 1 pkt. 4 rozporządzenia, dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system ten powinien zapewnić odnotowanie informacji o udostępnieniach danych odbiorcom, w rozumieniu art. 7 pkt. 6 ustawy, zawierające informacje komu, kiedy i w jakim zakresie dane osobowe zostały udostępnione, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych. Wynika stąd, że system informatyczny wykorzystywany do przetwarzania danych osobowych powinien posiadać funkcjonalności umożliwiające odnotowanie wspomnianych wyżej informacji. Sposób oraz forma odnotowania, jak wynika z § 5 pkt. 7 rozporządzenia, powinna zostać określona w instrukcji. Przy czym szczególną uwagę zwrócić należy na fakt, iż nie jest wystarczające odnotowanie w formie papierowej informacji, o których mowa w § 7 ust. 1 pkt 4, zatem instrukcja nie może przewidywać takiego sposobu realizacji wspomnianego wymogu, gdyż byłoby to niezgodne z przedstawioną w ustawie definicją systemu informatycznego.

Zauważyć należy również, iż w przypadku przetwarzania danych osobowych nie tylko w jednym systemie informatycznym wymagania, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu. Wynika stąd, że odnotowanie informacji o udostępnieniach możliwe jest w jednym systemie tylko wtedy, gdy zbiór danych przetwarzany w dwóch lub więcej systemach dotyczy dokładnie tych samych osób. Przykładem takiej sytuacji jest korzystanie przez wiele aplikacji z tej samej bazy danych. Niedopuszczalne jest natomiast odnotowanie wskazanej informacji wyłącznie w jednym systemie, gdy grupy osób, których dane przetwarzane są w poszczególnych systemach nie są dokładnie tożsame. W sytuacji, gdy zbiór osób, których dane przetwarzane są w jednym systemie różni się od zbioru osób, których dane przetwarzane są w drugim systemie i nie zachodzi relacja zawierania się pomiędzy tymi zbiorami, wówczas konieczne jest odnotowanie

informacji o udostępnieniach odrębnie w każdym systemie obsługującym te zbiory lub ewentualnie w systemie dedykowanym odnotowaniu informacji, o których mowa w § 7 ust. 1 pkt 4.

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych (§ 5 pkt 8 rozporządzenia)

W punkcie tym należy określić cel, zakres, częstotliwość oraz procedury wykonywania przeglądów i konserwacji systemu informatycznego. Należy wskazać podmioty i osoby uprawnione do dokonywania przeglądów i konserwacji systemu informatycznego. Procedury wykonywania czynności konserwacyjnych systemu, w przypadku, gdy czynności te zleca się osobom nie posiadającym upoważnień do przetwarzania danych (np. specjalistom z firm zewnętrznych), powinny określać sposób, w jaki czynności te nadzorowane są przez administratora danych. W przypadku przekazywania do naprawy nośników informatycznych zawierających dane osobowe należy określić sposób usuwania danych osobowych z tych nośników, przed ich przekazaniem. W procedurach dotyczących naprawy sprzętu komputerowego należy uwzględnić wymóg określony w punkcie **V**I ppkt. 3 załącznika do rozporządzenia, który nakazuje, aby urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do naprawy, pozbawiać wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie, bądź też naprawiać je pod nadzorem osoby upoważnionej przez administratora danych.

Wybrane przykłady zgód (złe i dobre)

Wskazówka nr 1: orzeczenie NSA (sygn. akt II SA 2135/2002)

- **Zgoda na przetwarzanie danych osobowych musi mieć charakter wyraźny, a jej wszystkie aspekty muszą być jasne dla podpisującego w momencie jej wyrażania.**
- Czynności takiej nie konwaliduje późniejsze poinformowanie o treści regulaminu, ani możliwość zgłoszenia zastrzeżeń wobec pewnych form przetwarzania danych.

Wskazówka nr 2: …z orzecznictwa wynika, że…

- zgoda:
  - **nie może mieć charakteru abstrakcyjnego;**
  - **nie może dotyczyć przetwarzania danych w ogóle;**
  - **musi się odnosić do skonkretyzowanego stanu faktycznego;**
  - **musi obejmować jedynie pewnie i jednoznacznie określone dane;**
  - **musi mieć sprecyzowany sposób i cel ich przetwarzania.**

Wskazówka nr 3: zgoda na przetwarzanie danych osobowych jako oświadczenie woli

- Wyrażenie zgody
- Podpis
- Wskazanie zakresu podmiotowego
  - (kto? komu?)
- Wskazanie zakresu przedmiotowego
  - (na co wyraża się zgodę? – cel wyrażenia zgody)
  - (wskazanie zakresu danych osobowych)
  - (gdzie i kiedy zgoda jest wyrażana?)
    - (wskazanie zakresu czasowego i miejscowego obowiązywania zgody)
      - (wskazanie ewentualnej formy, trybu itp. obowiązywania zgody)

Wskazówka nr 4: idea ogólna

w tworzeniu dokumentów korespondencji handlowej, pism rynku pracy oraz pism urzędowych zakłada się, że współcześnie powinny obowiązywać następujące zasady:

- ***„minimum słów”***
- ***„maksimum treści”***
- ***„nie obrażać”***
- ***„nie marnować czasu”***
- ***„w Polsce pisać po polsku”***

Wybrane przykłady

W odniesieniu do tych zasad można zaprezentować przykłady dobrych i złych praktyk przygotowywania takich dokumentów, jak np. zgody na przetwarzanie danych osobowych w powiązaniu z wymogami art. 57, 60, 62 i 94 ustawy o SIO.

Przykład zgody nr 1 (zgoda na pozyskiwanie i przechowywanie danych osobowych – art. 58, 59, 60, 94)

Walor GEMTT:	Bardzo niski (1)	Niski (2)	Trudny do określenia (3)	Wysoki (4)	Bardzo wysoki (5)
Gramatyczny		*			
Estetyczny				*	
Merytoryczny	*				
Typograficzny		*			
Typologiczny				*	

OŚWIADCZENIE ZGODY

Ja ..... legitymujący/ca się dowodem osobistym

(imię i nazwisko)

nr ..... oświadczam, że:

(nr dowodu osobistego)

1) wyrażam zgodę na pozyskiwanie moich danych osobowych z bazy głównej SIO o których mowa w art. **58** ust. **1** pkt **2** i art. **59** pkt **2** ustawy z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej (Dz. U. z 2011 r. Nr 139, poz. 814 z późn. zm.),

2) wyrażam zgodę na przechowywanie moich danych osobowych w bazie lokalnej SIO przez okres dłuższy niż **5** lat od daty ostatniej dokonanej modyfikacji, o której mowa w art. **94** pkt. **3** ustawy z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej (Dz. U. z 2011 r. Nr 139, poz. 814 z późn. zm.).

....

(data i czytelny własnoręczny podpis pracownika) (podpis dyrektora)

Przykład zgody nr 5 (zgoda na pozyskiwanie danych osobowych – art. 58, 59, 60)

Walor GEMTT:	Bardzo niski (1)	Niski (2)	Trudny do określenia (3)	Wysoki (4)	Bardzo wysoki (5)
Gramatyczny				*	
Estetyczny				*	
Merytoryczny					*
Typograficzny					*
Typologiczny				*	

Wojciech Jamilicz

Wrocław, 26.02.2013

Miejski Zespół Obsługi Szkół i Przedszkoli
ul. Długa 23
54-202 Wrocław

Wyrażam zgodę na pozyskanie moich danych osobowych:
ze zbioru PESEL w zakresie płci, daty i miejsca urodzenia oraz obywatelstwa;
z bazy danych SIO w zakresie wykształcenia, przygotowania pedagogicznego, posiadanych kwalifikacji do nauczania, stopnia awansu zawodowego, ukończonych form dokształcania i doskonalenia zawodowego,
w celu realizacji zadań związanych z obsługą ekonomiczno administracyjną realizowanych przez Miejski Zespół Obsługi Szkół i Przedszkoli we Wrocławiu w okresie pozostawania pracownikiem Szkoły Podstawowej nr 60 we Wrocławiu.
Wyrażenie zgody wynika z art. 60 ustawy o systemie informacji oświatowej (Dz. U. z 2011 r. Nr 139, poz. 814 z późn. zm.) w powiązaniu z art. 59, gdzie zdefiniowano wskazany wyżej zakres danych osobowych.

Przykład zgody nr 6 (zgoda na przechowywanie danych osobowych – art. 58, 59, 60, 94)

Walor GEMTT:	Bardzo niski (1)	Niski (2)	Trudny do określenia (3)	Wysoki (4)	Bardzo wysoki (5)
Gramatyczny				*	
Estetyczny				*	
Merytoryczny					*
Typograficzny					*
Typologiczny				*	

Wojciech Jamilicz

Wrocław, 26.02.2013

Liceum Ogólnokształcące nr 94
ul. Długa 23
54-202 Wrocław

Wyrażam zgodę na przechowywanie moich danych osobowych zgromadzonych w lokalnej bazie danych SIO do 26.02.2020 roku w celu wykorzystania ich do przygotowywania raportów statystycznych na potrzeby Liceum Ogólnokształcącego nr 94 we Wrocławiu.

Wyrażenie zgody wynika z art. 94 ustawy o systemie informacji oświatowej (Dz. U. z 2011 r. Nr 139, poz. 814 z późn. zm.) w powiązaniu z art. 27-29, gdzie wskazano zakres danych osobowych przechowywanych w lokalnej bazie danych SIO.

Przed podpisaniem zgody zapoznałem się z zakresem danych osobowych przechowywanych w lokalnej bazie danych SIO.

Przykład zgody nr 7 (zgoda ogólna)

Walor GEMTT:	Bardzo niski (1)	Niski (2)	Trudny do określenia (3)	Wysoki (4)	Bardzo wysoki (5)
Gramatyczny	*				
Estetyczny	*				
Merytoryczny	*				
Typograficzny	*				
Typologiczny	*				

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

KOWALSKI JAN
54-200 Wrocław
Oś. Jasne 18

.....
/nazwisko imię adres
osoby składającej oświadczenie/

OŚWIADCZENIE

Ja niżej podpisany Jan Kowalski oświadczam, iż wyrażam zgodę na przetwarzanie przez firmę „ZAUFANIE" Sp. Z o.o. w Wrocławiu, zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. nr 133, poz. 883), w celach marketingowych moich danych osobowych:
Imię i nazwisko: Jan Kowalski
Adres miejsca zamieszkania: Oś. Jasne 18 / 54-200 Wrocław
Inne: prenumerator czasopisma „Zaufanie"

Równocześnie upoważniam także Spółkę „ZAUFANIE" do przesyłania mi drogą pocztową najnowszych informacji o nowych publikacjach oferowanych przez Spółkę.

Wrocław dnia 26-10-11r.

....
/data/ /miejscowość/ */czytelny własnoręczny podpis/*

Przykład zgody nr 8 (zgoda ogólna)

Walor GEMTT:	Bardzo niski (1)	Niski (2)	Trudny do określenia (3)	Wysoki (4)	Bardzo wysoki (5)
Gramatyczny				*	
Estetyczny				*	
Merytoryczny					*
Typograficzny					*
Typologiczny				*	

Jan Kowalski

Wrocław, 26.10.2011

ZAUFANIE Sp. z o. o.
ul. Długa 23
54-202 Wrocław

Wyrażam zgodę na przetwarzanie moich danych osobowych do końca 2011 roku w celach marketingowych polegających na informowaniu mnie drogą pocztową o nowych publikacjach.

Zgoda na przetwarzanie dotyczy następujących danych osobowych:
imię i nazwisko: Jan Kowalski;
adres miejsca zamieszkania: Os. Jasne 18, 54-200 Wrocław;
rodzaj zobowiązania: prenumerator czasopisma „Zaufanie".

podpis

Przykłady upoważnień

Przykład upoważnienia proponowanego przez CIE

PRZYKŁAD

Pieczęć / logo / inne oznaczenie organu upoważniającego
Np.: *Kuratorium Oświaty*
Wójt Gminy X
Szkoła Podstawowa Nr ... w ……..

……
(Sygnatura dokumentu lub inne oznaczenie)

Miejscowość, 2012- -

UPOWAŻNIENIE
DO DOSTĘPU DO BAZY DANYCH SIO

Na podstawie art. 72 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej (Dz. U. Nr 139, poz. 814, z późn. zm.) upoważniam Panią /Pana

……

(imię i nazwisko, stanowisko, komórka organizacyjna)

……

do dostępu w moim imieniu do bazy danych SIO
na okres* do dnia ……

……
(podpis oraz pieczęć osoby upoważniającej)

Przykład upoważnienia proponowany przez autora opracowania

Marcin Dyrektorewicz

Dyrektor

Szkoła Podstawowa nr 999 we Wrocławiu

Wrocław, 26.02.2013

Marta Siocka

Referent do spraw administracyjnych

Szkoła Podstawowa nr 999 we Wrocławiu

ODO.142.78.2.DMD

Upoważniam Panią Martę Siocką (numer PESEL 82061105917), wykonującą obowiązki operatora aplikacji SIO, do dostępu do bazy danych SIO w zakresie gromadzenia i przekazywania danych identyfikacyjnych oraz danych dziedzinowych, o których stwierdza się w rozdziale 2 ustawy z dnia 15 kwietnia 2011 roku o systemie informacji oświatowej (Dz. U. Nr 139, poz. 814, z późn. zm.) na okres do 26.02.2018 roku (okres ważności upoważnienia).

Udzielenie upoważnienia wynika z brzmienia art. 72 wskazanej wyżej ustawy w powiązaniu z art. 69-71.

Klauzula o zachowaniu tajemnicy (art. 70 ust. 3 pkt 9 wymienionej wyżej ustawy):

„Osoba upoważniona do przetwarzania danych objętych zakresem dostępu do bazy danych systemu informacji oświatowej, określonym w niniejszym upoważnieniu, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia, oraz zachowania w tajemnicy informacji o ich zabezpieczeniu."

Podpis osoby upoważnionej jest jednocześnie znakiem potwierdzenia zapoznania się z klauzulą o zachowaniu tajemnicy.

podpis osoby upoważniającej

podpis osoby upoważnionej

Bibliografia

Barta Janusz, Fajgielski Paweł, Markiewicz Ryszard, **Ochrona danych osobowych Komentarz,** lipiec 2011, Wolters Kluwer Polska
Publikacja jest jedynym na rynku tak obszernym Komentarzem do Ustawy o ochronie danych osobowych. Autorzy omawiają założenia ustawy i najistotniejsze problemy związane z ochroną danych osobowych oraz prezentują polskie rozwiązania prawne w ujęciu prawa międzynarodowego, w tym unijnego.

Jagielski Mariusz, **Prawo do ochrony danych osobowych**, 2010, Wolters Kluwer Polska
Książka poświęcona jest problematyce ochrony danych osobowych i przedstawia ogól problematyki z tym związanej.

Andrzej Drozd, **Ustawa o ochronie danych osobowych. Komentarz wzory pism i przepisy,** 2008, LexisNexis
Komentarz zawiera szczegółowe omówienie przepisów ustawy o ochronie danych osobowych. Autor w sposób przystępny wyjaśnia zagadnienia z zakresu ochrony danych osobowych, wykorzystując najnowsze orzecznictwo sądów administracyjnych.

Przemysław Kral, **Wzorcowa dokumentacja ochrony danych osobowych z komentarzem (z suplementem elektronicznym),** 2007, Ośrodek Doradztwa i Doskonalenia Kadr
Książka zawiera kompleksowy zestaw firmowych dokumentów niezbędnych w prawidłowym funkcjonowaniu podmiotów gospodarczych.

Ochrona danych osobowych. Wybór zagadnień, 2010, Omni Modo
Publikacja jest zbiorem artykułów dotyczących wybranych - najciekawszych zagadnień dotyczących ochrony danych osobowych. Ambicją autorów - praktyków, w większości byłych pracowników Biura GIODO, było przedstawienie w sposób klarowny zagadnień nurtujących administratorów danych.

Kontrola przetwarzania i ochrony danych osobowych. Studium teoretyczno-prawne
Paweł Fajgielski, 2008, KUL

Adam Gałach, **Instrukcja ochrony danych osobowych w systemie informatycznym,** 2004, Ośrodek Doradztwa i Doskonalenia Kadr

Wizerunek – jak publikować legalnie?

Pismo przewodnie kierowane we wrześniu do szkół i placówek oświatowych

Szanowni Państwo,

Ochrona danych osobowych i dóbr osobistych w szkołach i placówkach oświatowych jest na poziomie wymagającym ciągłej troski.

Obecnie organizujemy szkolenia, w których obok przedstawienia w komunikatywnej i praktycznej formie problematyki ochrony danych osobowych w odniesieniu do funkcjonowania szkoły, prezentowany jest dodatkowo przykład przeprowadzenia lekcji na temat ochrony wizerunku: „Wizerunek – jak publikować legalnie?".
Uczestnik szkolenia pozna wszystkie potrzebne szczegóły dotyczące możliwości przeprowadzenia takiej lekcji „u siebie", a także nauczenia innych tego, jak taką lekcję przeprowadzić.
Pod adresem egocki.pl/odo/propozycja_lekcji.pdf jest dostępny plik, który zawiera uszczegółowienie zakresu tematycznego, wskazanie celów do osiągnięcia w czasie lekcji oraz propozycję przebiegu lekcji. Prowadzący szkolenie posiada stosowną wiedzę i doświadczenie (także dydaktyczne). Wszystkie przygotowane do przeprowadzenia lekcji treści, materiały, pomoce a także scenariusz lekcji zostaną udostępnione uczestnikom szkoleń do swobodnego użytkowania (pozostając w zgodzie z powszechną licencją Creative Commons Uznanie autorstwa 3.0 Polska).

Pod adresem egocki.pl/odo/program_odo_sipo.pdf jest dostępny plik, który zawiera szczegółową propozycję programu szkolenia z zakresu ochrony danych osobowych w szkole i placówce oświatowej (…szkolenia, którego częścią jest realizacja wyżej przedstawionej propozycji). Jednym z celów szkolenia jest w szczególności wyposażenie uczestników szkolenia w wiedzę, umiejętności i materiały, które pozwolą im przeprowadzić podobne szkolenie w czasie posiedzenia rady pedagogicznej. W ostatnich kilku latach prowadzący szkolenie przeprowadził wiele podobnych szkoleń; wie precyzyjnie „o co chodzi" na szkoleniu rady pedagogicznej.

Polecamy przy okazji zainteresowanie się programem edukacyjnym GIODO „Twoje dane – Twoja sprawa" (giodo.gov.pl/1520244/id_art/8800/j/pl/). W czasie proponowanego wyżej szkolenia jest także relacjonowany ów program edukacyjny GIODO, a uczestnicy szkolenia są zachęcani do wzięcia w nim udziału.

Pozostajemy do Państwa dyspozycji w przypadku zainteresowania przedstawionymi wyżej propozycjami.

Krzysztof.Slugocki@gmail.com

Propozycja przeprowadzenia lekcji

Krzysztof Sługocki, 05.09.2015

501 091 995, Krzysztof.Slugocki@gmail.com

Wizerunek – jak publikować legalnie?

Ochrona wizerunku

Uczniowie dowiedzą się (poprzez wykład i odpowiednie ćwiczenia), czym są dobra osobiste i wizerunek. Zapoznają się z prawnymi i etycznymi aspektami rozpowszechniania wizerunku oraz zastanowią się, jak postępować w codziennych (szkolnych) sytuacjach związanych z utrwalaniem wizerunku.

Zostanie przekazana odpowiednio do wieku uczniów „wiedza w pigułce" w zakresie:

- *wizerunek jako dobro osobiste;*
- *zasady rozpowszechniania wizerunku;*
- *rozpowszechnianie wizerunku a współczesna technologia;*
- *uzyskanie zgody na rozpowszechnianie wizerunku.*

Cele

Uczniowie:

- *wiedzą, czym są dobra osobiste i wizerunek;*
- *rozumieją, na jakich zasadach można rozpowszechniać wizerunek innych osób;*
- *potrafią rozpoznać sytuacje, w których mogliby zranić innych lub naruszyć ich prawa, publikując ich wizerunek w sieci;*

Propozycja przebiegu lekcji

1. *Ćwiczenie „Portret" – wprowadzenie do pojęć: „utrwalenie", „publikacja" i „rozpowszechnienie" „wizerunku"; zdefiniowanie wizerunku (przez uczniów); poszerzenie definicji wizerunku jako „dobra osobistego".*
2. *Ćwiczenie „Czy obraz (zdjęcie, fotografia) jest wizerunkiem, czy podlega ochronie?" – utrwalenie pojęcia „wizerunek"; wprowadzenie do zagadnienia „ochrony wizerunku".*
3. *Omówienie przykładów „rozpowszechniania wizerunku" w oparciu o doświadczenia i spostrzeżenia uczniów.*
4. *„Ochrona wizerunku". Omówienie możliwych, poprawnych i zgodnych z prawem reakcji i zachowań głównie po stronie uczniów w sytuacjach rozpowszechniania wizerunku i podejrzenia naruszenia dobra osobistego jakim jest wizerunek.*

W czasie lekcji zostaną wykorzystane zasoby, treści i materiały przygotowane przez prowadzącego, które zostaną w całości przekazane do użytku szkolnego. Lekcja zakończy się w szczególności przeprowadzeniem zadania sprawdzającego oraz rozdaniem „mini słowniczka" podstawowych pojęć. Zostaną także zaprezentowane możliwe inne tematy z zakresu prawa nowych technologii i ochrony dóbr w społeczeństwie informacyjnym.

Skrypt: wizerunek — jak publikować legalnie?

Informacje o lekcji

Eksperci:	Wojciech Klicki, Małgorzata Szumańska, Kamil Śliwowski
Autorka wiedzy w pigułce:	Anna Obem
Autorka scenariusza:	Izabela Meyza
Organizacja publikująca:	Fundacja Panoptykon
Przedmiot:	Wiedza o społeczeństwie, informatyka, etyka
Sugerowany poziom kształcenia:	Szkoły ponadgimnazjalne
Licencja:	Creative Commons Uznanie autorstwa — Na tych samych warunkach 3.0 Polska

Wiedza w pigułce

Każdemu człowiekowi przysługuje prawo do ochrony swoich dóbr osobistych przed naruszeniami ze strony innych osób. Dobrami osobistymi są m.in. dobre imię, cześć, zdrowie, swoboda sumienia, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa czy artystyczna, prawo do kultu osoby zmarłej, jak również wizerunek. Dobra te mają charakter niemajątkowy (nie można ich sprzedać) i ściśle wiążą się z daną osobą.

Wizerunek jako dobro osobiste

Wizerunek jest jednym z dóbr osobistych i też podlega ochronie. Wizerunek jest rozumiany bardzo szeroko: mogą to być cechy twarzy i całej postaci, budowa ciała — innymi słowy cechy wyglądu, na podstawie których można kogoś rozpoznać. Prawo do ochrony wizerunku, podobnie jak innych dóbr osobistych, przysługuje tylko osobom żyjącym. Ochrona wizerunku nie dotyczy postaci fikcyjnych, np. Myszki Miki i Sherlocka Holmesa, ani zmarłych, np. Marii Skłodowskiej-Curie i Mikołaja Kopernika.

Wizerunek może być utrwalany na różne sposoby, np. w formie zdjęcia, obrazu, filmu, karykatury; przy pomocy różnych narzędzi, np. aparatu fotograficznego, smartfona, tabletu, drona, a także ołówka i kartki papieru. Warto pamiętać o tym, że osobie utrwalającej czyjś wizerunek (np. malarzowi czy osobie robiącej zdjęcie) przysługują określone uprawnienia — efekt ich pracy (np. obraz, zdjęcie) jest chroniony przez prawo autorskie. W tej lekcji nie zajmujemy się jednak tym zagadnieniem, skupiamy się natomiast na zasadach wykorzystywania cudzego wizerunku.

Nie należy utrwalać wizerunku osoby, która sobie tego nie życzy; standardem powinno być zapytanie najpierw o zgodę. Utrwalenie czyjegoś wizerunku może wiązać się z naruszeniem innych dóbr osobistych tej osoby, np. dobrego imienia lub czci, jeśli zostanie sfotografowana w sytuacji ośmieszającej, prywatnej (np. podczas pogrzebu) lub intymnej.

Jeśli wizerunek nie jest utrwalany w celach prywatnych, a np. w celach biznesowych, może dochodzić do przetwarzania danych osobowych — na które trzeba uzyskać zgodę lub wykazać inną podstawę prawną (więcej na ten temat w lekcji pt. „Podstawy ochrony danych osobowych").

Zasady rozpowszechniania wizerunku

Według ogólnej zasady nie wolno rozpowszechniać wizerunku danej osoby — czyli umożliwiać zapoznania się z nim bliżej nieokreślonemu, niezamkniętemu kręgowi osób — bez jej zgody. Od tej zasady są wyjątki. Można udostępniać czyjś wizerunek, jeśli:

- dana osoba otrzymała wynagrodzenie za pozowanie — np. model czy modelka;
- dana osoba na zdjęciu stanowi jedynie szczegół, część większej całości — np. przypadkowi turyści, którzy znaleźli się na dalszym planie czyjejś fotografii z wakacji i nie są tematem tego zdjęcia;
- jest to osoba powszechnie znana, a wizerunek utrwalono w związku z wykonywaniem przez nią funkcji publicznych: politycznych, społecznych, zawodowych itp. — np. prezydent państwa w trakcie przemówienia czy artysta na scenie.

Rozróżnienie, czy dana sytuacja może być zakwalifikowana jako wyjątek, nie zawsze jest proste. Oto przykłady sytuacji, które takimi wyjątkami nie są:

- zdjęcie klasowe — każdy uczeń jest tematem tego zdjęcia;
- zdjęcie, na którym ktoś znajduje się w tle, ale np. w charakterystycznej, przykuwającej uwagę pozie — ta osoba przestaje być tłem, a staje się tematem zdjęcia;
- nagranie nauczyciela prowadzącego lekcję — nawet popularnego nauczyciela trudno nazwać osobą powszechnie znaną;
- zdjęcie znanego polityka czy aktora na plaży z rodziną — to sytuacja prywatna, a nie zawodowa.

Wizerunek mogą wykorzystywać (ale nie rozpowszechniać) różne instytucje, np. szkoła, żeby wydać legitymację; urząd, żeby wydać paszport, dowód osobisty czy prawo jazdy. Urzędnicy mogą wykorzystać wizerunek (a więc w praktyce najczęściej przyniesione im zdjęcie) tylko w tym celu, do jakiego upoważnia ich prawo.

Rozpowszechnianie wizerunku a współczesna technologia

Trudno wyznaczyć wyraźną granicę, gdzie zaczyna się, a gdzie kończy rozpowszechnianie wizerunku. Dostępne technologie sprawiają, że od utrwalenia wizerunku do jego rozpowszechnienia jest naprawdę niedaleko. Użytkownicy smartfonów i tabletów mają do dyspozycji aplikacje, które za jednym kliknięciem przenoszą zrobione właśnie zdjęcie do chmury, by po automatycznej korekcie opublikować je w sieci lub przesłać drugiej osobie (aplikacje Instagram, Snapchat). Pokazanie zdjęcia koledze nie jest rozpowszechnianiem, ale opublikowanie go na otwartym blogu w sieci — już tak. Opublikowanie tego samego wizerunku w zamkniętej grupie na portalu społecznościowym przynajmniej teoretycznie nie jest rozpowszechnianiem. Sytuacja jest jednak trudna do jednoznacznej oceny, gdy grupa jest duża lub dostęp do niej swobodny. Co więcej — wystarczy, że jeden z członków grupy skopiuje wizerunek i umieści go na innym portalu, który jest publicznie dostępny, by wizerunek został rozpowszechniony.

Rozróżnienie sytuacji granicznych komplikują też dostępne dzięki najnowszym gadżetom możliwości powiększania obrazu. Wizerunek osoby, która dawniej byłaby tylko w tle zdjęcia, dziś może być powiększony i wyostrzony do tego stopnia, że będzie możliwe nawet oznaczenie jej za pomocą funkcji rozpoznawania twarzy. Na rozpowszechnianie takiego zdjęcia trzeba już uzyskać zgodę.

Uzyskanie zgody na rozpowszechnianie wizerunku

Jeśli masz wątpliwości, czy dany sposób użycia wizerunku będzie oznaczał rozpowszechnianie, lepiej załóż, że tak jest, i poproś o zgodę osoby, której wizerunek utrwalasz. Jeśli jej nie otrzymasz — nie powinieneś/-aś go opublikować. Zgoda na rozpowszechnianie wizerunku nie musi przybierać formy pisemnej: wystarczy upewnić się, że dana osoba nie ma nic przeciwko temu.

Warto pamiętać, że zgoda dotyczy rozpowszechniania wizerunku przez konkretną osobę — czyli jeśli ktoś zgodzi się, żeby koleżanka rozpowszechniła jego/jej wizerunek, nie daje to prawa innej osobie do skopiowania go i dalszego wykorzystywania. Jeśli natkniesz się w sieci na zdjęcie, przy którym nie podano wyraźnie informacji, że materiał można rozpowszechniać, możesz z dużym prawdopodobieństwem założyć, że rozpowszechnianie go będzie wiązało się z naruszeniem ochrony wizerunku lub prawa autorskiego. To ogranicza możliwości wykorzystania dostępnych zasobów, ale ich nie zamyka.

Pomysł na lekcję

Uczestnicy i uczestniczki dowiedzą się, czym są dobra osobiste i wizerunek. Następnie zapoznają się z prawnymi i etycznymi aspektami rozpowszechniania wizerunku oraz zastanowią się, jak postępować w codziennych sytuacjach związanych z utrwalaniem wizerunku.

Cele operacyjne

Uczestnicy i uczestniczki:

- wiedzą, czym są dobra osobiste i wizerunek;
- potrafią rozpowszechniać wizerunek zgodnie z zasadami prawa;
- są bardziej wrażliwi na sytuacje, w których utrwalanie i publikacja wizerunku może naruszyć czyjeś dobra osobiste.

Przebieg zajęć

Ćwiczenie 1.

Czas: *20 min*

Metoda: *Praca w parach i miniwykład*

Pomoce: *Kartki formatu A4, ołówki/kredki/mazaki (w liczbie odpowiadającej liczbie uczestników), taśma malarska/magnesy/patafix*

Poproś uczestników, aby usiedli w dwóch rzędach naprzeciwko siebie. Rozdaj każdemu kartkę i kredkę/ołówek/mazak. Powiedz, że osoby siedzące po prawej stronie za chwilę zamienią się w modelki i modeli. Osoby siedzące po lewej stronie poproś o narysowanie portretów osób siedzących naprzeciwko oraz podpisanie ich imieniem i nazwiskiem pozujących. Daj na to kilka minut, a następnie poproś o zmianę ról (modelki/modele zmieniają się w artystów/artystki i rysują portrety kolegów i koleżanek).

Przy pomocy taśmy malarskiej, magnesów lub patafiksu przymocuj powstałe portrety do ściany lub tablicy, tak żeby były widoczne dla wszystkich uczestników lekcji (zapytaj wcześniej uczestników, czy nie mają nic przeciwko — jeżeli ktoś nie wyrazi zgody, nie wieszaj jego portretu).

Po wykonaniu zadania zapytaj uczestników:

- Jak czuliście się, pozując do portretu? A jak jako osoby malujące portrety? Czy to było dla was komfortowe, że ktoś tworzy wasz portret?
- Czy możecie rozpoznać siebie w narysowanych przez kolegów i koleżanki wizerunkach?
- Jak czujecie się z tym, że wszyscy uczestnicy lekcji mogą patrzeć na wasz wizerunek?
- Jak czulibyście się, gdyby zamiast portretów wisiały wasze prywatne zdjęcia? Czy mielibyście coś przeciwko, żeby wszyscy na nie patrzyli?

- A jak czulibyście się, gdyby te portrety zostały zamieszczone w Internecie, w którym nie wiecie, kto je ogląda?
- Czy przypominacie sobie zdjęcia, które zamieściliście w sieci, a po jakimś czasie uznaliście, że nie chcecie, żeby tam były? Czy żałowaliście, że je zamieściliście?

Zbierz i podsumuj wypowiedzi uczestników. Następnie zapisz na tablicy hasło „wizerunek" i zaproponuj jego definicję („cechy twarzy lub całej postaci, które pozwalają rozpoznać osobę", więcej na ten temat znajdziesz w „Wiedzy w pigułce"). Na koniec zapytaj, czy powstałe portrety według uczestników spełniają warunki bycia wizerunkiem.

Powiedz, że wizerunek jest jednym z naszych dóbr osobistych. Zapytaj uczestników, z czym kojarzy im się hasło „dobra osobiste". Zbierz ich skojarzenia. Powiedz, że dobra osobiste przysługują każdemu człowiekowi i że wartości te są chronione przez polskie prawo. Na podstawie „Wiedzy w pigułce" dopowiedz, jakie inne — oprócz wizerunku — dobra osobiste możemy wyróżnić (np. dobre imię, wolność, tajemnica korespondencji, nietykalność mieszkania).

Ćwiczenie 2.

Czas: *5 min*

Metoda: *Miniwykład*

Pomoce: *Karta pracy „Wizerunek", kreda i tablica lub marker i flipchart*

Powiedz, że wizerunkiem może być nie tylko obraz twarzy jakiejś osoby, ale też inne cechy, dzięki którym można ją rozpoznać, np. charakterystyczna blizna, sylwetka itp. Powiedz, że prawo do ochrony wizerunku przysługuje tylko żyjącym osobom. Żeby ktoś wykorzystał nasz wizerunek, potrzebuje do tego naszej zgody. Powiedz, że zgoda nie musi być wyrażona na piśmie, ale nie może także być domyślna. Opowiedz też o wyjątkach od tej zasady ochrony wizerunku (informacje z „Wiedzy w pigułce").

Następnie pokaż uczestnikom zamieszczone w karcie pracy „Wizerunek" obrazy (możesz pokazać je na projektorze, korzystając z załączonych linków, lub wydrukować) i poproś o rozpoznanie:

- czy obraz jest wizerunkiem, czy podlega ochronie.

Rozmawiając o pokazywanych obrazach, zwróć uwagę na to, że nie wszystkie wizerunki podlegają ochronie (zwróć uwagę na wizerunki osób fikcyjnych oraz zmarłych).

Ćwiczenie 3.

Czas: *5 min*

Metoda: *Miniwykład*

Pomoce: *Kreda i tablica*

Zapytaj uczestników, czy spotkali się z terminem „rozpowszechnianie wizerunku". Powiedz, że rozpowszechnianiem jest sytuacja, w której zostaje stworzona możliwość zapoznania się z wizerunkiem bliżej nieokreślonemu, otwartemu kręgowi osób, i że jeśli ktoś chciałby rozpowszechnić ich wizerunek, potrzebuje na to zgody. Powiedz, że aktualna sytuacja, kiedy portrety uczestników wiszą w klasie, nie jest sytuacją rozpowszechniania, bo mamy tu zamknięty krąg osób, ale gdyby ktoś z nich zrobił portretowi zdjęcie i wrzucił je na swojego bloga, byłoby to rozpowszechnianie. Możesz też przywołać inne hipotetyczne sytuacje, w których wywieszenie portretów w klasie byłoby ich rozpowszechnianiem (np. portrety wiszą przez cały tydzień, do pomieszczenia wchodzą różne klasy, rodzice uczniów i inne osoby).

Ćwiczenie 4.

Czas: *15 min*

Metoda: *Dyskusja*

Pomoce: *Sznurek/taśma malarska/kreda, karta pracy „TAK/NIE", karta pracy „Rozpowszechnianie wizerunku"*

Zrób przez środek sali linię. Możesz użyć do tego sznurka, taśmy malarskiej lub kredy. Na tej linii rozłóż kartki (z karty pracy „TAK/NIE") w kolejności TAK; TAK, ALE...; NIE WIEM; NIE, ALE...; NIE. Powiedz uczestnikom, że za chwilę będziesz czytać opisy różnych sytuacji. Poproś, żeby ustosunkowali się do tych opisów i zajęli miejsce na linii zgodnie z tym, co myślą.

Następnie przeczytaj uczestnikom opisy znajdujące się w załączniku „Rozpowszechnianie wizerunku". Jeżeli masz czas, po każdym twierdzeniu możesz przeprowadzić krótką dyskusję na temat prawnych i etycznych aspektów rozpowszechniania wizerunku. Proponowane pytania:

- Co robić w sytuacji, kiedy nie jesteśmy pewni, czy jakaś sytuacja jest rozpowszechnianiem wizerunku?
- Czy możliwa jest sytuacja, że zdjęcie wrzucone np. do zamkniętej grupy na Facebooku trafi do szerszego kręgu odbiorców? Jakie mogą być tego konsekwencje?

Na koniec podkreśl, że zamieszczając coś w Internecie, nigdy nie jesteśmy pewni, do jak szerokiego kręgu odbiorców trafi dana treść. Powiedz, że niezależnie od sytuacji, zawsze kiedy wrzucamy do sieci zdjęcie, warto przestrzegać dwóch zasad:

- zastanowić się, czy jesteśmy gotowi przyjąć konsekwencje tego, że wizerunek może trafić do szerszego kręgu odbiorców, niż początkowo sądziliśmy (w przypadku własnego wizerunku);
- pytać o zgodę osoby, które występują na zamieszczanych przez nas zdjęciach i filmach.

Ewaluacja

Czy po przeprowadzeniu zajęć uczestnicy i uczestniczki:

- wiedzą, czym są dobra osobiste i wizerunek?
- rozumieją, na jakich zasadach można rozpowszechniać wizerunek innych osób?
- potrafią rozpoznać sytuacje, w których mogliby zranić innych lub naruszyć ich prawa, publikując ich wizerunek w sieci?

Opcje dodatkowe

Przed zajęciami możesz poprosić uczestników, żeby przynieśli swoje prywatne zdjęcia (możecie je także wspólnie wydrukować w szkole). Zamiast rysować portrety możecie rozwiesić te zdjęcia w klasie. To opcja dla grup, które są mniej chętne do prac plastycznych.

Materiały

- Karta pracy „Wizerunek"
- Karta pracy „Wizerunek" — wersja dla prowadzącego z odpowiedziami
- Karta pracy „TAK/NIE"
- Karta pracy „Rozpowszechnianie wizerunku"

Zadania sprawdzające

Zadanie 1

Prawda czy fałsz (P/F)?

1. _ Wszystkie zdjęcia polityków można rozpowszechniać.
2. _ Wizerunek to jedno z dóbr osobistych.
3. _ Ochrona wizerunku przysługuje także osobom zmarłym.
4. _ Mam prawo wrzucić do sieci zdjęcie, na którym w tle znajdują się przypadkowi przechodnie bez pytania ich o zgodę.
5. _ W świecie nowoczesnych technologii trudno wskazać jasną granicę między utrwalaniem a rozpowszechnianiem wizerunku.

Słowniczek

Dane osobowe – wszelkie informacje dotyczące określonej osoby fizycznej (czyli zidentyfikowanej lub możliwej do zidentyfikowania). Nie mamy do czynienia z danymi osobowymi wówczas, gdy informacja dotyczy instytucji (np. firmy), grupy osób, osoby fikcyjnej (np. postaci literackiej) czy takiej, której nie jesteśmy w stanie rozpoznać. Dane osobowe podlegają ochronie i nie mogą być zbierane bez odpowiedniej podstawy prawnej (np. zgody osoby, której dotyczą).

Dobra osobiste – przysługujące każdemu człowiekowi dobra o charakterze niemajątkowym, chronione prawem cywilnym. Należą do nich m.in. zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, prawo do prywatności, poczucie przynależności do płci.

Mem internetowy – popularna internetowa forma komentowania rzeczywistości, zazwyczaj przybierająca formę graficzną (rysunek, zdjęcie) z nałożonym krótkim tekstem. Memy charakteryzują się dużym potencjałem wiralnym — powielane i komentowane przez użytkowników sieci mogą dotrzeć do szerokich rzesz odbiorców.

Ochrona wizerunku – wizerunek każdej osoby (czyli jej podobizna utrwalona na przykład na zdjęciu bądź filmie) podlega ochronie. Oznacza to, że nie może on być rozpowszechniany bez zgody danej osoby. Są jednak wyjątki. Rozpowszechnianie wizerunku bez zgody jest możliwe na przykład w przypadku: (1) osób powszechnie znanych, jeżeli wizerunek wykonano w związku z pełnieniem przez nie funkcji publicznych, (2) osób stanowiących jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza, (3) osób, które otrzymały zapłatę za pozowanie, chyba że wyraźnie zastrzegły inaczej, (4) osób ściganych listem gończym.

Przetwarzanie danych osobowych – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak np. zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, zwłaszcza gdy odbywa się w systemach informatycznych.

Rozpowszechnianie wizerunku – umożliwienie zapoznania się z wizerunkiem bliżej nieokreślonemu, niezamkniętemu kręgowi osób, np. publikacja w prasie, na blogu, w otwartej grupie na portalu społecznościowym, wywieszenie na ogólnodostępnej tablicy.

Wizerunek – utrwalona podobizna człowieka przedstawiająca cechy wyglądu, które pozwalają na jego identyfikację. Na wizerunek składają się zarówno cechy naturalne, m.in. rysy twarzy, postaci czy budowa

ciała, jak i dodane, np. fryzura, makijaż, ubranie, okulary (o ile są charakterystyczne dla danej osoby). Wizerunek podlega ochronie prawnej.

Czytelnia

1. *Fotografie a prawa osób fotografowanych*, IP blog o prawie własności intelektualnej i nowych technologii [dostęp: 12.08.2015] http://www.ipblog.pl/2014/06/fotografie-a-prawa-osob-fotografowanych/.

Ten materiał jest częścią projektu „Cyfrowa wyprawka" Fundacji Panoptykon.

Projekt współfinansowany ze środków Ministra Kultury i Dziedzictwa Narodowego.