Europejski Fundusz Rolny na rzecz Rozwoju Obszarów Wiejskich: Europa inwestująca w obszary wiejskie.

Modelowy System Administrowania Danymi Osobowymi w Lokalnych Grupach Działania

mgr inż. Anna Predko-Maliszewska
mgr Konrad Wnorowski

1. WSTĘP

Celem niniejszego opracowania jest omówienie podstawowych zagadnień związanych z przetwarzaniem danych osobowych przez Lokalne Grupy Działania. Opracowanie zawiera definicje, wymagania, uwarunkowania prawne, potencjalne zagrożenia dotyczące przetwarzania danych osobowych. Stan prawny na dzień 21 września 2016 r.

2. ŹRÓDŁA PRAWA REGULUJĄCE OCHRONĘ DANYCH OSOBOWYCH

Problematyka ochrony danych osobowych na płaszczyźnie prawa międzynarodowego została dostrzeżona w drugiej połowie XX wieku. Przesłankami do tego były: rosnący rozwój gospodarczy i konieczność przepływu danych pomiędzy współpracującymi ze sobą krajami, w tym także poprzez sieci komputerowe. Nie było jednak aktu prawnego, który kompleksowo regulowałby powyższą materię. Natomiast w aktach prawnych wydawanych pod auspicjami Organizacji Narodów Zjednoczonych pojawiają się pewne fragmentaryczne regulacje związane z tą problematyką, jednakże dotyczą one raczej ochrony prywatności, niż ochrony danych *sensu stricto*.

Do najważniejszych aktów prawnych regulujących ochronę danych osobowych lub odnoszących się do owej materii należy zaliczyć:

2.1. Akty międzynarodowe

POWSZECHNA DEKLARACJA (UNESCO) W SPRAWIE GENOMU LUDZKIEGO I PRAW CZŁOWIEKA Z DNIA 11 LISTOPADA 1997 R.

Powszechna Deklaracja (UNESCO) w sprawie genomu ludzkiego i praw człowieka z dnia 11 listopada 1997 r. jest dokumentem o charakterze uniwersalnym. Zgodnie z jego założeniami danym genetycznym - dającej się zidentyfikować osoby - należy zapewnić poufność (art. 7). Jak wynika z treści tego aktu, taką ochroną objęte są dane genetyczne bez względu na cel w jakim są one gromadzone. Przykładowo wskazano, iż takie dane mogą być gromadzone w celach badawczych. Ograniczenie powyższej zasady poufności może nastąpić wyłącznie w granicach przewidzianych przepisami prawa.

REZOLUCJA 45/95 ZGROMADZENIA OGÓLNEGO ONZ Z 26 CZERWCA 1985 R.

26 czerwca 1985 r. pod patronatem Komisji Praw Człowieka ONZ przygotowany został projekt wytycznych dotyczący regulacji odnoszących się do elektronicznych banków danych zawierających m.in. dane osobowe. Dokument ten przyjęty w 1988 r., ogłoszony został 14 grudnia 1990 r., jako rezolucja zawierająca wytyczne w sprawie uregulowania kartotek skomputeryzowanych danych osobowych. Powyższe wytyczne nie mają charakteru wiążącego.

Stanowią jedynie zalecenia odnośnie gwarancji, jakie powinny być zapewnione w przepisach krajowych w zakresie komputerowego przetwarzania danych osobowych. Rezolucja opiera się na kilku podstawowych zasadach (zgodności z prawem i słuszności, poprawności, celowości, dostępu osoby zainteresowanej, niedyskryminacji oraz bezpieczeństwa), które winny być uwzględnione w prawie krajowym.

REKOMENDACJA ORGANIZACJI WSPÓŁPRACY GOSPODARCZEJ I ROZWOJU (OECD) Z DNIA 23 WRZEŚNIA 1980 R., W SPRAWIE WYTYCZNYCH DOTYCZĄCYCH OCHRONY PRYWATNOŚCI I PRZEKAZYWANIA DANYCH OSOBOWYCH POMIĘDZY KRAJAMI

Rekomendacja Organizacji Współpracy Gospodarczej i Rozwoju (OECD) z dnia 23 września 1980 r., w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami, nie jest dokumentem o wiążącym charakterze. Są to jedynie zalecenia Rady OECD odnośnie zawartych w ustawodawstwie krajowym regulacji dotyczących ochrony prywatności i przepływu danych osobowych przez granice. W powyższych wytycznych podkreślono wagę i wpływ międzynarodowego transferu danych na światowy rozwój gospodarczy i ujemny wpływ ograniczeń w tym zakresie. Rekomendacja w swych zaleceniach dopuszcza wprawdzie wprowadzenie takich ograniczeń w przepisach krajowych, jednakże zaleca ich eliminowanie.

REZOLUCJA 34/169 ZGROMADZENIA OGÓLNEGO ONZ

Rezolucja 34/169 z 1979 r. "Kodeks Postępowania Funkcjonariuszy Porządku Prawnego" porusza (w wąskim zakresie) w art. IV zagadnienia dotyczące problematyki ochrony danych osobowych. Stanowi jedynie zalecenie dla funkcjonariuszy, którzy z racji pełnionych funkcji pozyskują dane innych osób, dotyczące postępowania z tymi danymi. Mogą być one udostępniane wyłącznie w celu wypełniania obowiązków służbowych, a także dla potrzeb wymiaru sprawiedliwości.

2.2. Akty europejskie

a) Prawo Unii Europejskiej

Karta Praw Podstawowych Unii Europejskiej

Karta Praw Podstawowych Unii Europejskiej, której projekt uzgodniony został w październiku 2000 r, to dokument przyjęty i uroczyście ogłoszony na szczycie Unii Europejskiej w Nicei, w grudniu 2000 r. Karta określa katalog podstawowych praw i wolności obywatela Unii Europejskiej. Katalog ten, poza wartościami uznawanymi powszechnie przez różne akty prawa międzynarodowego (m.in. prawo do godności osoby ludzkiej, prawo do życia, zakaz tortur

i nieludzkiego traktowania, prawo do wolności, rzetelnego procesu), zawiera też prawo do ochrony danych osobowych (zagwarantowane w artykule 8). Karta stała się podstawą do dalszych dyskusji na temat praw i wolności obywatela Unii. Wskazane w niej wartości zainicjowały dyskusję nad ewentualną Konstytucją Unii.

Dyrektywy kierowane są wyłącznie do państw członkowskich. Nie wynikają z nich żadne prawa ani obowiązki dla osób prawnych i fizycznych. Państwo jest zobowiązane, w swoim prawie wewnętrznym, zrealizować wymagania dyrektywy przy czym z reguły obojętna jest forma ich realizacji. Dyrektywa nie należy więc do *self-executing law*. Może ona być stosowana bezpośrednio jedynie w wypadku, gdy upłynął termin jej realizacji, a państwo nie dokonało jej implementacji lub dokonana implementacja jest wadliwa. Należy wyróżnić następujące dyrektywy:

- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW
- Dyrektywa 2009/136/WE Parlamentu Europejskiego i Rady WE
- Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady WE
- Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady WE
- Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej (Dyrektywa o ochronie prywatności i komunikacji elektronicznej).
- Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady WE.

Warto także nadmienić, iż w Dzienniku Urzędowym został opublikowany oficjalny tekst decyzji ramowej 2008/977/WSiSW w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych przyjęty przez Radę Unii Europejskiej.

Konwencje:

- KONWENCJA sporządzona na podstawie artykułu K.3 Traktatu o Unii Europejskiej w sprawie wykorzystania technologii informatycznej dla potrzeb celnych

- KONWENCJA sporządzona na podstawie art. K.3 Traktatu o Unii Europejskiej, w sprawie ustanowienia Europejskiego Urzędu Policji (konwencja o Europolu).

b) Dokumenty Rady Europy

W standardach Rady Europy fundamentalną pozycję w dziedzinie ochrony danych osobowych zajmuje Konwencja Rady Europy Nr 108 z dnia 28 stycznia 1981 r. o Ochronie Osób w Związku z Automatycznym Przetwarzaniem Danych Osobowych. Wśród standardów traktatowych uwzględnić należy również postanowienia Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (Europejskiej Konwencji Praw Człowieka) z 4 listopada 1950 r. wraz z najnowszym orzecznictwem strasburskim w zakresie przekazywania danych medycznych. Istotne są także postanowienia Europejskiej Konwencji Bioetycznej z 4 kwietnia 1997 r. w obszarze odnoszącym się do ochrony danych osobowych, wraz z odpowiednimi fragmentami Sprawozdania Wyjaśniającego do niej.

W dniu 19 stycznia 1993 r. Polska ratyfikowała Europejską Konwencję Praw Człowieka, a z dniem 1 maja 1993 r. uznała kompetencje Europejskiej Komisji i Europejskiego Trybunału Praw Człowieka w zakresie rozpatrywania skarg indywidualnych.

W dniu 21 kwietnia 1999 r. Polska podpisała Konwencję Nr 108 RE. Konwencja została ratyfikowana przez Polskę 24 maja 2002 r.

- *Konwencja Rady Europy Nr 108 z dnia 28 stycznia 1981 roku*
- *Protokół dodatkowy do Konwencji Rady Europy Nr 108 o Ochronie Osób w związku z automatycznym przetwarzaniem danych osobowych*
- *Europejska Konwencja Bioetyczna z dnia 4 kwietnia 1997 r. w obszarze odnoszącym się do ochrony danych osobowych, wraz z odpowiednimi fragmentami Sprawozdania Wyjaśniającego do niej. (tekst angielski)*
- *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności*

Zalecane standardy europejskie w zakresie ochrony danych osobowych, sformułowane w trybie rezolucji i rekomendacji Komitetu Ministrów RE lub Zgromadzenia Parlamentarnego RE, odnoszą się do różnych dziedzin życia. Akty te rozwijają ogólne zapisy Konwencji 108, precyzują jej wymagania oraz wprowadzają dodatkowe warunki przetwarzania danych osobowych w określonych dziedzinach (marketing bezpośredni, policja, zatrudnienie, terminy płatności, telekomunikacja ze szczególnym uwzględnieniem usług telefonicznych itd.).

- Rekomendacja R (2002) 9 z dnia 18 września 2002 r. w sprawie ochrony danych osobowych zbieranych i przetwarzanych dla celów ubezpieczeniowych

- Rekomendacja z dnia 23 listopada 2010 r. w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili
- Rezolucja (73) 22 z dnia 26 września 1973 r. o ochronie życia prywatnego osób fizycznych w kontekście elektronicznych banków danych w sektorze prywatnym.
- Rekomendacja R (91) 10 I Nota wyjaśniająca Komitetu Ministrów dla Państw Członkowskich w sprawie udostępniania osobom trzecim danych osobowych będących w posiadaniu instytucji publicznych
- Rekomendacja R (87) 15 Komitetu Ministrów Rady Europy o Ochronie Danych Osobowych wykorzystywanych w sektorze policji z 17 września 1987 roku
- Rekomendacja R (85)20 Komitetu Ministrów dla Państw Członkowskich w sprawie ochrony danych osobowych używanych dla celów marketingu bezpośredniego, Rady Europy "Ochrona Danych Osobowych Wykorzystywanych dla potrzeb marketingu bezpośredniego" z 25 października 1985 roku
- Rekomendacja Nr R (83) 10 Komitetu Ministrów dla Państw Członkowskich w sprwie ochrony danych osobowych gromadzonych i przetwarzanych dla celów badań naukowych i statystycznych
- Rekomendacja R (81) 1 Komitetu Ministra dla Państw Członkowskich w sprawie regulacji mających zastosowanie do zautomatyzowanych banków danych medycznych
- Rekomendacja R (2002) 9 Komitetu Ministrów dla Państw Członkowskich w sprawie ochrony danych osobowych gromadzonych i przetwarzanych dla celów ubezpieczeniowych
- Rekomendacja R (1999) 5 Komitetu Ministrów dla Państw Członkowskich w sprawie ochrony prywatności w internecie, wytyczne w sprawie ochrony osób w zakresie gromadzenia i przetwarzania danych osobowych na "infostradach"
- Rekomendacja R (97) 18 Komitetu Ministrów dla Państw Członkowskich w sprawie ochrony danych osobowych gromadzonych i przetwarzanych dla celów statystycznych
- Rekomendacja R (1986) 1 Komitetu Ministrów dla Państw Członkowskich w sprawie ochrony prywatności w internecie, wytyczne w sprawie ochrony danych osobowych używanych dla celów zabezpieczeń społecznych
- Rekomendacja R (97) 5 Komitetu Ministrów do Państw Członkowskich dotycząca ochrony danych osobowych
- Rezolucja (74) 29
- Rekomendacja R(81) 1
- Rekomendacja R(99) 5

- Rekomendacja R(97) 18 z dnia 30 września 1997 r. dotycząca ochrony danych osobowych gromadzonych i przetwarzanych dla celów statystycznych.
- Rekomendacja R(97) 5
- Rekomendacja R(95) 4 z dnia 7 lutego 1995 r. dotycząca ochrony danych osobowych w telekomunikacji ze szczególnym uwzględnieniem usług telefonicznych.
- Rekomendacja R(91) 10 z dnia 9 września 1991 r. dotycząca ochrony danych osobowych przekazywanych osobom trzecim przez instytucje publiczne.
- Rekomendacja R(90) 19 z dnia 13 września 1990 r. dotycząca ochrony danych osobowych wykorzystywanych dla potrzeb płatności oraz innych analogicznych operacji.
- Rekomendacja R(87) 15 z dnia 17 września 1987 r. dotycząca ochrony danych osobowych wykorzystywanych w sektorze policji.
- Rekomendacja R(86) 1 z dnia 23 stycznia 1986 r. dotycząca ochrony danych osobowych dla potrzeb ubezpieczenia społecznego.
- Rekomendacja R(85) 20 z dnia 25 października 1985 r. dotycząca ochrony danych osobowych wykorzystywanych dla potrzeb marketingu bezpośredniego.
- Rekomendacja R(83) 10 z dnia 23 września 1983 r. dotycząca ochrony danych osobowych wykorzystywanych w badaniach naukowych i statystyce.
- Nowa rekomendacja Rady Europy w sprawie ochrony danych osobowych w sektorze zatrudnienia

2.3. Prawo w Polsce

- Konstytucja Rzeczypospolitej Polskiej
- Ustawa o ochronie danych osobowych

Akty wykonawcze:

- Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 19 listopada 2015 r. zmieniające rozporządzenie w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. 2015, poz 2020).
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015, poz. 745)

- Rozporządzenie Ministra Administracji i Cyfryzacji z 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2015, poz. 719)
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. 2014, poz. 1934)
- Rozporządzenie ministra spraw wewnętrznych i administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2004 r. Nr 94, poz. 923) i Rozporządzenie ministra spraw wewnętrznych i administracji z dnia 11 maja 2011 r. zmieniające rozporządzenie w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2011 r. Nr 103, poz. 601)
- 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. z 2004 r. Nr 100, poz. 1024)
- Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2011, Nr 225, poz. 1350)
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 r., Nr 229, poz. 1536)

Przepisy proceduralne:

- Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. tekst jednolity z 2000 r., Nr 98, poz. 1071, ze zm.)
  Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. 2005 r. Nr 229 poz. 1954)[1].

[1] http://www.giodo.gov.pl/, dostęp na dzień 15.09.2016 r.

Wskazane powyżej akty normatywne oraz inne akty odnoszące się do tematyki ochrony danych osobowych wskazują na dynamiczny rozwój prawodawstwa dotyczącego owej materii, co wymuszane jest przez praktykę.

3. PODSTAWOWE DEFINICJE W OCHRONIE DANYCH OSOBOWYCH

Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Jest to zestaw informacji pozwalający daną osobę odróżnić od innych osób. Do takich informacji zaliczyć można numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Dane wrażliwe – są to dane ujawniające 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.

Przetwarzanie danych osobowych – operacje dokonywane na danych osobowych takie jak np. gromadzenie, rejestracja, porządkowanie, **przechowywanie**, modyfikacja, odzyskiwanie, konsultowanie, archiwizowanie, wykorzystywanie, ujawnianie poprzez transmisję, publikowanie, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie.

Zbiór danych – uporządkowany zestaw danych osobowych posiadający określoną strukturę, umożliwiający przeglądanie lub wyszukiwanie według określonych kryteriów (np. data urodzenia, nazwisko).

Administrator Danych Osobowych (ADO) – instytucja (podmiot) decydująca o celach i środkach przetwarzania danych osobowych. Odpowiedzialny za przetwarzanie danych osobowych, organizację środków niezbędnych do zgodnego z prawem przetwarzania danych i za kontrolę nad przetwarzaniem. Do obowiązków ADO m.in. należy przygotowanie i opracowanie polityki bezpieczeństwa danych osobowych, nadawanie upoważnień do przetwarzania danych osobowych, prowadzenie ewidencji osób upoważnionych.

Administrator Bezpieczeństwa Informacji (ABI) – osoba powołana przez ADO, odpowiedzialna za nadzorowanie stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych. Powołanie ABI jest dobrowolne. ABI przejmuje zakres obowiązków ADO, natomiast nie jest przenoszona na ABI odpowiedzialność.

ASI – Administrator Systemu Informatycznego, jest to osoba lub podmiot sprawująca zadania związane z administracją systemami informatycznymi, bazami danych lub aplikacjami administratora danych osobowych.

Rozporządzenie MSWiA - 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.

Poufność danych - zapewnienie, że dane nie są udostępniane nieautoryzowanym osobom lub podmiotom.

Integralność danych - zapewnienie, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

Rozliczalność danych - zapewnienie, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie.

Użytkownik – osoba uprawniona (posiadająca upoważnienie) do przetwarzania danych osobowych w systemie informatycznym.

Login (identyfikator użytkownika) – ciąg znaków identyfikujących jednoznacznie danego użytkownika.

Zgoda osoby, której dane są przetwarzane – rozumie się przez nią oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tej osoby, która składa oświadczenie. Zgoda będzie stosowana wszędzie tam, gdzie w przepisie prawa nie ma zezwolenia na przetwarzanie danych osobowych. Zgoda nie może być domniemana lub dorozumiana z innego oświadczenia woli, np. z faktu zaakceptowania regulaminu sklepu internetowego.

Odbiorca danych - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

- osoby, której dane dotyczą,
- osoby upoważnionej do przetwarzania danych,
- przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych (przedstawiciel wyznaczany jest przez podmioty mające siedzibę albo miejsce zamieszkania w państwie trzecim),
- podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych (podmiot, któremu powierzono przetwarzanie danych osobowych),

- organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

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

GIODO – Generalny Inspektor Ochrony Danych Osobowych.

4. DANE OSOBOWE – OD OGÓŁU DO SZCZEGÓŁU

4.1. Jak rozpoznać dane osobowe?

W praktyce bardzo często można spotkać się z sytuacjami, w których dany podmiot może mieć wątpliwości czy przetwarzane przez niego dane są „osobowe" czy też nie. Definicja ustawowa wydaje się być nieprecyzyjna i niewystarczająca do ustalania owej kwestii. GIODO jednak zauważa, iż „przy rozstrzyganiu, czy określona informacja lub informacje stanowią dane osobowe, w większości przypadków, nieuniknione jest dokonanie zindywidualizowanej oceny, przy uwzględnianiu konkretnych okoliczności oraz rodzaju środków czy metod potrzebnych w określonej sytuacji do identyfikacji osoby"[2]. W życiu codziennym może się wydawać, iż to intuicja podpowiada co jest danymi osobowymi, a co nimi nie jest. Przykładem na to może być powszechne uznanie, iż imię, nazwisko i adres stanowią dane osobowe, dzięki którym możliwa jest identyfikacja danej osoby. Może to wynikać z faktu, iż tego typu dane znajdują się na dokumentach etc. Jednak takie intuicyjne ustalanie co należy do kategorii danych osobowych może być głęboko mylące, gdyż ustawa o ochronie danych osobowych stanowi, iż 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, które określają jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. W związku z powyższym ustalenie danej osoby po konkretnej cesze lub cechach jest wyłącznie kwestią koniecznej ilości nakładu pracy. Ustawodawca ustanowił, iż informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. Kryterium nadmierności wydaje się bardzo nieprecyzyjne, gdyż, np. posiadając numer PESEL danej osoby można uzyskać o niej informacje ze zbioru prowadzonego przez MSWiA, gdzie wystarczy wypełnić wniosek, uzasadnić potrzebę posiadania owych danych i wnieść stosowną opłatę. Powstaje pytanie: czy kryterium „nadmierności" w tym momencie

[2] http://www.giodo.gov.pl/317/id_art/973/j/pl.

zostało wyczerpane? Jest to kolejny przykład konieczności indywidualnej oceny kryterium „nadmierności".

4.2. Wybrane rodzaje danych

Można stwierdzić, iż dowolny zestaw informacji o konkretnej osobie może stanowić o tym, że mamy styczność z danymi osobowymi, a uzależnione to jest od tego czy na tej podstawie ich posiadacz będzie mógł ustalić tożsamość osoby i w jakim czasie może tego dokonać. Poniżej zostaną omówione podstawowe przykłady danych osobowych z jakimi mogą stykać się Lokalne Grupy Działania.

Imię i nazwisko

Jak powszechnie wiadomo w społecznościach imiona i nazwiska często się powtarzają, co może utrudniać zidentyfikowanie tożsamości konkretnej osoby. W związku z tym należy uznać za trafny pogląd, iż samo imię i nazwisko nie stanowi danych osobowych, gdyż tworzą one jedynie katalog pewnej ilości osób o danym imieniu i nazwisku, ale nie pozwalają na zidentyfikowanie danej osoby. Imiona i nazwiska unikatowe (nie powtarzające się często) także nie stanowią danych osobowych pomimo tego, iż ułatwiają identyfikację, gdyż to pracownicy LGD musieliby sami ustalać o posiadaniu przez nie owej cechy. Samo imię i nazwisko w połączeniu z inną informacją o konkretnej osobie może stać się danymi osobowymi, np.:

- Jan Nowak – prezes LGD Rybaki,

- Anna Predko – Maliszewska z Wasilkowa,

- Konrad Wnorowski – doktorant prawa międzynarodowego,

- Małgorzata Kowalska – adwokat.

Warto zauważyć, iż samo imię i pierwsza litera nazwiska nie będą stanowiły danych osobowych, ale w połączeniu z inną informacją mogą umożliwić identyfikację danej osoby. Dodatkowo należy pamiętać, że pewne nazwiska w polskiej pisowni wskazują na płeć danej osoby.

Adres i kod pocztowy

Sam adres nie zalicza się do kategorii danych osobowych, gdyż określa on wyłącznie dane miejsce. Jednak adres w połączeniu z inną informacją może umożliwić identyfikację tożsamości danej osoby, np. imię i nazwisko wraz z adresem zalicza się do danych osobowych. W piśmiennictwie można dostrzec pogląd, iż adres w połączeniu z samym imieniem będzie stanowił

dane osobowe, ponieważ umożliwi to kontakt z konkretną osobą[3]. Warto pamiętać, iż sam adres zestawiony z inną informacją, która może wydawać się nieistotna, umożliwią identyfikację konkretnej osoby. Przykładem jest wywieszanie przez spółdzielnię mieszkaniową informacji o zaległości z czynszem, która ciąży na danym lokalu[4]. Na podstawie odrębnych przepisów inny członek spółdzielni ma prawo wglądu w rejestr członków i może z łatwością poznać tożsamość właściciela zadłużonego mieszkania. W związku z tym spółdzielnia mieszkaniowa nie może uprawiać takich praktyk[5].

Numer dokumentu

GIODO w swojej opinii dotyczącej kart miejskich stwierdził, iż numery dokumentów nie będą stanowiły danych osobowych, gdyż „dla zwykłego obywatela, który miałby dostęp do karty miejskiej z samym tylko jej numerem ustalenie tożsamości jej właściciela wymaga jednak pewnego czasu i działań. Dlatego dla niego sam numer karty miejskiej nie będzie stanowił danej osobowej”[6]. Jednocześnie GIODO wskazał, iż: „jest daną osobową […], ale tylko dla tych osób, które na jego podstawie mogą ustalić tożsamość jej właściciela. Będą to np. pracownicy przewoźnika upoważnieni do przetwarzania informacji zawartych w systemie informatycznym związanym z funkcjonowaniem karty miejskiej”[7].

Na pierwszy rzut oka przytoczone cytaty GIODO mogą wydawać się jako sprzeczne, ale tak nie jest. Reasumując należy podkreślić, iż każdy numer dokumentu będzie daną osobową dla jego wystawcy, o ile prowadzi on ewidencję informacji komu dokumenty są wystawiane i na jaki czas. W stosunku do innych osób numery dokumentów takich jak np. dowód osobisty, prawo jazdy, paszport nie będą stanowiły danych osobowych.

Numer PESEL

PESEL jest numerem identyfikacyjnym osoby, który nie zmienia się od chwili nadania, a co istotne zakłada się, że nie ma takich samych dwóch numerów PESEL. Jego unikalność podkreśla ustawodawca w art. 31a ust. 1 ustawy o ewidencji ludności i dowodach osobistych: „Numer Powszechnego Elektronicznego Systemu Ewidencji Ludności, zwany w niniejszej ustawie „numerem PESEL”, jest to 11 – cyfrowy, stały symbol numeryczny, **jednoznacznie** identyfikujący

[3] L. Kępa, *Ochrona danych osobowych w praktyce*, Warszawa 2015, s. 47.
[4] http://www.giodo.gov.pl/353/id_art/994/j/pl.
[5] Ustawa z dnia 16 września 1982 r. prawo spółdzielcze, Dz. U. 2016 r. poz. 1250.

[6] http://www.giodo.gov.pl/319/id_art/3512/j/pl.
[7] *Ibidem*.

osobę fizyczną, w którym sześć pierwszych cyfr oznacza datę urodzenia (rok, miesiąc, dzień), kolejne cztery – liczbę porządkową i płeć osoby, a ostatnia jest cyfrą kontrolną służącą do komputerowej kontroli poprawności nadanego numeru ewidencyjnego”[8]. Upraszczając należy przyjąć, iż konkretne osoby w społeczeństwie są ponumerowane, a PESEL jest tylko i wyłącznie owym numerem. GIODO wyraźnie określił swoje stanowisko stwierdzając, iż: „sam numer PESEL stanowi dane osobowe w rozumieniu ustawy o ochronie danych osobowych”[9]. W związku z powyższym, pomimo odrębnych głosów doktryny[10], numer PESEL należy traktować jako dane osobowe, gdyż stanowisko GIODO wydaje się być rozstrzygające i w przypadku ewentualnej kontroli będzie ono przedstawiane przez urzędników GIODO.

Numer telefonu

Numer telefonu występując samodzielnie nie jest daną osobową, ale jest to kategoria informacji, która może prowadzić do naruszenia sfery prywatności danej osoby, dlatego należy go traktować jako przypadek „swoisty”, a ponadto niejako owa kwestia „wymyka” się spod regulacji prawnych. Ustawa o ochronie danych osobowych stanowi o konieczności identyfikacji, ale posiadanie wyłącznie numeru telefonu może, lecz nie musi, prowadzić do określenia tożsamości danej osoby. GIODO w owej kwestii zajął następujące stanowisko: „Wskazać należy, iż informacje w zakresie: kod respondenta, numer telefonu i imię respondenta stanowią dane osobowe w rozumieniu ustawy o ochronie danych osobowych. Wprawdzie ww. informacje rzeczywiście nie określają bezpośrednio tożsamości osoby, jednakże dają możliwość określenia tożsamości tych osób np. poprzez bezpośredni kontakt z respondentem. Z powyższego wynika więc jednoznacznie, że wskazane wyżej dane dotyczące respondentów stanowią informacje dotyczące możliwej do zidentyfikowania osoby fizycznej, a samo ustalenie tożsamości nie wymaga nadmiernych kosztów, czasu lub działań. Wobec tego, stosownie do treści cytowanego wyżej art. 6 ustawy, stanowią one dane osobowe”[11]. Oczywiście w ww. sprawie GIODO za dane osobowe uznał numer telefonu połączony z imieniem oraz kodem respondenta, co stanowi znacznie szersze informacje. Jednoznacznie należy stwierdzić, iż numer telefonu połączony z imieniem albo nazwiskiem należy uznać za daną osobową, gdyż jedno z nich dodatkowo określa informacje o konkretnej osobie, a przez co ułatwia identyfikację. Z drugiej strony dla operatora, który świadczy usługi telekomunikacyjne sam numer telefonu będzie stanowił dane osobowe, gdyż

[8] Ustawa z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych, Dz. U. z 2013 r. poz. 1650.
[9] http://www.giodo.gov.pl/317/id_art/2912/j/pl.
[10] Por. L. Kępa, *Ochrona danych…*,*op. cit*., s. 52-53.
[11] http://www.giodo.gov.pl/306/id_art/2329/j/pl.

posiada on w bazie klientów inne informacje, które w powiązaniu ze sobą pozwalają na identyfikację tożsamości osoby.

Adres e-mail

W pierwszej kolejności należy dokonać podziału adresów e-mail na: służbowe oraz prywatne. W przypadku służbowych należy przyjąć pogląd, iż będą one stanowiły dane osobowe, gdyż z samego adresu możemy uzyskać takie informacje jak: imię i/lub nazwisko, nazwa zakładu pracy, adres i telefon zakładu pracy (np. sprawdzając w Internecie).

Prywatnych adresów e-mail nie powinno się traktować jako danych osobowych, gdyż maksymalnie można uzyskać informacje o imieniu i nazwisku właściciela, które nie muszą być prawdziwe, gdyż na darmowych serwerach pocztowych nic nie stoi na przeszkodzie, aby założyć konto na fikcyjne dane. Warto jednak pamiętać, że adres e-mail w połączeniu z innymi informacjami mogą stanowić dane osobowe, co świadczy o konieczności zachowania stałej czujności przez ich posiadaczy.

W przypadku prowadzenia platformy, na której będą się rejestrować osoby i podawać swoje adresy elektronicznych skrzynek pocztowych, należy uznać, że zbierane będą dane osobowe, gdyż istnieje możliwość, że ktoś poda adres służbowy etc.

Numer IP

Ów numer pozwala na identyfikację urządzeń w sieci Internet. Na stronie internetowej GIODO w zakładce poświęconej najczęściej zadawanym pytaniom można przeczytać, iż „adres IP może być w pewnych przypadkach uznany za dane osobowe". Tego typu komentarz wydaje się zbyt ogólny i niejednoznaczny, dlatego warto sprawdzić kiedy adres IP można traktować jako dane osobowe.

Należy zgodzić się z poglądem Leszka Kępy, który twierdzi, iż dla przeciętnej osoby numer IP nie będzie daną osobową, gdyż za jego pomocą nie można jednoznacznie ustalić osoby ani komputera (np. gdy komputer łączy się z Internetem za pomocą routera, to wyświetlał się będzie numer routera, a nie komputera), gdyż pozwala to na identyfikację tzw. interfejsu sieciowego komputera, routera lub modemu GSM[12]. Ponadto istnieje możliwość schowania się za innym numerem IP lub podszycie się pod innym numer IP. Za podsumowanie tej kwestii można uznać stwierdzenie GIODO: „[…] należy uznać, że w przypadkach, gdy adres IP jest na stałe lub na

[12]L. Kępa, *Ochrona danych…*,*op. cit*., s. 61 – 62.

dłuższy okres czasu przypisany do konkretnego urządzenia, które przypisane jest z kolei konkretnemu użytkownikowi, należy uznać, że stanowi on daną osobową”[13].

Numer rachunku bankowego

Identyfikacji osoby poprzez numer rachunku bankowego w zasadzie może dokonać bank macierzysty posiadacza rachunku. Przeciętna osoba nie będzie w stanie tego dokonać, a więc sam numer rachunku bankowego nie stanowi danych osobowych. W sposób oczywisty należy podkreślić, iż numer rachunku bankowego przyjmie charakter danych osobowych dopiero po połączeniu z innymi informacjami, które pozwolą zidentyfikować daną osobę.

Wizerunek

W dobie rozwoju technologii bardzo częstą praktyką jest uwiecznianie różnego rodzaju przedsięwzięć kulturalnych, społecznych, naukowych etc. na zdjęciach lub filmach. Wizerunek konkretnej osoby można traktować z jednej strony jako dobro osobiste (art. 23 Kodeksu Cywilnego), a z drugiej strony jako specyficzny rodzaj danych biometrycznych, które podlegają ochronie. Wydaje się, że owe ujęcia są ze sobą na stałe skorelowane. Przetwarzając tego typu dane należy mieć w pierwszej kolejności na uwadze art. 81 ust. 1 i 2 ustawy o prawie autorskim i prawach pokrewnych, który stanowi: „Rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie. 2. Zezwolenia nie wymaga rozpowszechnianie wizerunku: 1) osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych; 2) osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza”[14].

Naruszeniem prawa do ochrony wizerunku jest bezprawne rozpowszechnianie wizerunku, **nie zaś samo jego sporządzenie.** „Rozpowszechnianie” należy rozumieć jako publiczne udostępnianie, stworzenie możliwości zapoznania się z wizerunkiem bliżej nieokreślonej grupie osób. Rozpowszechnianie wizerunku nie będzie wymagało zezwolenia osoby przedstawionej na zdjęciu w sytuacji, gdy wizerunek stanowi jedynie element „akcydentalny lub akcesoryjny” przedstawionej całości wydarzenia (np. konferencji naukowej czy koncertu plenerowego z okazji rocznicy ważnego wydarzenia historycznego). Chodzi tutaj o takie przypadki, gdy wizerunek

[13] http://www.giodo.gov.pl/319/id_art/2258/j/pl.
[14] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, Dz. U. z 2016 r. poz1333.

osoby sportretowanej na zdjęciu stanowi rzeczywiście jedynie przypadkowy element. Takie przedstawienie wizerunku nie będzie wymagało zezwolenia, „albowiem **usunięcie wizerunku tej osoby nie zmienia charakteru filmu** ani też sposobu przedstawienia jego problematyki”[15].

Z perspektywy funkcjonowania Lokalnych Grup Działania istotną kwestią może wydawać się publikowanie zdjęć pracowników, np. na stronach internetowych. Udostępnienie na rzecz pracodawcy zdjęcia przez pracownika nie jest wymagane przepisami prawa (w tym prawa pracy). W związku z tym GIODO w swojej opinii klarownie stwierdza, iż: „[…] zasadnym wydaje się być twierdzenie, że aby działanie pracodawcy polegające na wykorzystaniu zdjęcia (wizerunku) pracownika, w tym umieszczanie na stronie internetowej firmy, było legalne, wskazane jest pozyskanie na to jego zgody” jednocześnie zastrzegając istnienie wyjątków od owej reguły, np.: „Istnieją jednak sytuacje wyjątkowe, gdy wizerunek pracownika jest ściśle związany z wykonywanym przez niego zawodem czy charakterem pracy. Jako przykład podać można choćby pracowników ochrony, co do których – ze względów bezpieczeństwa – powinna być możliwość ich identyfikacji. Wówczas można odstąpić od pozyskiwania takiej zgody w tym właśnie celu”[16].

W związku z powyższym co do zasady pracodawca nie chcąc narazić się na zarzut bezpodstawnego przetwarzania danych osobowych powinien zwrócić się do pracownika o wyrażenie zgody na publikację jego wizerunku czy to na stronie internetowej, czy też na identyfikatorze.

5. OBOWIĄZKI ZWIĄZANE Z PRZETWARZANIEM DANYCH OSOBOWYCH

5.1. Dokumentacja ochrony danych osobowych

Administrator Danych Osobowych zobowiązany jest do opracowania dokumentacji ochrony danych osobowych. 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 określa zasady i zakres prowadzenia dokumentacji ochrony danych osobowych. Na tę dokumentację składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

[15] Wyrok SA w Warszawie z 10.02.2005 r., I ACa 509/04, LEX nr 535042.
[16] http://www.giodo.gov.pl/348/id_art/4859/j/pl/.

a. Polityka bezpieczeństwa danych osobowych

Polityka bezpieczeństwa jest dokumentem określającym zasady i standardy pracy przy przetwarzaniu danych osobowych wdrożone i stosowane w organizacji. Zgodnie z wymogami Rozporządzenia MSWIA zawierać musi:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe – element ten stanowi opis obszaru przetwarzania danych osobowych,

2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych – zawierać powinien wszystkie zbiory przetwarzane w organizacji, niezależnie od tego, czy dane zbiory podlegają rejestracji czy też nie.

3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi – jest to wykaz szczegółowy wykaz przetwarzanych danych. GIODO zaleca aby opis jednoznacznie wskazywał jakiego rodzaju dane są przetwarzane, łącznie z typem zastosowanych danych. Przygotowanie opisu struktury danych bywa niejednokrotnie bardzo trudne, szczególnie w przypadku przetwarzania danych w systemach informatycznych, z uwagi na fakt, iż z poziomu użytkownika struktura taka nie jest dostępna. W takich sytuacjach można:
- zwrócić się do producenta o opis struktury zbiorów danych – jednak z doświadczenia autorów wynika, iż takie dane niechętnie się udostępniane. Do wyjątków należy np. program Płatnik stosowany do rozliczeń z ZUS,
- załączyć do polityki instrukcję obsługi danej aplikacji,
- wykonać zrzuty z ekranu przedstawiające formularze do wprowadzania danych,
- przygotować opis przetwarzanych pól informacyjnych.

4) sposób przepływu danych pomiędzy poszczególnymi systemami – w tym przypadku należy dokładnie przeanalizować i określić w jaki sposób i w jakim kierunku dane przepływają pomiędzy systemami informatycznymi (np. z programu Kadry i płace do programu Płatnik – dane przenoszone są poprzez wyeksportowane pliku przez użytkownika i zaimportowanie go w programie Płatnik)

5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych – jest to wykaz stosowanych procedur mających na celu zabezpieczenie danych przed utratą, udostępnieniem, zniszczeniem. Przygotowanie tego wykazu wymaga uprzedniej analizy potencjalnego ryzyka związanego z przetwarzaniem danych i opracowaniem procedur, które będą adekwatne do potencjalnych zagrożeń. W ramach stosowanych środków ADO:

- może powołać Administratora Bezpieczeństwa Informacji,
- musi prowadzić i aktualizować dokumentację ochrony danych osobowych,
- musi nadawać upoważnienia do przetwarzania danych osobowych,
- musi prowadzić ewidencję osób upoważnionych do przetwarzania danych osobowych,
- musi zapewnić zapoznanie osób upoważnionych do przetwarzania danych osobowych z obowiązującymi regulacjami prawnymi.

b. Instrukcja obsługi systemu informatycznego

Instrukcja obsługi systemu informatycznego musi uwzględniać następujące elementy:

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

2) opis stosowanych metod i środków uwierzytelnienia (logowania) oraz procedury związane z ich zarządzaniem i użytkowaniem,

3) procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemach informatycznych,

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

5) sposób, miejsce i okres przechowywania:

- elektronicznych nośników informacji zawierających dane osobowe,
- kopii zapasowych

6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania szkodliwego (wirusy, konie trojańskie itp.)

7) sposób odnotowywania:

- daty pierwszego wprowadzenia danych do systemu,
- identyfikatora użytkownika wprowadzającego dane osobowe do systemu,
- źródła danych, w przypadku zbierania danych nie od osoby, której one dotyczą,
- informacji o odbiorcach,

- sprzeciwu na przetwarzanie danych w celach marketingowych lub na przekazanie ich innemu administratorowi danych.

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

5.2. Nadawanie upoważnień do przetwarzania danych osobowych oraz ich ewidencjonowanie

ADO lub ABI, jeśli został powołany, powinien nadawać upoważnienia do przetwarzania danych osobowych dla pracowników LGD i innych osób wykonujących zadania na rzecz LGD. Do grona osób niebędących pracownikami LGD zaliczyć można np. Radę Stowarzyszenia, zewnętrzną firmę, która administruje sprzęt informatyczny. Ponadto każde upoważnienie powinno być zewidencjonowane – musi być odnotowana data nadania i odebrania uprawnień, imię i nazwisko przetwarzającego, wykaz zbiorów, do których dana osoba ma dostęp oraz rodzaj uprawnień (np. wprowadzanie, modyfikacja, usuwanie, wgląd). GIODO zaleca, aby upoważnienie było w formie pisma, nawet elektronicznego, a nie przekazane ustnie. Upoważnienie powinno zawierać zobowiązanie osoby do przetwarzania danych zgodnie z przyjętymi procedurami oraz prawem, dlatego logiczne jest, aby wcześniej pracownik został zapoznany z przepisami i potwierdził to na piśmie w postaci oświadczania.

5.3. Obowiązek informacyjny

Obowiązek informacyjny dopełnić należy w dwóch sytuacjach:

- W momencie zbierania danych bezpośrednio od osoby, której dane dotyczą,
- W przypadku zbierania danych niebezpośrednio od osoby, której dane dotyczą (np. kupując bazę danych).

Obowiązek informacyjny polega na poinformowaniu danej osoby o:

- nazwie administratora danych (LGD),
- siedzibie LGD,
- celu zbierania danych,
- odbiorcach danych,
- prawie dostępu do treści danych oraz do ich poprawiania,
- źródle danych (w przypadku gdy dane nie pochodzą bezpośrednio od osoby, której dotyczą),

- zakresie danych (w przypadku gdy dane nie pochodzą bezpośrednio od osoby, której dotyczą),
- dobrowolności albo obowiązku podania danych (w przypadku obowiązku należy podać podstawę prawną).

Przyjąć należy, iż dopełnienie obowiązku informacyjnego pozwala zainteresowanemu na właściwą ocenę i podjęcie decyzji dotyczącej przekazania swoich danych osobowych.

Ponadto, na mocy Art. 32. 1 ustawy, „*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 tajemnicy państwowej, służbowej lub zawodowej,*
5) *uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane."*

W związku z powyższym każda osoba, której dane są przetwarzane przez LGD, może zwrócić się do LGD z prośbą o udzielenie powyższych informacji. Szczególną uwagę należy zwrócić na to, iż zapytanie może dotyczyć daty, od której dane są przetwarzane. Prowadząc elektroniczne zbiory danych należy zwrócić uwagę na to, czy odnotowują informację o dacie pierwszego wprowadzenia danych do systemu. Z doświadczeń autorów wynika, iż takie informacje od producenta najłatwiej jest uzyskać jeszcze przed zakupem aplikacji, a zakup każdej aplikacji przetwarzającej dane osobowe powinien być przeanalizowany pod kątem zgodności z wymogami prawa. Prowadząc bazę w arkuszu kalkulacyjnym należy dodać dwie

kolumny, w których będzie odnotowywana data wprowadzenia danych oraz imię i nazwisko wprowadzającego.

5.4. Przesłanki legalizujące przetwarzanie danych osobowych

Polska ustawa o ochronie danych osobowych w art. 23 stanowi o przesłankach dopuszczalności przetwarzania danych osobowych. Warto nadmienić, iż wystarczy, aby zrealizowana została wyłącznie jedna z określonego katalogu, aby przetwarzanie było legalne.

W pierwszej kolejności przetwarzanie danych osobowych dopuszczalne jest w sytuacji, gdy osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych. Zgoda na przetwarzanie danych osobowych musi być wyrażona w sposób wyraźny, a jej wszystkie aspekty muszą być jasne dla podpisującego w momencie jej wyrażania. Nie spełnia tego wymagania podpisanie oświadczenia o wyrażeniu zgody na przetwarzanie danych, stanowiącego dodatkowy element innego zobowiązania niezawierającego informacji o celach i zakresie przetwarzania tych danych. Ponadto, orzecznictwo wskazuje, iż: "[…] posługiwanie się taką czy inną techniką utrwalania danych nie przesądza o legalności albo nielegalności takiego utrwalania (przetwarzania). Dla takich ocen istotne znaczenie mają przede wszystkim podstawa prawna przetwarzania danych, rodzaj przetwarzanych danych oraz granice przetwarzania"[17]. Oświadczenie woli w kwestii przetwarzania danych osobowych osoba może w każdej chwili odwołać lub wycofać. Prawidłowo złożone oświadczenie woli powinno być poprzedzone udzieleniem wszelkich informacji i najlepiej odebraniem potwierdzenie, iż osoba składająca takie oświadczenie rozumie konsekwencje własnej decyzji. Mogą się także zdarzyć sytuacje, w których odebranie takowej zgody nie będzie możliwe, a kontekst uzasadni przetwarzanie danych osobowych ze względu na to, iż będzie to niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a uzyskanie oświadczenia woli jest niemożliwe, można przetwarzać dane bez zgody tej osoby, do czasu, gdy uzyskanie zgody będzie możliwe.

Po wtóre przetwarzanie danych osobowych jest dopuszczalne, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Podstawa prawna przetwarzania danych osobowych z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych będzie miała w szczególności zastosowanie do organów administracji publicznej. Są one zobowiązane do działania na podstawie i w granicach prawa, a co za tym idzie zbierając informacje i dane osobowe o obywatelach, ich działanie powinno opierać się na stosownej

[17]Wyrok WSA w Warszawie z 27.2.2004 r., II SA 291/03, Legalis.

podstawie prawnej umożliwiającej takie czynności. Owa zasada dotyczy wszelkich form przetwarzania danych osobowych, w tym i do ich udostępniania. W przypadku udostępniania danych osobowych przepisy ustawy o ochronie danych osobowych nie określają bowiem szczególnych wymogów w tym zakresie. W pierwszej kolejności odwołać się więc należy do przepisów prawa, na podstawie których dany zbiór danych jest prowadzony[18].

Kolejną przesłanką dopuszczalności przetwarzania danych osobowych jest sytuacja, gdy 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. Na konieczność przetwarzania danych osobowych w celu realizacji umowy można powoływać się tylko i wyłącznie po zawarciu umowy. W ujęciu praktycznym to zagadnienie budzi wątpliwości. Natomiast komentarza wymaga druga część ww. przesłanki. Otóż dopuszczalne jest przetwarzanie danych osobowych jeżeli zostaną spełnione następujące warunki:

1) przetwarzanie jest niezbędne do podjęcia działań przed zawarciem umowy,

2) zawarcie umowy następuje na żądanie osoby, której dane dotyczą.

Problematyczne wydaje się sformułowanie – *"na żądanie osoby, której dane dotyczą".* Należy zgodzić się tutaj z poglądem P. Barta i P. Litwińskiego, którzy twierdzą, iż: „do legalnego przetwarzania danych osobowych w związku z (przed) zawarciem umowy może dochodzić tylko i wyłącznie w przypadku, gdy to przyszła strona umowy w sposób jednoznaczny wyrazi chęć jej zawarcia. Należy jednocześnie podkreślić, że powołanie się na tę przesłankę jest możliwe, gdy osoba, której dane dotyczą, wyraża stanowczą propozycję zawarcia umowy, która wcale nie musi być ofertą w rozumieniu KC"[19]. W ów katalog legalizujący wpisze się także sytuacja, w której druga strona (np. przedsiębiorca) przedstawi propozycję zawarcia umowy, a osoba fizyczna wyrazi co najmniej rzeczywiste zainteresowanie, które powinno przyjmować formę oświadczenia woli, ze wszelkimi tego konsekwencjami.

Następną przesłanką legalizującą przetwarzanie danych osobowych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego. W pierwszej kolejności należy stwierdzić, iż kluczowym wydaje się tu określenie stwierdzenia *„realizowanych dla dobra publicznego"*, co w nauce prawa jest powszechnie uznawane jako „wykonywane przez podmioty administracji publicznej". Warto nadmienić, iż nie może się to wiązać z działaniami władczymi aparatu państwa oraz podmioty publiczne nie mogą wykorzystywać tego w związku z prowadzoną przez nie działalnością zarobkową, np. poprzez posiadane udziału w spółkach prawa handlowego. Ponadto podmioty, o których mowa w art. 3 ust. 1 ustawy o ochronie danych

[18] P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2016, s. 14, Legalis.
[19] *Ibidem*.

osobowych, uważa się za jednego administratora danych, jeżeli przetwarzanie danych służy temu samemu interesowi publicznemu.

Dopuszczalne jest przetwarzanie danych osobowych, jeżeli jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów. Za prawnie usprawiedliwiony cel, o którym mowa powyżej, uważa się w szczególności:

1) marketing bezpośredni własnych produktów lub usług administratora danych;

2) dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

5.5. Klauzule informacyjne oraz zgody na przetwarzanie danych osobowych

W momencie zbierania danych osobowych należy poinformować osobę, której dane dotyczą o nazwie administratora danych osobowych i jego siedzibie, celu zbierania danych, dobrowolności (obowiązek informacyjny) oraz w pewnych sytuacjach należy zalegalizować przetwarzanie danych poprzez odebranie zgody na przetwarzanie danych osobowych (rozdział 5.4). Warto oba te elementy łączyć: np. pod klauzulą zgody (wymagającą zaznaczenia) dodać klauzulę informacyjną.

Klauzula informacyjna - rekrutacja pracownika w ogłoszeniu o pracę

> Zgodnie z art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych informuję, iż:
> 1) administratorem Pani/Pana danych osobowych jest (LGD) z siedzibą w (Adres LGD)
> 2) Pani/Pana dane osobowe przetwarzane będą w celu tej oraz **przyszłych rekrutacji** i nie będą udostępniane innym odbiorcom,
> 3) posiada Pani/Pan prawo dostępu do treści swoich danych oraz ich poprawiania,
> 4) podanie danych osobowych jest dobrowolne.

Zgoda na długotrwałe przechowywanie CV

> Zgodnie z ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997 wyrażam zgodę na przetwarzanie danych osobowych przez LGD zawartych w mojej ofercie pracy dla potrzeb aktualnej i **przyszłych** rekrutacji.

Klauzula informacyjna – składanie wniosków o przyznanie pomocy

> Zgodnie z art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych informuję, iż:
> 1) administratorem Pani/Pana danych osobowych jest (LGD) z siedzibą w (Adres LGD)

2) Pani/Pana dane osobowe przetwarzane będą w celu: oceny, realizacji oraz ewaluacji wniosku i nie będą udostępniane innym odbiorcom,

3) posiada Pani/Pan prawo dostępu do treści swoich danych oraz ich poprawiania,

4) podanie danych osobowych jest dobrowolne, niemniej niepodanie danych wskazanych we wniosku uniemożliwia dalsze procedowanie.

Klauzula informacyjna – przyjmowanie członków do stowarzyszenia

Zgodnie z art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych informuję, iż:

1) administratorem Pani/Pana danych osobowych jest (LGD) z siedzibą w (Adres LGD)

2) Pani/Pana dane osobowe przetwarzane będą w celach statutowych Stowarzyszenia (LGD) i udostępnione zostaną na stronie internetowej *adres strony internetowej LGD*,

3) posiada Pani/Pan prawo dostępu do treści swoich danych oraz ich poprawiania,

4) podanie danych osobowych jest dobrowolne.

Zgoda na publikację danych na stronie dla członków stowarzyszenia

Wyrażam zgodę na publikowanie moich danych osobowych (imię i nazwisko) przez LGD na stronie internetowej *adres strony*.

Zgoda na karcie doradztwa

Zgodnie z Ustawą z dnia 29 sierpnia 1997 roku o Ochronie Danych Osobowych wyrażam zgodę na przetwarzanie moich danych osobowych przez LGD do celów związanych z udokumentowaniem doradztwa.

Klauzula informacyjna – na karcie doradztwa

Zgodnie z art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych informuję, iż:

1) administratorem Pani/Pana danych osobowych jest (LGD) z siedzibą w (Adres LGD)

2) Pani/Pana dane osobowe przetwarzane będą w celu udokumentowania odbytego doradztwa i nie będą udostępniane innym odbiorcom,

3) posiada Pani/Pan prawo dostępu do treści swoich danych oraz ich poprawiania,

4) podanie danych osobowych jest dobrowolne.

Zgoda na liście obecności ze szkolenia

Zgodnie z Ustawą z dnia 29 sierpnia 1997 roku o Ochronie Danych Osobowych wyrażam zgodę na przetwarzanie moich danych osobowych przez LGD do celów związanych z udokumentowaniem oraz rozliczeniem szkolenia.

Klauzula informacyjna – na liście obecności na szkoleniu

Zgodnie z art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych informuję, iż:

1) administratorem Pani/Pana danych osobowych jest (LGD) z siedzibą w (Adres LGD),

2) Pani/Pana dane osobowe przetwarzane będą w celu udokumentowania oraz rozliczenia szkolenia i nie będą udostępniane innym odbiorcom,

3) posiada Pani/Pan prawo dostępu do treści swoich danych oraz ich poprawiania,

4) podanie danych osobowych jest dobrowolne.

Zgoda na wykorzystanie wizerunku

Zgodnie z Ustawą z dnia 29 sierpnia 1997 roku o Ochronie Danych Osobowych wyrażam zgodę na utrwalanie i publikację mojego wizerunku przez LGD do celów związanych z promowaniem działalności stowarzyszenia.

Klauzula informacyjna - formularz na stronie

Zgodnie z art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych informuję, iż:

1) administratorem Pani/Pana danych osobowych jest (LGD) z siedzibą w (Adres LGD)

2) Pani/Pana dane osobowe przetwarzane będą w celu prowadzenia korespondencji i nie będą udostępniane innym odbiorcom,

3) posiada Pani/Pan prawo dostępu do treści swoich danych oraz ich poprawiania,

4) podanie danych osobowych jest dobrowolne

Zgoda – formularz korespondencyjny

Zgodnie z Ustawą z dnia 29 sierpnia 1997 roku o Ochronie Danych Osobowych wyrażam zgodę na przetwarzanie moich danych przez LGD w celu prowadzenia korespondencji z LGD.

Klauzula informacyjna - newsletter

Zgodnie z art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych informuję, iż:

1) administratorem Pani/Pana danych osobowych jest (Nazwa LGD) z siedzibą w (Adres LGD)

2) Pani/Pana dane osobowe przetwarzane będą w celu subskrypcji do newslettera i nie będą udostępniane innym odbiorcom,

3) posiada Pani/Pan prawo dostępu do treści swoich danych oraz ich poprawiania,

4) podanie danych osobowych jest dobrowolne.

Zgoda – newsletter

Zgodnie z Ustawą z dnia 29 sierpnia 1997 roku o Ochronie Danych Osobowych wyrażam zgodę na przetwarzanie moich danych przez LGD w celu informowania przez LGD o podejmowanych działaniach

5.6. Rejestracja zbiorów danych osobowych

Ustawa o ochronie danych osobowych w pewnych sytuacjach nakłada obowiązek rejestracji zbiorów danych osobowych (art. 40), a niezgłoszenie zbioru jest przestępstwem zagrożonym odpowiedzialnością karną (art. 53).

W pierwszej kolejności należy rozbudować definicję zbioru danych osobowych zaproponowaną we wcześniejszym rozdziale publikacji. Otóż za zbiór danych osobowych uważa się:

- zestaw danych osobowych (pewna ilość informacji),
- posiadający określoną strukturę,
- posiadający odpowiednie kryteria dostępu (np. wyszukiwanie danych według odpowiedniego klucza),
- może być podzielony funkcjonalnie lub rozproszony (jeden zbiór można przetwarzać w wielu systemach lub wiele zbiorów można przetwarzać w jednym systemie)[20].

Należy dostrzec pogląd prezentowany w doktrynie, iż do wyodrębnienia zbioru wystarczy tylko jedno kryterium wyszukiwania pomimo użycia liczby mnogiej przy interpretacji ustawy, ale warto pamiętać, iż ostatnie słowo zawsze będzie należało do sądu[21]. Przykładami owych kryteriów może być nazwisko, rodzaj dokumentów, data, indeks itd.

W związku z tym, jeżeli uznamy, iż mamy do czynienia ze zbiorem danych osobowych, to należy pamiętać jakie obowiązki ADO wynikają z tego fakt, a są to:

[20] L. Kępa, *Ochrona danych…*,*op. cit*., s. 168.
[21] J. Barta, P. Fajgielski,R. Markiewicz*, Ochrona danych …*,*op. cit*, s. 364.

- zgłoszenie zbioru do rejestracji (gdy nie ma ABI lub gdy jest ABI, a zbiór zawiera dane wrażliwe),
- uwzględnienie praw osób, których dane zawarte w danym zbiorze dotyczą (m.in. prawo do informacji, celu przetwarzania, komu się je udostępnia, prawo do aktualizacji etc.)
- aktualizowanie zbioru w związku ze zmianami,
- wyrejestrowanie zbioru.

Istnieją 3 główne czynniki odróżniania od siebie zbiorów:

- cel ich przetwarzania,
- podstawa prawna pozwalająca na przetwarzanie danych osobowych,
- zakres owych danych (kategorie danych).

Istnieje także kategoria 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 ustawy o ochronie danych osobowych, czyli dotyczące zabezpieczenia danych osobowych na ogólnych zasadach.

Podmiot przetwarzający dane osobowe, niezależnie od swojej woli, musi zarządzać sprawnie zbiorami danych w oparciu o obowiązujące przepisy prawa, niezależnie od tego czy będą one podlegały zgłoszeniu czy też nie. Do najważniejszych czynności w tym zakresie należą:

- stała analiza przetwarzanych danych osobowych,
- weryfikacja adekwatności przetwarzania zbioru do ustawowej definicji zbioru,
- badanie ewentualnych przypadków zwolnień z rejestracji,
- prowadzenie dokumentacji zbiorów,
- przegląd zbiorów co 30 dni,
- aktualizowanie zbioru, jeżeli wystąpią zmiany,
- zgłoszenie wykreślenia zbioru, jeżeli zaprzestano przetwarzania danych osobowych w danym zbiorze.

Rejestracja zbiorów

Procedura rejestracji zbiorów uzależniona jest od tego czy powołano administratora bezpieczeństwa informacji (ABI) czy też nie. Jeżeli tego dokonano, to zbiory nie będą podlegały rejestracji w GIODO, za wyjątkiem zbiorów danych sensytywnych, a jeśli nie powołano ABI zbiory muszą być rejestrowane w GIODO.

Brak Administratora Bezpieczeństwa Informacji

W przypadku braku ABI-ego i przetwarzania danych osobowych w zbiorach jest wysoce prawdopodobne, że niektóre z nich należy zarejestrować. Jednak owa czynność powinna być dokonana już pod zapewnieniu zabezpieczenia i wdrożeniu wielu mechanizmów ochrony danych.

Zgłoszenie i aktualizacje zbiorów można wysłać do GIODO:

- w formie papierowej,
- wspomagane elektronicznie przez program e-GIODO,
- w całości wypełnione i wysłane elektronicznie za pomocą programu e-GIODO.

Należy bezwzględnie pamiętać, iż rozróżnia się 2 zasadnicze momenty w procedurze rejestracji zbioru:

- wysłanie wniosku rejestrowego,
- zarejestrowanie zbioru.

Od tego uzależnione są dalsze czynności, gdyż dane zwykłe można przetwarzać już po wysłaniu wniosku, a dane sensytywne dopiero po pozytywnym zarejestrowaniu zbioru w GIODO.

Za rejestrację zbioru GIODO nie pobiera żadnych opłat.

Rejestr zbiorów prowadzony przez Administratora Bezpieczeństwa Informacji

W przypadku powołania ABI nie ma konieczności zgłaszania zbiorów do GIODO, chyba że są to zbiory danych wrażliwych. Zasady prowadzenia rejestru przez ABI-ego określa właściwe rozporządzenie wykonawcze, które szczegółowo reguluje owe kwestie[22]. W zasadzie można uznać, iż obydwa rejestry niczym się nie różnią, gdyż podlegają analogicznemu reżimowi prawnemu z jedyną różnicą w postaci podmiotu prowadzącego. Rejestr ABI może być prowadzony elektronicznie lub papierowo i musi być udostępniany każdej zainteresowanej osobie. Informacje dotyczące powierzenia przetwarzania danych osobowych nie muszą być umieszczone w wersji elektronicznej, jeżeli prowadzony jest rejestr papierowy, a w rejestrze papierowym takie informacje muszą się znaleźć. ABI aktualizuje swój rejestr po każdym zdarzeniu to uzasadniającym. W rejestrze ABI rejestruje się te same zbiory co w GIODO z wyjątkiem zwolnionych. Ciekawostką jest fakt, iż w przypadku, gdy przez podmiot (LGD) przetwarzane są zbiory danych wrażliwych zarejestrowane w GIODO, to mimo wszystko ów zbiór musi znaleźć się w rejestrze prowadzonym przez ABI.

[22] Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbioru danych.

Jakie zbiory rejestrować?

Każdy zbiór danych osobowych należy zarejestrować (tu patrz: sytuacja z powołanym ABI), chyba że stanowi wyjątek z art. 43 ust. 1, tj.:

„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 właściwe 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;

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.”.

W dalszej części opracowania zostaną wskazane najczęściej spotykane zbiory podlegające rejestracji w związku z funkcjonowaniem Lokalnych Grup Działania.

6. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

6.1. Informacje ogólne

Administrator Danych Osobowych może samodzielnie przetwarzać dane osobowe lub na podstawie umowy zlecić konkretne czynności innemu podmiotowi, co jest szczególnie istotne przy dynamicznie rozwijających się relacjach pomiędzy podmiotami rynku. Najczęściej taka umowa będzie polegała na świadczeniu usług, co może świadczyć o tym, iż właściwą formą będzie umowa zlecenia w myśl Kodeksu Cywilnego. Owa umowa powinna być zawarta na piśmie, ale w doktrynie spotyka się poglądy, iż „brak dochowania tego wymogu nie będzie wywierał skutku w postaci nieważności umowy[23]. W konsekwencji, umowa powierzenia przetwarzania danych osobowych niespełniająca tego wymogu (np. umowa ustna) od strony prawa cywilnego jest ważna, natomiast może powodować niekorzystne skutki na gruncie prawa administracyjnego. Niespełnienie tego wymogu powoduje naruszenie przepisów ustawy o ochronie danych osobowych i może powodować sankcje w postaci decyzji administracyjnej wydanej na podstawie art. 18 ustawy o ochronie danych osobowych”[24]. Wszelkie kwestie dotyczące powierzenia przetwarzania danych osobowych strony mogą określić w umowie głównej jako jej integralną część lub w aneksie do umowy głównej lub w odrębnej umowie. Umowy powierzenia nie muszą zawierać między sobą podmioty z sektora publicznego takie jak: organy państwowe, organy samorządu terytorialnego oraz państwowe i komunalne jednostki organizacyjne. Podmiot, któremu powierzono przetwarzanie danych osobowych nie staje się ich właścicielem, gdyż jego rola sprowadza się do ich przetwarzania w zakresie i imieniu oraz za zgodą zleceniodawcy. W umowie powierzenia powinien być jak najbardziej precyzyjnie określony cel oraz zakres przetwarzania danych osobowych z zastrzeżeniem, iż cel oraz zakres nie mogą być szersze niż te, które przysługują zleceniodawcy. W zasadzie należy stwierdzić, że nie ma ograniczeń w kwestii powierzania przetwarzania danych osobowych. Wyjątkiem jest detektyw, któremu ustawa o usługach detektywistycznych w art. 8 ust. 2 tego zabrania. Zleceniodawca może powierzać przetwarzanie danych osobowych zarówno ze zbiorów zarejestrowanych, niezarejestrowanych oraz pojedynczo zawartych w zestawach.

[23] Zob. szerz. *A. Szewc*, *Z problematyki ochrony danych osobowych*, cz. III, R. Pr. 1999, Nr 5, s. 21.

[24] J. Barta, P. Fajgielski,R. Markiewicz*, Ochrona danych …, op. cit.*, s. 508.

6.2. Obowiązki zleceniodawcy

Podstawowym obowiązkiem zleceniodawcy jest ujawnienie w rejestrze zbiorów danych osobowych prowadzonym przez GIODO informacji, które dotyczą podmiotu, któremu powierzono przetwarzanie danych osobowych pod warunkiem, że dotyczy to danych, które podlegają zgłoszeniu. Informacje zgłaszane do GIODO należy aktualizować w razie zmiany zleceniobiorcy. W instytucjach, gdzie podpisuje się znaczne ilości umów powierzenia korzystnym wydaje się prowadzenie ich rejestru ze względu na przejrzystość i spełnienie obowiązków wynikających z ustawy. Zleceniodawca jest zwolniony z rejestracji zbioru zleceniobiorców, chyba że cel jest szerszy niż zakres umowy powierzenia, np. zleceniodawca ma zamiar prowadzić akcje marketingowe wśród podmiotów, którym powierzono przetwarzanie danych osobowych.

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.

Zleceniodawcy przysługuje także uprawnienie do przeprowadzania kontroli, co powinno być zawarte w umowie powierzenia, gdyż stały nadzór nad działalnością zleceniobiorcy leży w interesie zleceniodawcy, który powinien posiadać wiedzę na temat przetwarzania danych osobowych, za które ponosi odpowiedzialność.

6.3. Obowiązki zleceniobiorcy

Podmiot przyjmujący do przetwarzania dane osobowe obowiązany jest spełnić szereg wymagań przewidzianych przepisami prawa zanim jeszcze faktycznie otrzyma dane osobowe. Zleceniobiorca jest zobowiązany m.in. do: zabezpieczenia danych osobowych, wyznaczenia administratora bezpieczeństwa, wydania swoim pracownikom upoważnienia do przetwarzania danych osobowych, prowadzenia ewidencji osób upoważnionych i zastosowania wszelkich wymogów rozporządzenia MSWiA[25], tj.: przygotowania dokumentacji (polityka bezpieczeństwa, instrukcja zarządzania systemami informatycznymi – jeśli to konieczne), wdrożenia odpowiednich zabezpieczeń danych osobowych. Reasumując można stwierdzić, iż zleceniobiorcy będą dotyczyć wszystkie regulacje ustawy o ochronie danych osobowych za wyjątkiem: przesłanek legalności, obowiązku informacyjnego i prawa do informacji (można to przekazać zleceniobiorcy, ale w przypadku, gdy będzie zbierał dane w imieniu zleceniodawcy), rejestrowania i aktualizowania

[25]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 r. poz. 1024.

zbiorów danych osobowych. Zleceniobiorca może być także kontrolowany przez GIODO. Zleceniobiorca jest zwolniony z przymusu informowania konkretnych osób o przysługujących im prawach etc., gdyż przepisy prawa nie określają tej materii, co oznacza, że może być do tego zobligowany na podstawie zapisów umowy powierzenia.

6.4. Typowe sytuacje zawierania umów powierzenia

Do często spotykanych w praktyce przykładów kiedy należy zawierać umowy powierzenia należy zaliczyć sytuacje:

- poczta elektroniczna na serwerze zewnętrznym,
- księgowość prowadzona przez podmiot zewnętrzny,
- przechowywanie w archiwum dokumentów zleceniodawcy,
- usługi rzeczoznawców, likwidatorów szkód,
- pośrednictwo w sprzedaży,
- zewnętrzne usługi callcenter,
- niszczenie dokumentów,
- praktyka używania oprogramowania w tzw. chmurze,
- zlecenie administrowania siecią komputerową, serwerami firmowymi,
- medycyna pracy, bhp,
- obsługa IT,
- świadczenie usług doradztwa prawnego,
- zewnętrzna obsługa kadr.

Po analizie wyżej wymienionych przykładów można wnioskować, że owe umowy będą konieczne w sytuacjach, które determinują konieczność dostępu zleceniobiorcy do danych osobowych w celu wykonania zlecenia.

Oprócz tego warto podać przykłady, których analiza jest bardziej wymagająca w związku z nieprecyzyjnym ustawodawstwem. W pierwszej kolejności chodzi o przechowywanie danych osobowych na serwerach firmy hostingowej. Rozróżnia się tu dwa przypadki ze względu na to czy dane przechowywane ww. miejscach są zaszyfrowane. Jeśli nie są, to konieczne jest zawarcie umowy powierzenia. Natomiast w sytuacji, gdy dane znajdujące się na serwerach firmy hostingowej są zaszyfrowane, a jedynym podmiotem, który może je odszyfrować jest zleceniodawca, a oprócz tego firma hostingowi nie posiada wiedzy o rodzaju ww. danych, to od zawarcia takiej umowy można odstąpić[26].

[26] Zob. szerz. L. Kępa, *Ochrona danych…*,*op. cit*., s. 162.

Oprócz tego należy bezwzględnie pamiętać o każdorazowym dokonaniu analizy zawieranych umów z rozmaitymi kontrahentami pod kątem przetwarzania danych osobowych. W szczególności należy odpowiedzieć sobie na pytanie: czy w związku z wykonaniem przedmiotu umowy zleceniobiorca będzie potrzebował dostępu do tego typu danych, jeśli tak, to bezwzględnie należy to uregulować na jeden ze sposobów wskazanych powyżej!

7. ZABEZPIECZENIE DANYCH OSOBOWYCH

Ustawodawca w art. 36 ustawy o ochronie danych osobowych nakłada na ADO obowiązki ochrony danych, tj.: ”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”[27]. Uszczegółowienie ww. przepisu stanowi 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. z 2004 r. Nr 100, poz. 1024).

Wymogi dotyczące ochrony danych osobowych powinny być spełnione przed rozpoczęciem ich przetwarzania, a co istotne, powinien uczynić im zadość zarówno ADO, a także w przypadku powierzenia – zleceniobiorca. Warto podkreślić, że zawarte w ww. aktach prawnych obowiązki są minimalne i nic nie stoi na przeszkodzie, aby dodawać kolejne.

7.1. Pojęcie bezpieczeństwa danych osobowych i rodzaje zabezpieczeń

Punktem wyjścia przy zdefiniowaniu bezpieczeństwa danych osobowych jest norma PN-ISO/IEC 27001:2007, gdzie określono, iż za bezpieczeństwo informacji uznaje się zachowanie:

- poufności – dane pozostają w tajemnicy, a możliwość zapoznania się z nimi posiadają tylko właściwe osoby (art. 37 ustawy o ochronie danych osobowych),
- integralności – dane nie zostały zniszczone, uszkodzone lub zmienione przez osobę nieupoważnioną (art. 36 ust. 1 ustawy o ochronie danych osobowych),

[27] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. 2016 r. poz. 922.

- rozliczalności – możliwość przypisania konkretnych działań konkretnemu podmiotowi (art. 38 ustawy o ochronie danych osobowych).

W związku z analizą potencjalnych zagrożeń oraz typów danych wyróżnia się następujące poziomy bezpieczeństwa przetwarzania danych w systemie informatycznym: podstawowy (dotyczy wszystkich danych), podwyższony (wymagany przy danych sensytywnych), wysoki (zawiera dwa poprzednie i jest wymagany przy podłączeniu systemu do sieci publicznych[28]).

Wszelkie zabezpieczenia wymagane przepisami prawa mają na celu ograniczenie ryzyka wobec danych osobowych do poziomu akceptowalnego przez ustawodawcę. W związku z tym wyróżnia się zabezpieczenia ze względu na typ przetwarzanych danych (materialne lub niematerialne).

Podstawowe typy zabezpieczeń to:

- środki ochrony fizycznej,
- zabezpieczenia informatyczne,
- środki organizacyjne.

7.2. Zabezpieczenia fizyczne

Ten typ zabezpieczeń odnosi się głównie do danych w formie materialnej, czyli akt, wydruków, kserokopii etc. Wspomniane rozporządzenie nie określa wymaganych zabezpieczeń fizycznych. W związku z tym dobierając zabezpieczenia warto rozważyć sugerowane przez GIODO rodzaje określone w części E16 elektronicznego wniosku zgłoszenia zbioru do rejestracji. Są to m.in.: użycie systemu alarmowego, zabezpieczenie okien kratami, zabezpieczenie pomieszczeń drzwiami o podwyższonej odporności na włamania, system kontroli dostępu do pomieszczeń, stosowanie monitoringu z zastosowaniem kamer, niszczenie danych z użyciem niszczarek, przechowywanie danych w szafach, sejfach i kasach pancernych lub nadzorowanie pomieszczeń przez ochronę. Są to propozycje zabezpieczeń, które powinny być dobrane odpowiednio do zagrożeń. Warto wyróżnić wybrane zabezpieczenia i dokonać syntetycznego opisu ich specyfiki.

Przebywanie na obszarze przetwarzania i obsługa interesantów

Załącznik (I.1) do ww. rozporządzenia MSWiA stanowi, iż na terenie przetwarzania danych osobowych osoby nieupoważnione mogą przebywać wyłącznie za zgodą i w obecności osoby upoważnionej. Oprócz tego w praktyce spotyka się stosowanie monitoringu owych miejsc w celu

[28] L. Kępa, *Ochrona danych…,op. cit*., s. 256.

dokumentowania wizyt danych osób. Można zatem wyróżnić 2 typy miejsc, czyli te, gdzie mogą przebywać osoby nieupoważnione, np. interesanci, klienci oraz takie, gdzie dostęp jest w znaczny sposób ograniczony jak np. serwerownie.

Obsługiwany klient/interesant nie powinien mieć dostępu do danych innych niż swoje własne. Nie powinno się zostawiać osób nieupoważnionych osób samych w pomieszczeniu, gdzie przechowywane są inne niż jego dane lub jest włączony i niezablokowany komputer.

Serwerownie

Są to miejsca, gdzie usytuowane są centralne komputery zwane serwerami, na których zgromadzone są wszelkie bazy danych pliki etc. związane z działalnością podmiotu. Oczywiście mniejsze firmy czy stowarzyszenia mogą nie posiadać tego typu sprzętu. W sytuacji, gdy serwery występują, miejsca ich umieszczenia powinny być szczególnie chronione poprzez ograniczanie osób mających do nich dostęp, do wejścia konieczny jest klucz, a same serwery są umieszczane w specjalnych szafach, które także mogą, a nawet powinny być zamykane na klucz. Dodatkowo w serwerowniach powinny być zapewnione odpowiednie warunki obniżające ryzyko ich uszkodzenia, np.: klimatyzacja, system przeciwpożarowy, czy też powinny być to miejsca z minimalnym ryzykiem zalania.

Zasada czystego biurka

Niezależnie od skali podmiotu warto zastosować politykę czystego biurka, która polega na chowaniu dokumentów i innych nośników z danymi osobowymi do szaf i ich zamykania oraz blokowania lub wyłączania komputera, gdy odchodzi się od stanowiska pracy. Ograniczy to możliwości pozyskania danych osobowych przez osobę nieupoważnioną, która będzie przebywać w danym pomieszczeniu. Oprócz tego warto stosować tę zasadę w miejscach, gdzie korzysta się z usług firm/osób sprzątających lub ochrony.

Drukowanie dokumentów

W praktyce zdarza się, że drukarki pracowników stoją w miejscach dostępnych dla osób postronnych. Może się zdarzyć, że pracownik zapomni odebrać wydrukowany dokument, który następnie może wejść w posiadanie osoby spoza firmy. Wartym uwagi sposobem na ograniczanie tego typu sytuacji jest wprowadzenie hasła, które umożliwia wydrukowanie dokumentu.

Transportowanie informacji

W praktyce zdarza się, że dokumenty i inne nośniki z danymi osobowymi są transportowane przez pracowników. Warto pamiętać, iż przy tego typu praktykach należy zabezpieczyć się poprzez szyfrowanie danych na nośnikach, co stanowi wymóg zawarty w rozporządzeniu MSWiA. Ponadto warto tworzyć kopie zapasowe w innych miejscach, aby po utracie nośnika z zaszyfrowanymi plikami skończyło się na stracie finansowej, a nie utracie danych osobowych i ewentualnej odpowiedzialność – w tym karnej! Osobom, które praktykują pracę w trakcie podróży i chcą uchronić się przed podglądaczami z pewnością można rekomendować tzw. filtr prywatności, który nakleja się na ekran laptopa czy tabletu.

7.3. Zabezpieczenia organizacyjne

Zabezpieczenia organizacyjne mają za zadanie chronić dane przetwarzane przez stowarzyszenie poprzez zastosowanie usystematyzowanie zakresu obowiązków i odpowiedzialności związanej z przetwarzaniem danych.

Podstawowym elementem zabezpieczeń organizacyjnych jest opracowana i wdrożona polityka bezpieczeństwa danych osobowych, która powinna stanowić zbiór spójnych zasad stosowanych w LGD i jednocześnie określać obowiązki jak i odpowiedzialność poszczególnych osób.

Kolejnym elementem zabezpieczeń organizacyjnych jest powołanie ABI (nieobowiązkowe), czyli osoby mającej wiedzę i przygotowanie do bezpiecznego przetwarzania danych, która będzie dbać o zachowanie właściwych procedur.

Do zabezpieczeń organizacyjnych należy również zaliczyć procedury nadawania upoważnień do przetwarzania danych oraz ich ewidencjonowanie (rozdział 5.2).

Ponadto niezbędne jest zaznajomienie pracowników z właściwymi procedurami bezpiecznej pracy opartej o dane osobowe, uwrażliwienie na możliwe zagrożenia, informowanie o konsekwencjach. Za zapoznanie pracowników z przepisami odpowiada ABI, a jeśli nie został powołany – ADO.

7.4. Zabezpieczenia informatyczne

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. z 2004 r. Nr 100, poz. 1024) na systemy informatyczne oraz przetwarzanie danych w zbiorach elektronicznych nakłada określone wymogi, które

wstępnie zostały opisane w rozdziale 5.1. Warto przy tym wspomnieć, że na pierwszym, niechlubnym miejscu zagrożeń dla systemów informatycznych stoi człowiek. Stosowanie właściwych procedur może jeśli nie zapobiec to przynajmniej zminimalizować skutki popełnianych błędów.

Logowanie (uwierzytelnianie)

Jest to proces logowania się do systemu operacyjnego lub aplikacji bazodanowej. Jeśli dane przetwarzane są jedynie w programach (zabezpieczonych hasłami), to z hasła do systemu operacyjnego można zrezygnować, choć nie jest to wskazane z uwagi na to, że w każdym komputerze z pewnością można odnaleźć chociażby dokumenty zawierające dane osobowe lub inne dane istotne dla LGD.

Każdy użytkownik powinien mieć własny login oraz hasło, którego minimalna długość to 6 znaków (w przypadku systemów przetwarzających dane wrażliwe – 8 znaków, niemniej w LGD'ach nie zostały stwierdzone dane wrażliwe). Login do systemu nie może być przyznany innej osobie. Hasła powinny być zmieniane co 30 dni.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemach informatycznych

Z uwagi na rozległość możliwych zagrożeń należy przed uruchomieniem systemu informatycznego dokonać oględzin stanowiska pod kątem próby nieupoważnionego dostępu czy też obecności nieznanych urządzeń pendrive w portach komputera (mogą to być tzw. keyloggery sprzętowe lub pendrive'y prowadzące do zwarcia i tym samym zniszczenia sprzętu oraz zgromadzonych danych). Po uruchomieniu systemu przed opuszczeniem stanowiska należy włączyć wygaszacz ekranu zabezpieczony hasłem (skrót ⊞ + L), lub wygaszacz sam powinien się włączyć po określonym interwale czasu np. 10 minutach. Zakończenie pracy zawsze powinno polegać na wyłączeniu wszystkich działających aplikacji oraz wyłączeniu komputera i uporządkowaniu nośników danych.

Kopie bezpieczeństwa

Jest to podstawowe zabezpieczenie chroniące przed utratą danych. Powinny być wykonywane regularnie, a obejmować powinny nie tylko bazy danych, ale również dane gromadzone na dyskach komputerów. Wskazane jest, aby w kopie wykonywały się automatycznie z określoną częstotliwością, a jeśli nie jest to możliwe to wskazane jest, aby została do tego powołana osoba, której zadaniem będzie sporządzanie kopii lub weryfikowanie czy rzeczywiście zostały wykonane.

Ponadto, kopie bezpieczeństwa powinny być przechowywane w innej fizycznej lokalizacji niż komputery, których wykonywana jest kopia danych.

Nośniki danych

Dość powszechne jest zapominanie o tym, iż na nośnikach danych mogą być zgromadzone dane. Niestety często ulegają one zagubieniu, a dane na nich zgromadzone mogą wówczas być udostępnione osobom niepowołanym (znalazcy). Aby uchronić się przed tym zagrożeniem należy szyfrować przechowywane dane, a także zawsze być w posiadaniu ich kopii danych. Ponadto w komputerach należących do LGD nie należy umieszczać nieznanych nośników bowiem mogą zawierać szkodliwe oprogramowanie, doprowadzić do zwarcia i uszkodzenia sprzętu.

Komputery przenośne

Podobnie jak w przypadku nośników danych, dane znajdujące się w komputerach przenośnych powinny się znajdować na partycjach szyfrowanych. Należy również uważać na sposób przewożenia sprzętu np. samochodem – laptop powinien być przewożony np. przypięty pasami i niepozostawiany w samochodzie podczas nieobecności jego użytkownika. Istotne są również czynniki atmosferyczne – bardzo niskie temperatury mogą doprowadzić do uszkodzenia sprzętu. Jeśli laptopy są wykorzystywane do pracy w LGD'ach to należy je również przypinać linką bezpieczeństwa.

Oprogramowanie antywirusowe

Jest to niezbędny element każdego komputera, stanowi podstawową zaporę zabezpieczającą przed działaniem wirusów, koni trojańskich, robaków internetowych. Antywirusa nie można wyłączać, ani blokować jego aktualizacji.

Firewall – zapora ogniowa

Jest to oprogramowanie chroniące przed atakiem z zewnątrz sieci internetowej. Standardowo jest wbudowane w system Windows, ale może być również zainstalowane jako dodatkowe oprogramowanie. Nie wolno wyłączać tego oprogramowania.

Konserwacja i przeglądy systemu

System informatyczny wymaga regularnych usprawnień i konserwacji. Niestety jego działanie może być zakłócone awariami, które negatywnie przekładają się na zachowanie procesu ciągłości

pracy i potencjalną utratę danych (jeśli nie są sporządzane kopie danych). To zadanie należy powierzyć osobie mającej odpowiednią wiedzę i doświadczenie.

8. Przechowywanie danych osobowych

8.1. Zasady ogólne

Czas przetwarzania danych osobowych ograniczony jest m.in. przez ustawę o ochronie danych osobowych. Termin branżowy określający czas przetwarzania (przetrzymywania danych osobowych i to kiedy należy dane osobowe anonimizować lub je usunąć nazywa się: **retencja danych osobowych**. Zgodnie z przepisami prawa dane będą usuwane, np. w przypadku LGD w następujących sytuacjach:

- gdy należy zaprzestać je przetwarzać (skończył się cel przetwarzania, LGD zakończyło działalność na podstawie odrębnych przepisów, co oznacza, że administrator danych osobowych znikł),
- gdy zażąda tego osoba, której dane dotyczą (może to uczynić poprzez złożenie sprzeciwu, odwołanie zgody lub rozwiązanie umowy),
- gdy Generalny Inspektor Ochrony Danych Osobowych nakaże zaprzestać przetwarzania danych osobowych w trybie art. 18 ust. 1 ustawy o ochronie danych osobowych.

Dane osobowe można przetwarzać przez cały okres istnienia przesłanki ich legalności, tj. kiedy cel przetwarzania jest ciągle aktualny. Co do zasady dane osobowe przetwarza się do momentu osiągnięcia celu, dla którego rozpoczęto ich przetwarzanie. Dane osoby można usuwać bez jej zgody. W związku z tym *a contrario* dane osobowe można przetwarzać:

- jeżeli podstawą była zgoda do przetwarzania,
- w sytuacji, gdy dane przetwarzane są w celach marketingowych własnych towarów i usług administratora – do momentu złożenia sprzeciwu przetwarzania w tym celu lub gdy zniknie powód ich przetwarzania,
- gdy dane przetwarzane są w celu realizacji umowy – do czasu zrealizowania jej postanowień i wygaśnięcia roszczeń (proces windykacji zalicza się do okresu ważności roszczeń),
- gdy dane należy przechowywać na podstawie obowiązujących przepisów prawa – do czasu, gdy ów obowiązek wygaśnie (dane osobowe pracowników należy przechowywać 50 lat licząc od 1 stycznia roku następnego po dacie ich wytworzenia, co wynika z Rozporządzenia MPiPS z 28 maja 1996 r., a dla porównania dane osobowe kandydatów

do pracy przechowuje się w zależności od zamieszczonej klauzuli, tj. zależy od tego czy w klauzuli jest wskazanie o wyrażeniu zgody na przetwarzanie na konkretne stanowisko, czy takie oświadczenie jest złożone ogólnie).

8.2. Proces usuwania danych osobowych

Przez proces usuwania danych osobowych rozumie się zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą. Dane, które powinny podlegać niezwłocznemu usuwaniu to:

- imię i nazwisko (także rodowe),
- dane korespondencyjne,
- numery telefonów, komunikatorów, identyfikacyjne (NIP, PESEL),
- adresy e-mail.

Niektóre z nich samodzielnie nie będą stanowiły danych osobowych, ale mogą ułatwić kontakt z daną osobą, która odwołując zgodę lub wnosząc sprzeciw na przetwarzanie danych po ponownym kontakcie może z tego powodu wnieść skargę do GIODO.

Ustawa o ochronie danych osobowych w art. 32 ust. 3 dopuszcza jednak możliwość zatrzymania w zbiorze imienia, imion i nazwiska oraz numeru PESEL lub adresu wyłącznie w celu uniknięcia ponownego wykorzystania danych owej osoby w celach, które zostały objęte sprzeciwem (praktyczne wydaje się prowadzenie rejestru takich osób). Reasumując ustawodawca nakazał administratorom usuwać dane umożliwiające identyfikację danej osoby.

8.3. Metody usuwania danych osobowych

Dane osobowe zawarte w dokumentach papierowych powinno się niszczyć za pomocą niszczarki dokumentów, która będzie skuteczna, np. nie będzie się zacinać lub pozostawiać niepociętych fragmentów. W przypadku braku niszczarki można zastosować do tej czynności nożyczki z wieloma ostrzami, np. takie jak do warzyw.

Usuwanie danych z systemów informatycznych nie powinno ograniczyć się wyłącznie do usunięcia do kosza i jego opróżnienia (system Windows), gdyż dane te w dalszym ciągu będą mogły być odzyskane. Przykładami programów dostępnych na rynku do skutecznego usuwania danych z systemów informatycznych są Eraser lub FileShredder. Interesująco przedstawia się kwestia usuwania danych w związku z istnieniem kopii zapasowych. Z jednej strony dane podlegające procesowi usuwania powinny być także usunięte z kopii zapasowych, ale z drugiej strony kopie zapasowe służą do odtworzenia systemów informatycznych w przypadku awarii. Usunięcie pewnych danych z kopii zapasowych, czyli ich modyfikacja mogłaby skutkować

zaburzeniem integralności owych kopii przez co mogłyby one stać się bezużyteczne, a w pewnych przypadkach prawo nakazuje je posiadać.

8.4. Anonimizacja danych osobowych

Anonimizacją nazywamy taką modyfikację danych osobowych, która nie pozwoli na identyfikację osoby, której owe dane dotyczą.

Anonimizacja dokumentów papierowych może polegać na zaczernianiu lub wybielaniu danych umożliwiających identyfikację. Szczególnie często można spotkać się z tego typu praktykami w związku z działaniem organów państwa (sądy, urzędy).

W systemach informatycznych proces modyfikacji uniemożliwiający zidentyfikowanie tożsamości konkretnej osoby wydaje się być bardziej złożony. W pewnych przypadkach wystarczy w bazie danych pozmieniać dane każdej z osób tak, aby nie była możliwa ich identyfikacja. Jednak zdarzają się przypadki w tzw. systemach walidowanych, gdzie każdemu polu przypisana jest odpowiednia wartość. Często dokonywana jest anonimizacja zbiorów doraźnych (krótkoterminowych), np. kopia bazy danych do celów testowych.

9. ADMINISTROWANIE DANYMI OSOBOWYMI W LGD

LGD'y działają na podstawie ustawy o rozwoju lokalnym z udziałem lokalnej społeczności, a także w oparciu o Prawo o stowarzyszeniach, związane są z Urzędem Marszałkowskim Województwa Podlaskiego umową o warunkach i sposobie realizacji strategii rozwoju lokalnego kierowanego przez społeczność.

Powyższe ustawy stanowią już źródło informacji o przetwarzanych zbiorach danych osobowych:

1) Członkowie stowarzyszenia
2) Rada LGD
3) Wnioskodawcy

Ponadto LGD'y:

1) zatrudniają pracowników,
2) prowadzą i ewidencjonują doradztwo,
3) zobowiązane są do publikacji listy członków stowarzyszenia na stronie internetowej,
4) publikują na stronie internetowej listy wybranych i niewybranych operacji,
5) prowadzą ewaluację projektów,
6) mogą prowadzić szkolenia / spotkania.

W LGD'ach nie stwierdzono danych wrażliwych, ale mogą się pojawić jeśli np. stowarzyszanie będzie realizowało projekt skierowany do osób niepełnosprawnych i zbierane będą zaświadczenia dotyczące stanu zdrowia.
Poniżej przedstawione zostaną różnorodne zagadnienia dotyczące Lokalnych Grup Działania. W wielu miejscach jest odniesienie do obowiązku informacyjnego oraz zgody na przetwarzanie danych osobowych, które omówione zostały (wraz z przykładami) z rozdziale 5.5.

Członkowie stowarzyszenia

Działalność LGD'ów oparta jest o Prawo o stowarzyszeniach, w związku z powyższym LGD'y mają prawo prowadzenia listy członków stowarzyszenia. Zasady naboru określone są w statucie stowarzyszenia. Istotne jest to, aby od członków stowarzyszenia nie uzyskiwać danych nadmiarowych bowiem może być to uznane za nieadekwatną ilość w stosunku do celu przetwarzania (imię i nazwisko, adres zamieszkania, dane kontaktowe oraz sektor w przypadku osób fizycznych są danymi adekwatnymi do celu przetwarzania). Od członków stowarzyszania nie ma obowiązku odbierania zgody na przetwarzanie danych osobowych, natomiast pozostaje konieczność dopełnienia obowiązku informacyjnego. Warto zauważyć, że LGD'y są zobowiązane (w umowie z UMWP) do publikowania listy członków stowarzyszenia na stronie internetowej, natomiast nie jest to w żaden sposób opisane w postaci przepisu prawa. Wobec tego bez zgody osoby, której dane dotyczą nie można powyższych danych zamieszczać. Aby wywiązać się z umowy z UMWP należy odebrać zgody od członków stowarzyszenia. Zbiór nie podlega rejestracji.

Rada stowarzyszenia

Do rady stowarzyszenia obowiązują zalecenia jak w przypadku członków stowarzyszenia.

Wnioskodawcy

Wnioskodawcy składają w LGD wioski o przyznanie pomocy. LGD'y stają administratorami danych osobowych wnioskodawców na podstawie art. 23 ust. 1 punkt 2 - jest to niezbędne do dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (ustawa o rozwoju lokalnym z udziałem lokalnej społeczności oraz Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1303/2013 z dnia 17 grudnia 2013). W związku z tym LGD'y nie muszą odbierać zgody na przetwarzanie danych osobowych, natomiast muszą dokonać obowiązku informacyjnego. Po dokonaniu wyboru operacji LGD'y dokumentację (wybranych operacji) przekazują UWMP na podstawie art. 23 ust 1 ustawy o rozwoju lokalnym z udziałem lokalnej społeczności.

Zbiór podlega rejestracji jeśli dane są przetwarzane w postaci elektronicznej, np. w arkuszu kalkulacyjnym zawierającym ewidencję złożonych wniosków. Do zbioru wnioskodawców można włączyć zbiór Doradztwo. Na kartach udzielonego doradztwa należy dokonać obowiązku informacyjnego, ale również zamieścić formułę zgody na przetwarzanie danych osobowych bowiem karty doradztwa nie są ujęte w przepisach prawa.

LGD'y zobowiązane są również do publikacji na stronie internetowej listy operacji zgodnych z LSR oraz listę operacji wybranych. W związku z tym, iż pojęcie operacji w Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1303/2013 określone jest bardzo ogólnie, jako „projekt, umowa, przedsięwzięcie lub grupa projektów" sugeruje się umieszczenie na stronie internetowej numeru projektu (znaku sprawy) bez podawania informacji dotyczących danych personalnych wnioskodawcy.

Pracownicy stowarzyszenia

Jest to zbiór przetwarzany zarówno w postaci elektronicznej jak i papierowej. LGD ma prawo przetwarzać dane pracowników w oparciu o Kodeks Pracy (art.23, ust 1, pkt 2 jest to niezbędne do dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa). Zbiór nie podlega rejestracji.

Szkolenia / spotkania

Z reguły spotkania i szkolenia są dokumentowane w postaci list obecności. Należy o tym pamiętać, że i w tym przypadku należy dopełnić obowiązku informacyjnego oraz odebrać zgodę na przetwarzanie danych osobowych przez LGD. Chociaż od odebrania zgody na przetwarzanie danych mogą wystąpić odstępstwa – uczestnik jest np. beneficjentem Projektu X, a LGD ma już zgodę beneficjenta na przetwarzanie danych osobowych w związku z udziałem w Projekcie X. Każdą sytuację należy rozpatrzyć indywidualnie. Zbiór nie podlega rejestracji (chyba, że jest prowadzony elektronicznie).

Poniżej przedstawiamy praktyczny przykład przygotowania listy obecności połączony ze zgodą oraz obowiązkiem informacyjnym.

Lista obecności ze szkolenia…..

Imię i nazwisko	Zgoda na przetwarzanie danych osobowych	Podpis
Jan Kowalski	☐ Wyrażam zgodę na przetwarzanie moich danych osobowych w celu …. przez …	
Anna Nowak	☐ Wyrażam zgodę na przetwarzanie moich danych osobowych w celu …. przez …	
	☐ Wyrażam zgodę na przetwarzanie moich danych osobowych w celu …. przez …	

Administratorem Pani/Pana danych osobowych jest… itd.

Formularze na stronie internetowej

Formularze mogą być wykorzystywane do kontaktowania się LGD jak i do zapisania się do tzw. newsletter'a. W obu przypadkach przesyłanie danych powinno odbyć się protokołem szyfrowanym. I w obu przypadkach należy dopełnić obowiązek informacyjny oraz uzyskać zgodę na przetwarzanie danych osobowych (w przypadku newsletter'a w celu informowania o działalności stowarzyszenia, w przypadku formularza kontaktowego w celu prowadzania korespondencji z LGD). Adresy kontaktowe uzyskane poprzez zapisanie się do newsletter'a tworzą elektroniczny zbiór danych osobowych podlegający rejestracji.

Wizerunek

Niejednokrotnie szkolenia czy też konferencje utrwalane są na zdjęciach. Należy pamiętać o tym, że wizerunek również jest daną osobową i nie można go dowolnie wykorzystywać. Zdjęcie można opublikować gdy osoba ujęta na zdjęciu jest:

- częścią większej całości, jako jedna z wielu osób tworzących jakieś zgromadzenie, a jej usunięcie nie zmieniłoby wymowy obrazu,
- powszechnie znana, a zdjęcie zrobiono w czasie pełnienia przez nią funkcji publicznych, społecznych, zawodowych[29].

Powierzenie danych

[29]Ustawa z dnia 4 lutego 1994r. o prawie autorskim i prawach pokrewnych Dz.U. 1994 nr 24 poz. 83

LGD'y mogą dane, którymi administrują powierzyć innym podmiotom. Do podmiotów tych zaliczyć można:

- podmioty wykonujące świadczenia z zakresu medycyny pracy,
- firmę świadczącą usługi BHP,
- firmę, na której serwerach przetwarzane są dane wnioskodawców,
- firmy audytorskie,
- firmy, którym zlecono badania ewaluacyjne.

W sytuacji powierzenia danych osobowych konieczne jest podpisanie umowy powierzenia danych osobowych.

Ciągłość działania

Warto pamiętać o tym, aby zapewnić pracownikom LGD'ów ciągłość pracy, którą zakłócić mogą np. awarie komputera. W takich sytuacjach oczywiście należy zwrócić się do informatyka współpracującego ze stowarzyszeniem. Niestety jednak czasem zdążyć się może, że osoba odpowiedzialna za kontakt jest nieobecna, a pozostali pracownicy nie są w posiadaniu danych kontaktowych. Aby zapobiec powyższej sytuacji należy numer telefony do informatyka umieścić w znanym wszystkim miejscu.

Bywa również tak, że informatyk znajduje się na urlopie, a awarią ma się zająć inna osoba (firma). Często napotykanym problemem w takich sytuacjach jest nieznajomość loginów i haseł do aplikacji, routera, serwera, a w związku z tym niemożliwe może stać się usunięcie problemu lub bardzo utrudnione (ewentualnie bardzo kosztowne). W celu uniknięcia opisanej sytuacji należy zadbać o to, by hasła i loginy wraz z nazwami systemów znalazły się w zamkniętej kopercie zdeponowanej u ADO.

Zbiory danych w arkuszach kalkulacyjnych

Częstą praktyką jest przetwarzanie danych osobowych z wykorzystaniem arkuszy kalkulacyjnych. Nie są to jednak aplikacje dedykowane do typowej pracy bazodanowej, niemniej wielokrotnie są do tego celu używane (np. spis członków stowarzyszenia). Problemem arkuszy kalkulacyjnych jest fakt, iż nie odnotowują daty pierwszego wprowadzenia danych do systemu oraz identyfikatora osoby, która to uczyniła. Jednak z tym problemem można sobie poradzić dodając dwie kolumny w arkuszu:

- data pierwszego wprowadzenia danych,
- imię i nazwisko osoby, która dane wprowadziła.

10. INSTRUKCJA WDROŻENIA POLITYKI BEZPIECZEŃSTWA

Przed przystąpieniem do wdrożenia polityki bezpieczeństwa należy zapoznać się z polityką ochrony danych osobowych dołączoną do niniejszego opracowania. Może się okazać, że niektóre procedury należy zmodyfikować lub usunąć załączniki np. wykaz osób posiadających klucze do budynku (UWAGA – nie każdy załącznik można usunąć, wykaz niezbędnych elementów polityki znajduje się w rozdziale 5.1). Opracowana polityka stanowi jedynie szablon, który można zmodyfikować i dostosować do wymagań danej organizacji. Należy również pamiętać o tym, że polityka wymaga regularnych analiz oraz aktualizacji.

Krok 1

Należy podjąć decyzję w sprawie powoła ABI. W podjęciu decyzji pomocne będzie zapoznanie z rozdziałem 11 Administrator bezpieczeństwa informacji oraz z rozdziałem 12 Pytania i Odpowiedzi – czy warto powołać ABI. Jeśli odpowiedź będzie twierdząca należy uzupełnić załącznik nr 1 oraz przesłać do GIODO wypełniony wniosek o zarejestrowanie ABI w rejestrze GIODO (zgłoszenie_ABI_GIODO.docx). Zgłoszenia można również dokonać poprzez ePUAP: http://epuap.gov.pl/wps/portal/strefa-klienta/katalog-spraw/opis-uslugi/zgloszenie-powolania-administratora-bezpieczenstwa-informacji-do-rejestracji-generalnemu

UWAGA – zgłoszenia należy dokonać w terminie 30 dni od daty powołania ABI.

Krok 2

Wykaz budynków i pomieszczeń wykorzystywanych do przetwarzania danych osobowych – załącznik nr 2. Na tym etapie wypisujemy wszystkie miejsca przetwarzania danych. Przy okazji należy sprawdzić zabezpieczenia przetwarzanych danych i je również wypisać. Dla miejsc szczególnie wrażliwych (serwerownia, archiwum) – najlepiej wykonać opis zabezpieczeń oddzielnie.

Krok 3

Identyfikacja zbiorów danych stowarzyszenia (załącznik nr 3) – aby chronić dane najpierw należy określić co mamy chronić. Istotną częścią tego etapu jest:

- wytypowanie wszystkich zbiorów danych osobowych,
- zbadanie legalności przetwarzania danych osobowych (art. 23 ustawy o ochronie danych osobowych oraz rozdział 5.4 niniejszego opracowania),
- zbadanie zbiorów pod kątem zakresu gromadzonych danych (czy przypadkiem nie zbieramy danych zbędnych, nadmiarowych)

- dodatkowo należy ocenić czy zbiór podlega rejestracji, jeśli tak – czy rejestracji w zbiorze ABI (jeśli jest powołany) czy w rejestrze GIODO (gdy ABI nie został powołany i gdy zbiór zawiera dane wrażliwe) – rozdział 5.6 niniejszego opracowania.

Na tym etapie warto przejrzeć wszystkie deklaracje, formularze, listy obecności ze szkoleń stosowane przez LGD. Zwrócić należy szczególną uwagę na klauzule zgody (jeśli są wymagane) oraz obowiązek informacyjny i nanieść zmiany jeśli są konieczne.

Krok 4

Struktura zbiorów danych – załącznik nr 4. W załączniku został wykonany przykładowy opis zbiorów danych, który oczywiście należy zweryfikować pod kątem danych przetwarzanych przez LGD. Dodatkowo umieszczony jest plik w katalogu Załącznik nr 4 – StrykturyDanych.pdf – plik ten można nagrać na płycie CD i dołączyć do dokumentacji. Jest to opis struktury danych przetwarzanych w programie Płatnik, który służy do przekazywania informacji do ZUS.

Opisu wymaga każdy zbiór danych. Tak jak wcześniej zostało wspomniane najlepiej:

- zwrócić się do producenta o opis struktury zbiorów danych (warto o tym pamiętać zamawiając oprogramowanie do oceny wniosków - warto zawrzeć ten wymóg w umowie, jako przykład można wskazać sposób opisu programu Płatnik),
- ewentualnie można załączyć do polityki instrukcję obsługi danej aplikacji,
- lub wykonać zrzuty z ekranu przedstawiające formularze do wprowadzania danych,
- ostatecznie można przygotować opis przetwarzanych pól informacyjnych (tak jak w chwili obecnej jest to zrobione w załączniku).

Krok 5

Sposób przepływu danych pomiędzy systemami – załącznik nr 5. Istotą tego etapu jest określenie w jaki sposób pomiędzy jakimi programami przekazywane są dane. Jeśli obsługa kadr i płac nie jest prowadzona przez zewnętrzną firmę to z całą pewnością wykorzystywany jest program Płatnik, a dane do Płatnika są eksportowane z innych programów kadrowo-płacowych – tak więc jest to już jedno miejsce przepływu danych. Ponadto należy rozważyć każdy system wykorzystywany przez LGD i umieścić na schemacie. Na chwilę obecną nie stwierdziliśmy dodatkowego przepływu danych pomiędzy systemami. W momencie wdrożenia elektronicznej oceny wniosków należy załącznik uzupełnić.

Krok 6

Osoby upoważnione do przetwarzania danych osobowych.

Na początek należy sprawdzić i uzupełnić upoważnienie (załącznik nr 6) – należy dodać / lub usunąć systemy informatyczne oraz zbiory danych przetwarzanych w LGD. Zostały przygotowane dwie wersje upoważnienia – wersja I jest bardziej skomplikowana pod kątem rodzaju uprawnień (wprowadzanie, modyfikacja, usuwanie, archiwizacja etc.). Wersja II jest uproszczona i również może być z powodzeniem stosowana w LGD.

Następnie należy zapoznać osoby, które mają uzyskać upoważnienia do przetwarzania danych osobowych z przyjętą polityką oraz przepisami prawa. UWAGA – zapoznani powinni być pracownicy, rada stowarzyszenia, która ocenia wnioski, stażyści etc. Czyli wszystkie osoby mające dostęp do danych osobowych.

Po zapoznaniu z obowiązującymi przepisami należy odebrać oświadczenia o poufności (Załącznik nr 12). Następnie ABI lub ADO nadaje upoważnienie do przetwarzania danych osobowych (załącznik nr 6) i daną osobę wprowadza do ewidencji osób upoważnionych (załącznik nr 7). Ewidencja powinna być aktualizowana za każdym razem gdy dojdzie do zmiany (nowy pracownik, odejście pracownika, zmiana składu rady LGD). Wymagane jest również anulowanie upoważnienia – załącznik nr 13. Warto przy tym pamiętać, że jeśli dane przetwarzany w systemie informatycznym to należy konto takiego użytkownika zawiesić.

Krok 7

Rejestr zbiorów ABI lub rejestracja w rejestrze GIODO.

Bazując na uzupełnionym załączniku nr 3 - wykaz zbiorów danych, można przejść do rejestru zbiorów danych. Jeśli powołany był ABI wówczas wystarczy jawny rejestr ABI – załącznik nr 10 (chyba, że chodzi o zbiory danych wrażliwych, które należy zarejestrować w rejestrze GIODO, a przetwarzanie w zbiorze można rozpocząć dopiero po uzyskaniu potwierdzenia zarejestrowania zbioru). Jeśli ABI nie został powołany, ADO ma obowiązek zarejestrować zbiór w rejestrze GIODO. W tym celu należy dokonać rejestracji na stronie https://egiodo.giodo.gov.pl/formular_step0.dhtml, jeśli LGD dysponuje podpisem cyfrowym to należy wniosek podpisać cyfrowo, a jeśli nie ma podpisu cyfrowego wniosek należy wydrukować, podpisać i przesłać do GIODO.

Krok 8

Powierzenie danych – rozdział 6 niniejszego opracowania. Na tym etapie należy przyjrzeć się wszystkim usługom zewnętrznym i zbadać czy też nie zachodzi konieczność podpisania umowy

powierzenia danych osobowych (załącznik 17). Istotne w umowie powierzenia jest określenie celu powierzenia danych oraz zakresu powierzenia danych. Może się również okazać, że podpisane przez LGD umowy już zawierają klauzulę powierzenia danych, wówczas nie ma konieczności załączenia dodatkowego dokumentu. ABI lub ADO powinien uzupełnić również załącznik nr 18 zawierający ewidencję powierzeń danych osobowych.

Krok 9

Jeśli istnieje taka potrzeba można przygotować dodatkowe załączniki. Do polityki bezpieczeństwa jest dołączony załącznik nr 16 - ewidencja osób upoważnionych do posiadania kluczy do budynku. Nie jest to niezbędny element polityki, jednak może zwiększyć kontrolę nad kluczami będącymi w posiadaniu pracowników LGD.

Krok 10

Sprawdzenia zgodności przetwarzania danych z obowiązującymi przepisami. Jest to ustawowym obowiązkiem ABI. Najpierw należy przygotować plan sprawdzeń na okres nie krótszy niż kwartał, nie dłuższy niż rok. Plan sprawdzeń (załącznik nr 8) powinien być przedłożony ADO przynajmniej na 2 tygodnie przed okresem objętym sprawdzeniem i zawierać minimum jedno sprawdzenie. Następnie w okresie 30 dni od sprawdzenia ABI powinien złożyć pisemne sprawozdanie z przeprowadzonej kontroli (załącznik nr 9).

Czynności wykonywane regularnie

- Nowy pracownik, stażysta, członek rady – należy przeszkolić z ochrony danych osobowych, odebrać podpisane oświadczenie o poufności i nadać upoważnienie do przetwarzania danych osobowych oraz zaktualizować ewidencję osób upoważnionych. Działania powyższe powinny nastąpić niezwłocznie po wystąpieniu powyżej sytuacji.
- Odejście pracownika, stażysty, członka rady – należy anulować upoważnienie do przetwarzania danych osobowych oraz zaktualizować ewidencję osób upoważnionych.
- Podpisanie dowolnej umowy – powinno być zawsze przeanalizowane pod kątem ochrony danych osobowych ze szczególnym uwzględnieniem dostępu do danych osobowych przez zleceniobiorcę. Jeśli powyższe przesłanki zostaną spełnione należy zawrzeć powierzenie danych w umowie głównej lub podpisać umowę dodatkową.
- Zmiany w rejestrze zbiorów danych osobowych (prowadzonym przez ABI lub GIODO) – należy na bieżąco analizować, czy nie powstał nowy zbiór, lub czy też nie zaszły zmiany w zbiorze już zarejestrowanym (np. poprzez zmianę podmiotu, któremu powierzono dane).

- Zakup / zmiana oprogramowania – jeśli oprogramowanie służy do przetwarzania danych osobowych należy je zaktualizować schemat przepływu danych pomiędzy systemami informatycznymi, oraz nanieść zmiany w strukturze zbiorów danych (o ile jest to konieczne). Warto w tym miejscu raz jeszcze przypomnieć, iż najłatwiej od producenta oprogramowania uzyskać strukturę zbiorów danych jeszcze przed zawarciem umowy kupna.
- Przygotowywanie list obecności / formularzy zgłoszeniowych etc. – przy każdym wspomnianym działaniu należy określić podstawę legalności (Art. 23 ust. 1 ustawy o ochronie danych osobowych), a także cel przetwarzania danych osobowych oraz właściwie napisać obowiązek informacyjny.

11. ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

Administrator bezpieczeństwa informacji jest osobą, którą ADO może powołać do przejęcia obowiązków w zakresie ochrony danych osobowych. Warto, przy tym zauważyć, że nie zwalnia to ADO z odpowiedzialności.

Do głównych zadań ABI, przewidzianych ustawą, należy:

1) zapewnianie przestrzegania przepisów o ochronie danych osobowych:
   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 polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym
   c) kontrola przestrzegania zasad określonych w opracowanej dokumentacji,
   d) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych (np. poprzez szkolenia);
2) prowadzenie (wewnętrznego) rejestru zbiorów danych przetwarzanych przez ADO,
3) na wniosek GIODO - przeprowadzanie sprawdzeń zgodności przetwarzania danych osobowych.

Jeśli ADO nie zdecyduje się na powołanie ABI to do jego obowiązków należeć będą:

   a) opracowanie i aktualizowanie polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym,
   b) zapewnienie przestrzegania zasad określonych w opracowanej dokumentacji,
   c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych (np. poprzez szkolenia),

d) zgłaszanie zbiorów do rejestru GIODO.

Wymagania wobec ABI

1) Musi posiadać pełną zdolność do czynności prawnych oraz korzystać z pełni praw publicznych;
2) Musi posiadać odpowiednią wiedzę w zakresie ochrony danych osobowych;
3) Nie może być karany za umyślne przestępstwo.

	Powołany ABI	**Niepowołany ABI**
Opracowanie i aktualizacja dokumentacji ochrony danych osobowych	Wykonuje ABI	Wykonuje ADO
Kontrola przestrzegania zasad określonych w opracowanej dokumentacji	Wykonuje ABI	Wykonuje ADO
Sprawdzanie zgodności przetwarzania danych osobowych z przepisami oraz opracowanie sprawozdania	Obowiązek ABI	ADO jest zwolniony z tego obowiązku
Zapewnianie zapoznania osób upoważnionych z przepisami)	Wykonuje ABI	Wykonuje ADO
Rejestrowanie zbiorów	ABI prowadzi wewnętrzny rejestr zbiorów wymagających rejestracji	ADO zgłasza zbiory do rejestracji w rejestrze GIODO
Kontrole na wniosek GIODO	ABI	nie dotyczy

12. PYTANIA I ODPOWIEDZI

Czy w Lokalnych Grupach Działania korzystne jest powołanie Administratora Bezpieczeństwa Informacji?

Ze względu na specyfikę działania Lokalnych Grup Działania wydaje się zasadnym powołanie ABI. Przemawia za tym, w pierwszej kolejności, fakt, iż bardzo często zdarza się, że osoba zarządzająca LGD (np. prezes) nie jest etatowym pracownikiem, a obowiązki spoczywające na administratorze danych osobowych mogą znacznie obciążyć tę osobę. Może to negatywnie wpływać na jakość wypełniania obowiązków, a przez może to rodzić ujemne konsekwencje prawne – także na gruncie prawa karnego. W związku z tym istnieją 2 możliwości:

- powołanie ABI spośród pracowników LGD, co może wydawać się analogicznie niekorzystne z perspektywy wdrażania prowadzonych kontroli przez „kolegę z pracy", czy też „podwładnego", a po drugie kadry LGD nie są na tyle liczne, a zasoby finansowe tak znaczne, aby tworzyć odrębny etat dla ABI,
- powołanie ABI spoza pracowników i członków LGD, co stworzy strukturę partnerską i biznesową, a klauzule zawarte w umowie mogą wpłynąć na jakość wypełniania obowiązków oraz rozłożenie odpowiedzialność za ewentualne wady.

Czy w ramach funkcjonowania Lokalnych Grup Działania dopuszczalne i uzasadnione jest wykonywanie, przechowywanie kserokopii dowodu osobistego członków LGD lub innych osób?

Tak, jeśli jest to uzasadnione przepisami prawa lub przesłankami legalności przetwarzania danych osobowych. W opinii GIODO w analogicznej sprawie czytamy: „Z punktu widzenia ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, każdy administrator danych (m.in. bank), aby móc legalnie przetwarzać dane osobowe, w tym je pozyskiwać, musi wykazać się uprawniającą go do tego podstawą. W przypadku danych osobowych tzw. zwykłych, jak np. imię i nazwisko, adres zamieszkania czy numer PESEL, musi spełnić przynajmniej jedną z pięciu, enumeratywnie wymienionych w art. 23 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przesłanek. Jedną z nich jest istnienie szczególnego przepisu prawa, który uprawnia do wykorzystywania danych osobowych.

W przypadku banków przepisem uprawniającym je do pozyskiwania od klientów danych osobowych zawartych w dowodzie osobistym jest art. 112 b ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe, zgodnie z którym, banki mogą przetwarzać dla celów prowadzonej działalności bankowej informacje zawarte w dokumentach tożsamości osób fizycznych. Przepis ten legalizuje zatem pozyskiwanie przez banki danych osobowych zawartych w dowodach osobistych klientów.

Samo kserowanie dowodów jest zaś, w opinii Generalnego Inspektora Ochrony Danych Osobowych, czynnością stricte techniczną. Taki pogląd wyrażony został również w wyroku Naczelnego Sądu Administracyjnego z 19 grudnia 2001 r. (sygn. akt II SA 2869/2000), zgodnie z którym gromadzenie danych poprzez wykonanie kopii dokumentu zawierającego dane osobowe jest kwestią techniczną; posługiwanie się taką, czy inną techniką utrwalania tych

danych (kopiowanie lub przepisywanie) nie przesądza samo przez się o legalności albo nielegalności tego utrwalania (przetwarzania)”[30].

Czy pracownik administracyjny lub stażysta w LGD organizujący szkolenia, nabory wniosków etc. musi mieć upoważnienie do przetwarzania danych osobowych?
Tak. Upoważnienie do przetwarzania danych osobowych muszą mieć wszyscy pracownicy mający dostęp do danych. Warto podkreślić, że oprócz pracowników takie upoważnienia powinni posiadać członkowie ciał kolegialnych LGD[31].

Inne pytania być może napłyną od LGD….

13. KONSEKWENCJE DZIAŁAŃ NIEZGODNYCH Z PRAWEM

W celu ustalenia ewentualnej odpowiedzialności za niezgodność działań (lub ich braku) z przepisami dotyczącymi ochrony danych osobowych należy ustalić kto (podmiot) i w jakim zakresie doszło do naruszeń.

13.1. Podmioty mogące ponosić odpowiedzialność

ADO

W pierwszej kolejności należy wskazać **administratora danych osobowych (ADO)**, który jest odpowiedzialny za całokształt obowiązków wynikających z ustawy o ochronie danych osobowych oraz aktów wykonawczych. ADO odpowiada za prawidłowe funkcjonowanie procesów, wdrożeń oraz pełni nadzór nad danymi osobowymi. Można stwierdzić, iż ADO ponosi pełną odpowiedzialność i jest głównym podmiotem, na którego wskazuje ustawa w przypadku ustalania odpowiedzialności. Pomimo delegowania niektórych zadań odpowiedzialność ADO będzie nadal miała charakter pełny, a jego odpowiedzialność rozciąga się na działania innych podmiotów, które wykonują określone zadania na podstawie umowy powierzenia.

ABI

Nie pojawiły się natomiast żadne przepisy karne dotyczące odpowiedzialności Administratora Bezpieczeństwa Informacji (ABI), który zawsze odpowiada przed ADO. Jego odpowiedzialność

[30] http://www.giodo.gov.pl/332/id_art/2839/j/pl/.
[31] Por. M. Jendra (red.), Ochrona *danych medycznych w 2015 r. Prawo, praktyka, wzory dokumentów według najnowszych przepisów*, Warszawa 2015, s. 76.

może mieć charakter pracowniczy, gdy jest zatrudniony na umowę o pracę (sankcje z Kodeksu Pracy), a gdy obowiązki ABI wynikają z innej podstawy (umowa zlecenia, zlecenie zadań innej firmie), to jego odpowiedzialność będzie na podstawie ww. umów oraz Kodeksu Cywilnego. Jedyną sankcją przewidzianą w ustawie wobec ABI jest wykreślenie go z rejestru przez GIODO w przypadku niedopełnienia obowiązków, co utrudni ponowny wpis w przyszłości.

Zleceniobiorca

Art. 31 ust. 3 ustawy o ochronie danych osobowych ustanawia odpowiedzialność podmiotu (zleceniobiorcy, procesora) taką jak ponosi ADO, któremu dane osobowe zostały powierzone, za których zabezpieczenie jest odpowiedzialny (artykuły 36-39a ustawy o ochronie danych osobowych). Pomimo tych zapisów odpowiedzialność w pierwszej kolejności ponosi ADO, a dopiero potem procesor (art. 31 ust. 4).

Osoby upoważnione do przetwarzania danych

W praktyce zdarzają się sytuacje, w których pracodawca upoważnia pracownika do przetwarzania danych osobowych, które powinien chronić. Jego odpowiedzialność będzie w głównej mierze przed pracodawcą (ADO), ale ustawa o ochronie danych osobowych dopuszcza możliwość pociągnięcia go do odpowiedzialności karnej (art. 51 ustawy o ochronie danych osobowych). Jeśli inspektor GIODO podczas kontroli uzna, iż dany pracownik winien jest określonym uchybieniom, to może zobowiązać pracodawcę do wszczęcie postępowania dyscyplinarnego (art. 17 ust. 2).

13.2. Rodzaje postępowań

Przepisy administracyjne

Art. 22 ustawy o ochronie danych osobowych stanowi, iż postępowanie w sprawach uregulowanych w owej ustawie prowadzi się w oparciu o przepisy Kodeksu Postępowania Administracyjnego o ile przepisy ustawy nie stanowią inaczej (np. zastosowanie przepisów karnych). GIODO zatem w przypadku naruszenia ww. przepisów wszczyna postepowanie administracyjne, którego celem jest przywrócenie stanu zgodnego z prawem, a w szczególności przesłankami wszczęcia będzie:

- brak pisemnej umowy powierzenia,
- brak prowadzonych ewidencji osób upoważnionych,
- brak dokumentacji, np. polityki bezpieczeństwa,
- brak zmian haseł częściej niż 30 dni,

- brak możliwości systemu do przygotowania raportu z danymi osobowymi lub raport nie będzie kompletny.

Przepisy egzekucyjne

Jeżeli GIODO podczas kontroli nakaże usunąć braki, a pomimo to przewidziany ustawą stan prawny nie zostanie przywrócony, to GIODO może podjąć działania egzekucyjne. W pierwszej kolejności będzie to upomnienie, później może zostać wystawiony tytuł wykonawczy oraz skierowany wniosek do organu egzekucyjnego o wszczęcie tegoż postępowania. Przy tej okazji należy rozróżnić postępowanie egzekucyjne o charakterze niepieniężnym (GIODO jest wierzycielem i organem egzekucyjnym) oraz pieniężnym (GIODO – wierzyciel, organ egzekucyjny – naczelnik urzędu skarbowego. Wyróżnia się następujące środki egzekucyjne: grzywna, wykonanie zastępcze oraz przymus bezpośredni.

Przepisy karne

O doniosłości materii związanej z ochroną danych osobowych świadczy fakt, iż cały rozdział 8 owej ustawy nosi tytuł: „Przepisy karne". Wszelkie przestępstwa związane z ochroną danych stanowią przestępstwa umyślne z wyjątkiem tych opisanych w art. 51 i 52, w których występek można popełnić także nieumyślnie. Ściganie ww. przestępstw następuje z urzędu, co oznacza, iż zawiadomienie organów ścigania o możliwości popełnienia przestępstwa na danych osobowych oznacza podjęcie przez nie czynności zgodnie z procedurami, np. zgłoszenie, iż wyrzucono dokumenty zawierające dane osobowe na śmietnik może uzasadniać takie zgłoszenie. Oto przepisy o odpowiedzialności karnej z ustawy o ochronie danych osobowych:

Art. 49 [Przetwarzanie danych przez nieuprawnionego]

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. 51 [Udostępnianie danych osobom nieuprawnionym]

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 [Naruszenie obowiązku zabezpieczenia danych] *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 [Niezgłoszenie danych do rejestru] *Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności* ***do roku****.*

Art. 54 [Niedopełnienie obowiązku poinformowania] *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 [Udaremnianie wykonania czynności kontrolnej] *Kto inspektorowi udaremnia lub utrudnia wykonanie*

czynności kontrolnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności ***do lat 2****."*

Postępowanie cywilne

Ten typ postępowania może być wszczęty niezależnie od pozostałych (administracyjne, karne), gdyż naruszenie uprawnień danej osoby w związku z ochroną danych osobowych może być podstawą do dochodzenia roszczeń na podstawie przepisów Kodeksu Cywilnego w kwestii dóbr osobistych, tj.:

„Art. 23. *Dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach.*

Art. 24. *§ 1. Ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny.*

§ 2. Jeżeli wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych.

§ 3. Przepisy powyższe nie uchybiają uprawnieniom przewidzianym w innych przepisach, w szczególności w prawie autorskim oraz w prawie wynalazczym"[32].

Warto nadmienić, iż oprócz ww. wskazanych roszczeń istnieje możliwość roszczeń na podstawie art. 415 Kodeksu Cywilnego, co może nastąpić w sytuacji, gdy, np. ujawnienie danych przyczyniło się do powstania szkody z winy sprawcy poprzez na przykład brak zabezpieczeń.

ZAPAMIĘTAJ!

Powoływanie się na nieznajomość przepisów lub nieświadomość ich istnienia nie wyłącza Twojej odpowiedzialności!

[32] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny, Dz. U. z 2016 r. poz. 380, 585.

14. BIBLIOGRAFIA

Akty prawne:

Ustawa z dnia 29 sierpnia 1997 r.o ochronie danych osobowych, Dz. U. 2016 r. poz. 922.

Ustawa z dnia 16 września 1982 r. prawo spółdzielcze, Dz. U. 2016 r. poz. 1250.

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, Dz. U. z 2016 r. poz. 1333.

Ustawa z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych, Dz. U. z 2013 r. poz. 1650.

Ustawa z dnia 4 lutego 1994r. o prawie autorskim i prawach pokrewnych Dz.U. 1994 nr 24 poz. 83.

Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny, Dz. U. z 2016 r. poz. 380, 585.

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 r. poz. 1024.

Rozporządzenie Ministra Administracji i Cyfryzacji z 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych, Dz. U. z 2015, poz. 719.

Orzecznictwo:

Wyrok SA w Warszawie z 10.02.2005 r., I ACa 509/04, LEX nr 535042.

Wyrok WSA w Warszawie z 27.2.2004 r., II SA 291/03, Legalis.

Monografie:

Kępa L., *Ochrona danych osobowych w praktyce*, Warszawa 2015.

Jendra M. (red.), Ochrona *danych medycznych w 2015 r. Prawo, praktyka, wzory dokumentów według najnowszych przepisów*, Warszawa 2015.

Barta J., Fajgielski P., Markiewicz R*., Ochrona danych osobowych. Komentarz,* Warszawa 2015.

P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2016.

Czasopisma:

Kaczmarek A. [w:]*ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych*, Wydawnictwo Sejmowe, Wydanie 1,Warszawa 2007r.

Szewc A., *Z problematyki ochrony danych osobowych*, cz. III, R. Pr. 1999, Nr 5.

Publikacje w Internecie (dostęp na dzień 15.09.2016 r.):

http://www.giodo.gov.pl/.

http://www.giodo.gov.pl/317/id_art/973/j/pl.

http://www.giodo.gov.pl/353/id_art/994/j/pl.

http://www.giodo.gov.pl/319/id_art/3512/j/pl.

http://www.giodo.gov.pl/317/id_art/2912/j/pl.

http://www.giodo.gov.pl/306/id_art/2329/j/pl.

http://www.giodo.gov.pl/319/id_art/2258/j/pl.

http://www.giodo.gov.pl/348/id_art/4859/j/pl/.

http://www.giodo.gov.pl/332/id_art/2839/j/pl/.