2015

Ochrona danych osobowych w przedsiębiorstwie – poradnik dla MŚP

enterprise europe network

Wsparcie dla biznesu w zasięgu ręki

PARP

Komisja Europejska

Ochrona danych osobowych w przedsiębiorstwie

– poradnik dla MŚP

Warszawa 2015

Ochrona danych osobowych w przedsiębiorstwie – poradnik dla MŚP

Autorzy:
dr Łukasz Kister – rozdziały: 1, 4, 5 i 6
mgr Bartosz Mendyk – rozdziały: 2, 3, 7 i 8

Recenzenci:
prof. dr hab. Leszek F. Korzeniowski i dr Paweł Litwiński

Niniejsza publikacja została współfinansowana przez Komisję Europejską ze środków pochodzących z programu COSME na lata 2014-2020 oraz ze środków budżetu państwa w ramach programu pn. „Udział Polski w programie na rzecz konkurencyjności przedsiębiorstw oraz małych i średnich przedsiębiorstw (COSME) oraz w instrumentach finansowych programów UE wspierających konkurencyjność przedsiębiorstw w latach 2015-2021".

Publikacja jest dostępna w formie e-booka na stronach internetowych:
www.parp.gov.pl oraz www.een.org.pl

ISBN 978-83-7633-369-4

Wydawca:
Polska Agencja Rozwoju Przedsiębiorczości ul. Pańska 81/83
00-834 Warszawa
www.parp.gov.pl

Wydanie I

Liczba arkuszy: 6

Nakład: 1 000 egzemplarzy

Przygotowanie do druku, druk i oprawa:
Agencja Reklamowo-Wydawnicza A. Grzegorczyk

Spis treści

1. SYSTEM OCHRONY DANYCH OSOBOWYCH W POLSCE

dr Łukasz Kister

Zrozumienie zasad ochrony danych osobowych wymaga poznania ich źródeł. Powinni to zrobić zwłaszcza ci, którzy są zobowiązani do praktycznego stosowania wspomnianych zasad. Czasy, w których prywatność jednostki określały i zabezpieczały pozaprawne normy zwyczajowe, kulturowe czy religijne kształtujące ludzkie postępowanie, już nigdy nie powrócą. Zmieniające się otoczenie, kształtowane szczególnie przez nienotowany dotąd **rozwój technologii informacyjnych**, powoduje, że jedynym sposobem na zapewnienie ochrony dóbr osobistych jest prawna regulacja tego obszaru[1].

Mając na uwadze fakt czynnego udziału naszego państwa w procesach integracji europejskiej, zobowiązani jesteśmy nie tylko do znajomości prawa krajowego, ale również tego, które je kształtuje. Pamiętajmy, że **prawo międzynarodowe** stoi ponad prawem krajowym, będąc dla tego ostatniego pewnym generalnym odniesieniem. Jest to szczególnie istotne dla przedsiębiorców, którzy, korzystając z zasad europejskiej swobody działalności gospodarczej, chcą realizować swoje międzynarodowe aspiracje biznesowe.

Rozdział ten nie może być zatem traktowany wyłącznie jako wykaz aktów prawa europejskiego i krajowego, które bezpośrednio określają zasady ochrony danych osobowych, ale przede wszystkim jako niezbędne wprowadzenie do zrozumienia systemu, które one współtworzą. Najczęstsze błędy w praktycznej realizacji ustawowego wymogu ochrony danych osobowych wynikają właśnie z nieznajomości istoty tych regulacji. Nie jest bowiem możliwe właściwe wykonanie dyspozycji przepisu – szczególnie wtedy, kiedy dotyczy on wartości niematerialnej – jeżeli nie jest znany i rozumiany cel jego wprowadzenia oraz ewolucja celu, któremu ma służyć. Należy też pamiętać, że ciągłej zmianie ulegają determinanty systemu ochrony danych. Chodzi o postrzeganie podstawowych terminów (np. prywatność, intymność czy wolność informacyjna), nowe wyzwania globalnej teleinformatyzacji (np. chmura obliczeniowa, czyli *cloud computing*, big data[2]) i wiele innych.

1.1. OCHRONA DANYCH OSOBOWYCH W EUROPIE

Problematyka **danych osobowych** jako przedmiotu prawnej regulacji pojawiła się na przełomie sześćdziesiątych i siedemdziesiątych lat ubiegłego wieku. Była to odpowiedź na upowszechnianie się wykorzystywania technologii komputerowych służących do zbierania, przetwarzania i transmisji różnych zasobów informacyjnych, w tym tych, które obejmują dane osobowe.

Choć inicjatywy w tym względzie miały bardzo różne podłoża, to jednak można je wszystkie sprawdzić do kilku najważniejszych determinantów:

- automatyzacja gromadzenia i przetwarzania niespotykanych dotychczas ilości informacji;
- nieograniczone wzmocnienie pozycji instytucji publicznych i organizacji prywatnych dysponujących rozbudowanymi bankami danych osobowych;
- utrata możliwości jakiejkolwiek kontroli nad gromadzeniem i przetwarzaniem informacji przez osobę, której to dotyczy[3].

Istniejące w tamtym okresie cywilnoprawne instrumenty ochrony dóbr osobistych okazywały się rażąco nieskuteczne, gdyż miały zastosowanie dopiero w sytuacji naruszenia tych dóbr lub co najmniej wystąpienia bezpośredniego zagrożenia naruszeniem – działanie *„post factum"*[4]. Taki system nie gwarantował jednostce podstawowego poczucia ochrony przed bezprawnymi działaniami godzącymi w jej prywatność.

1.1.1. EUROPEJSKA KONWENCJA PRAW CZŁOWIEKA

Pierwszym europejskim dokumentem poruszającym problematykę **prywatności**, rozumianej jako dobro bezwzględnie chronione przez prawo, jest przyjęta 4 listopada 1950 r. **Konwencja o ochronie praw człowieka i podstawowych wolności**[5].

---

[1] Patrz: A. Kopff: *Koncepcja praw do intymności i do prywatności życia osobistego*, „Studia Cywilistyczne", t. XX, 1972, s. 14.

[2] Niestety nie można tutaj zaproponować jakiegokolwiek polskiego odpowiednika (tłumaczenia) tego terminu, w szczególności, takiego, który odzwierciedlałby poprawnie jego istotę. Szerzej w: V. Mayer-Schonberger, K. Cukier: *Big Data. Rewolucja, która zmieni nasze myślenie, pracę i życie*, Warszawa: MT Biznes, 2014.

[3] A. Lewiński: Prawna ochrona danych osobowych w Polsce na tle europejskich standardów. 10-lecie polskiej Ustawy o ochronie danych osobowych, (w:) G. Goździewicz, M. Szabłowska (red.): Prawna ochrona danych osobowych w Polsce na tle europejskich standardów, Toruń: Wydawnictwo „Dom Organizatora", 2008, s. 9.

[4] A. Mednis: Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej, „Ochrona Danych Osobowych", nr 1, 2000, s. 9.

[5] (Dz.U. z 1993 r., nr 60, poz. 284, z późn. zm.).

Zgodnie z jej dyspozycją prawo do poszanowania swojego życia prywatnego i rodzinnego, mieszkania oraz tajemnicy korespondencji (art. 8 ust. 1) jest **zagwarantowane każdemu** bez względu na płeć, rasę, kolor skóry, język, religię, przekonania polityczne, pochodzenie narodowe lub społeczne, majątek, urodzenie lub z jakichkolwiek innych przyczyn (art. 14). **Ograniczenie** tego prawa jest dopuszczalne tylko wówczas, gdy:

1) wprowadzone zostanie aktem prawnym rangi ustawowej,
2) będzie stanowić środek niezbędny w społeczeństwie demokratycznym do zapewnienia:
   a) bezpieczeństwa narodowego,
   b) porządku i spokoju publicznego,
   c) gospodarczego dobrobytu kraju,
   d) obrony ładu i przeciwdziałania czynom karalnym,
   e) ochrony zdrowia i moralności,
   f) ochrony praw i wolności (art. 8 ust. 2).

Regulacja taka – choć nie odnosi się wprost do pojęcia danych osobowych – **wymusza pewne określone obowiązki** związane ze zbieraniem, a następnie dalszym przetwarzaniem danych osobowych. Wspomnianymi obowiązkami jest zatem podstawa formalna (ustawa) oraz faktyczna (wypełnienie wskazanego enumeratywnie celu)[6]. W szczególności dotyczyć to będzie takich danych osobowych, które swą zawartością treściową obejmują informacje o życiu prywatnym i rodzinnym[7].

1.1.2. KONWENCJA RADY EUROPY

Najszybciej na zagrożenia wynikające z nagłego i pozbawionego jakiejkolwiek regulacji rozwoju komputerowych banków danych zareagowała Rada Europy[8].

Zwieńczeniem jej prac nad wyzwaniem związanym z ochroną danych osobowych było przyjęcie 28 stycznia 1981 r. **Konwencji nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych**[9].

Dokument ten odegrał kluczową rolę w kreowaniu zasad ochrony danych osobowych w całej Europie, zarówno w odniesieniu do regulacji krajowych, jak również do międzynarodowych. Konwencja nie ma jednak charakteru samowykonalnego. Jej adresatem jest państwo[10], na które został nałożony konkretny obowiązek legislacyjny, tj. dostosowania krajowego systemu prawnego do **wspólnych minimalnych standardów** ochrony danych osobowych[11], pozostawiając **dane osobowe** jako szeroką swobodę w kształtowaniu poszczególnych środków bezpieczeństwa.

Konwencja zdefiniowała termin „*wszelkie informacje dotyczące osoby fizycznej o ustalonej tożsamości albo dającej się zidentyfikować*" (art. 2 lit. a)[12]. Jednocześnie z powyższego zbioru została wyodrębniona kategoria tzw. **danych wrażliwych**, do których zostały zaliczone informacje ujawniające pochodzenie rasowe, poglądy polityczne, przekonania religijne, stan zdrowia, szczegóły życia seksualnego oraz wyroki karne (art. 6).

Ponadto na wspomniane wcześniej **wspólne minimalne standardy** ochrony danych osobowych, składają się poniższe zasady.

1) Zasada jakości danych (art. 5), która wymusza, by dane osobowe były:
   a) zbierane i przetwarzane rzetelnie i zgodnie z prawem;
   b) rejestrowane dla określonych i prawnie uzasadnionych celów oraz niewykorzystywane w sposób niezgodny z tymi celami;
   c) stosowne, rzeczowe oraz niewykraczające poza potrzeby wynikające z celów, dla których zostały zarejestrowane;
   d) dokładne i, w razie potrzeby, aktualizowane;
   e) przechowywane w sposób pozwalający na identyfikację podmiotów danych, przez okres nie dłuższy niż ten, który jest niezbędny dla realizacji celów, dla których zostały zarejestrowane[13].

---

[6] J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych. Komentarz*, 5. wydanie, Warszawa: Wolters Kluwer Polska, 2011, s. 37-38.

[7] Orzecznictwo Europejskiego Trybunału Praw Człowieka w Strasburgu, jednoznacznie odrzuca spotykane w piśmiennictwie opinie, że art. 8 Konwencji nie obejmuje problematyki ochrony danych osobowych, a wręcz przeciwnie przyjmuje rozszerzającą definicję „życia prywatnego i rodzinnego", w której mieszczą się wszelkie dane osobowe. Patrz: J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 38-45; A. Posiadła, S. Winiecka: *Ochrona danych osobowych w świetle wybranych orzeczeń Europejskiego Trybunału Praw Człowieka*, (w:) G. Goździewicz, M. Szabłowska (red.): *Prawna ochrona danych osobowych* …, s. 197-208.

[8] Ważne jest by nie mylić „Rady Europy" z „Radą Unii Europejskiej", które są dwoma odmiennymi instytucjami europejskiego systemu współpracy międzynarodowej.

[9] (Dz.U. z 2003r., nr 3, poz. 25).

[10] Polska podpisała Konwencję – 21 kwietnia 1999 roku, ratyfikowała – 24 maja 2002 roku, a weszła ona w życie – 1 września 2002 roku.

[11] K. Czarnecki: ochrona danych osobowych w systemie Rady Europy na przykładzie Konwencji nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, (w:) G. Goździewicz, M. Szabłowska (red.): Prawna ochrona danych osobowych …, s. 190.

[12] Konwencja nie obejmuje swą ochroną danych o „osobach prawnych", ale daje możliwość państwom przystępującym do niej rozszerzenia jej także na informacje o grupach osób, związkach, fundacjach, stowarzyszeniach, korporacjach i innych podmiotach, które bezpośrednio lub pośrednio składają się z osób fizycznych. Patrz: J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 47.

[13] W piśmiennictwie nazywane są one także „zasadami ogólnymi dopuszczalności przetwarzania danych osobowych". Patrz: P. Fajgielski: *Zasady ogólne przetwarzania i ochrony danych osobowych*, (w:) G. Goździewicz, M. Szabłowska (red.): *Prawna ochrona danych osobowych* …, s. 17 i nast..

2) Zasada bezpieczeństwa danych (art. 7), która nakazuje zastosowanie odpowiednich środków, w celu ochrony danych osobowych przed:
   a) zniszczeniem (przypadkowym lub dokonanym bez zezwolenia);
   b) przypadkową utratą;
   c) nieautoryzowaną zmianą;
   d) udostępnieniem lub rozpowszechnieniem bez zezwolenia.
3) Zasada informowania o przetwarzaniu (art. 8), która upoważnia podmiot danych do:
   a) uzyskania informacji o istnieniu zbioru danych osobowych, o jego zasadniczych celach oraz o jego administratorze[14],
   b) uzyskania sprostowania lub usunięcia danych, jeśli zostały przetworzone z naruszeniem przepisów prawa.
   c) Zasada swobodnego przepływu danych (art. 12), która zobowiązuje wszystkie Strony Konwencji do zniesienia ograniczeń w transferze danych osobowych w sytuacji zapewnienia równoważnych standardów ochrony.
   d) Zasada odpowiedzialności karnej (art. 10), która zobowiązuje państwa do ustalenia odpowiednich sankcji karnych i odszkodowawczych za naruszenie zasad ochrony danych osobowych.

Największe wątpliwości w obszarze powszechności i kompleksowości ochrony danych osobowych budzi **zakres stosowania Konwencji**, gdyż w swoich dyspozycjach odnosi się ona **wyłącznie do danych przetwarzanych automatycznie**[15]. Oznaczałoby to wyłączenie z jurysdykcji tych danych, które są przetwarzane w ewidencjach tradycyjnych (papierowych). I chociaż celem Konwencji była odpowiedź na rosnące zagrożenia związane z funkcjonowaniem informatycznych banków danych, to jednak dano państwom możliwość rozszerzenia jej stosowania także na zbiory nieobjęte automatyzacją przetwarzania[16].

Ponadto system wymagań Konwencji uzupełniają **Rekomendacje Rady Europy**, czyli wyspecjalizowane wytyczne dla najważniejszych obszarów problemowych ochrony danych osobowych, tj.: medycyna[17], opieka społeczna, ubezpieczenia, zatrudnianie pracowników, policja i wymiar sprawiedliwości, marketing, badania naukowe, bankowość czy telekomunikacja[18].

Nie są to bezwzględne wymagania, a raczej zbiór dobrych praktyk i wskazówek jak radzić sobie z przetwarzaniem danych osobowych. Niemniej jednak bardzo wiele z nich stanowi podstawę dla decyzji wydawanych przez krajowe organy nadzoru, a tym samym wspomniane praktyki i wskazówki stają się powszechnymi wytycznymi dla określanych przez nie obszarów działalności.

1.1.3. DYREKTYWA UNII EUROPEJSKIEJ

Początkowo Wspólnoty Europejskie[19] nie podejmowały prac nad odrębnym uregulowaniem prawnym problematyki ochrony danych osobowych, postulując raczej, żeby państwa członkowskie ratyfikowały w całości Konwencję nr 108 Rady Europy[20].

Niestety, ustawodawstwa wewnętrzne, które powstały pod jej wpływem, okazywały się nadmiernie **zróżnicowane**, co miało negatywne konsekwencje w kontekście budowy wspólnego europejskiego rynku. Wraz z rosnącą wymianą handlową zwiększała się potrzeba transferu informacji osobowych, niezbędnych zarówno dla sektora prywatnego, jak również dla służb i instytucji publicznych[21]. Choć wspomniana Konwencja wyraźnie nakazywała swobodę przepływu danych osobowych pomiędzy przyjmującymi ją państwami (art. 12), to jednak zbyt duża swoboda w kreowaniu prawa krajowego powodowała, że znacznie utrudnione lub wręcz niemożliwe było porównanie **adekwatnego poziomu ochrony** przyjętego przez poszczególne państwa. Koniecznym stało się zatem ujednolicenie europejskiego systemu ochrony danych osobowych.

Efektem prac wielu podmiotów Unii Europejskiej było wydanie 24 października 1995 r. **Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych** (dalej: Dyrektywa 95/46/WE)[22].

---

[14] W treści Konwencji występuje termin „kontroler zbioru".

[15] Automatyczne przetwarzanie – oznacza następujące operacje wykonywane w całości lub części przy pomocy metod zautomatyzowanych: rejestrowanie danych, z zastosowaniem do nich operacji logicznych i/albo arytmetycznych, ich modyfikowanie, usuwanie, odzyskiwanie lub rozpowszechnianie (art. 2 lit. c).

[16] M. Polok: *Bezpieczeństwo danych* …, s. 31; J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 47.

[17] Szczególnie wszelka działalność medyczna związana z przetwarzaniem danych osobowych objęta jest wyróżniającym się zainteresowaniem ze strony Rady Europy. Patrz: J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 56-62.

[18] Teksty Rekomendacji dostępne są na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych: http://www.giodo.gov.pl.

[19] Błędnie w wielu pracach nazywane już Unią Europejską, która powstała dopiero w 1993 roku

[20] J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 64.

[21] A. Mednis: Ochrona danych osobowych …, s. 10.

[22] (Dz.Urz. WE z 1995r. L 281, s. 31; Dz.Urz. UE [PL] z 2004r., rozdz. 13, t. 15, s. 355).

Zasadnicze cele, którym mają służyć regulacje przewidziane tą Dyrektywą, to:

- wyznaczenie **jednolitego minimalnego standardu** ochrony prywatności osób fizycznych w związku z przetwarzaniem ich danych osobowych przez wszelkie podmioty działające na terenie państw członkowskich;
- zapewnienie możliwości swobodnego przepływu danych osobowych pomiędzy krajami członkowskimi[23].

Powyższe cele są od siebie wzajemnie zależne. Osiągnięcie pierwszego z nich jest warunkiem koniecznym do możliwości skorzystania z drugiego. Tym samym tylko wdrożenie wyznaczonych zasad bezpiecznego przetwarzania danych osobowych daje państwu przywilej udziału w otwartym systemie gospodarczym Unii Europejskiej.

Mając na uwadze fakt, że Polska jako państwo kandydujące do członkostwa w Unii Europejskiej implementowała Dyrektywę 95/46/WE do krajowego porządku prawnego, na tym etapie pominiemy szczegółowe jej omawianie, a jedynie wskażemy na najważniejsze elementy wprowadzone przez Dyrektywę 95/46/WE; determinują one do dzisiaj europejski system ochrony danych osobowych praktycznie w niezmienionej formie.

Po pierwsze, zostały sprecyzowane terminy związane z przedmiotem ochrony. Pojęcie **danych osobowych**, zostało rozszerzone na *„wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej"*, której tożsamość można ustalić powołując się na numer identyfikacyjny lub jeden bądź kilka szczególnych jej cech fizycznych, fizjologicznych, umysłowych, ekonomicznych, kulturowych lub społecznych (art. 2 lit. a). Wprowadzono kryterium **zbioru danych**, czyli uporządkowanego zestawu informacji osobowych (art. 2 lit. c), który jako regułom ochrony. Jednoznacznie zdefiniowano termin **przetwarzanie danych osobowych**, który oznacza każdą operację na danych osobowych przy pomocy środków zautomatyzowanych lub innych, czyli np.: gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, udostępnianie, układanie lub kompilowanie, blokowanie, usuwanie, aż po ich niszczenie (art. 2 lit. b).

Po drugie, jednoznacznie został wskazany podmiot odpowiedzialny za ochronę przetwarzanych zbiorów danych osobowych – **Administrator danych osobowych**. Jest nim osoba fizyczna lub prawna, która określa cele i sposoby przetwarzania danych (art. 2 lit. d).

Po trzecie, zostały rozbudowane **zasady ogólne** (art. 6) oraz wprowadzono **kryteria legalności** przetwarzania danych osobowych (art. 7). Szczególną uwagę skierowano na **dane o charakterze wrażliwym**, czyli takie, które ujawniają pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, stan zdrowia oraz życie seksualne (art. 8), wprost wskazując na zakaz ich przetwarzania, w przypadku braku którejkolwiek z wymienionych przesłanek zezwalających na przetwarzanie danych wrażliwych.

Po czwarte, zostały powtórzone podstawowe wymagania w zakresie **zabezpieczenia** przetwarzanych danych osobowych przed zagrożeniami, płynącymi z sytuacji niepożądanych. Kraje członkowskie otrzymały swobodę w zakresie określenia wymaganych środków zabezpieczenia, przy bezwzględnym uwzględnieniu ich odpowiedniości do zagrożeń i rodzaju przetwarzanych danych osobowych (art. 17 ust. 1).

Po piąte, zostało wymuszone powołanie **krajowych organów nadzoru**[24] nad przestrzeganiem ustanowionych przez Dyrektywę 95/46/WE zasad ochrony danych osobowych (art. 28). Ponadto przedstawiciele organów nadzoru zostali zobowiązani do udziału w **zespole doradczym** na poziomie całej Unii Europejskiej – tzw. Grupa Robocza (art. 29) – którego opinie i analizy chociaż nie są wiążące, stanowią podstawę wszelkich szczegółowych rozważań na temat aktualnych problemów ochrony danych osobowych[25].

Wymagania Dyrektywy 95/46/WE są **obowiązkowe** dla całego Europejskiego Obszaru Gospodarczego, tj. **dla wszystkich państw członkowskich Unii Europejskiej** oraz Islandii, Luksemburga i Lichtensteinu. Ponadto z jej standardu korzystają także inne kraje europejskie i azjatyckie.

Aktualnie trwają prace nad przyjęciem nowego, dostosowanego do zmienionego otoczenia społecznego i technicznego, europejskiego prawa ochrony danych osobowych.

1.2. USTAWOWA OCHRONA DANYCH OSOBOWYCH W POLSCE

Zmiany społeczno-polityczne, które nastąpiły w naszym kraju po 1989 r., skutkowały przede wszystkim zupełnie innym podejście do roli obywatela i jego praw. Z biernego obserwatora życia publicznego, jednostka przeistoczyła się w czynnego aktora, którego prawa stały się fundamentem demokratycznego państwa.

---

[23] J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 64.

[24] Na poziomie całej Unii Europejskiej w 2004 roku powołano Europejskiego Inspektora Ochrony Danych (ang.: *European Data Protection Supervisor*) – Rozporządzenie 45/2001Wspólnoty Europejskiej z dnia 18 grudnia 2000 roku *o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych* (Dz.U. WE L 8 z 12.01.2001, s. 1).

[25] Więcej o funkcjonowaniu „Grupy Roboczej art. 29" na stronie polskiego organu nadzorczego – Generalnego Inspektora Ochrony Danych Osobowych: http://www.giodo.gov.pl.

Ponadto wola przystąpienia do struktur zachodnioeuropejskich wymusiła dostosowanie prawa krajowego do standardów w nich obowiązujących. Dotyczyło to nie tylko zmian w sferze ekonomiczno-gospodarczej, ale także w zakresie faktycznej ochrony praw obywatelskich. Był to element decydujący o spełnieniu wymagań członkostwa w Unii Europejskiej.

W odniesieniu do przedmiotu poniższych rozważań najważniejsze było zapewnienie obowiązkowej ochrony osób w związku z przetwarzaniem ich danych osobowych. Wiązało się to bezpośrednio z zaimplementowaniem do krajowego systemu prawnego dyspozycji **Dyrektywy 95/46/WE**.

Wskazać należy, że był to obszar – zarówno prawa, jak również praktyki – dotychczas nieznany w naszym kraju.

1.2.1. KONSTYTUCJA RP

Podstawowym i najwyższym aktem determinującym system prawny w Polsce jest uchwalona 2 kwietnia 1997 r. Konstytucja Rzeczpospolitej Polskiej[26] wyznaczająca **generalne standardy** demokratycznego państwa.

Także ochrona danych osobowych znalazła swoje ważne miejsce w treści norm konstytucyjnych. Niemniej jednak zgodnie ze standardem tego rodzaju aktów, nie są to dyspozycje szczegółowe – nie obejmują one wszelkich obszarów zbierania i przetwarzania danych osobowych. Konstytucja skupia się na wskazaniu podstawowych interesów obywateli, które wymagają ochrony przed nadmierną ingerencją w ich prywatność[27].

Przede wszystkim Konstytucja gwarantuje każdej osobie fizycznej prawo do **ochrony**:

- życia prywatnego i rodzinnego,
- czci i dobrego imienia,

oraz do decydowania o swoim życiu osobistym (art. 47).

Chociaż ten zapis nie odnosi się bezpośrednio do **danych osobowych**, to nie można mieć wątpliwości, że ich przetwarzanie zawsze będzie wkraczać w obszar szeroko rozumianego **prawa do prywatności**, stanowiąc jego szczególny i wyspecjalizowany cel ochrony[28].

Bardzo ważnym jest tutaj fakt, że prawo to dotyczy każdej osoby; nie jest zatem ograniczone wymogiem posiadania polskiego obywatelstwa lub jakimkolwiek innym warunkiem, w tym kryterium wieku, stanu psychicznego, zdolności do czynności prawnych. Nie można go też pozbawić w żaden sposób, np. poprzez odebranie praw publicznych[29].

Najważniejszym jednak konstytucyjnym zapewnieniem dbałości państwa o informacje dotyczące obywateli, jest wymóg **ustawowej podstawy** do żądania od nas danych osobowych (art. 51 ust. 1) oraz zasad ich dalszego gromadzenia i udostępniania (art. 51 ust. 5). Oznacza to, że ewentualny obowiązek ujawniania informacji o nas samych nie może pochodzić nawet z poziomu rozporządzenia, a już na pewno jego źródłem nie mogą być wewnętrzne regulaminy, instrukcje, czy polecenia. To samo dotyczy ustawowej rangi przepisu, który musi określać sposób postępowania z zebranymi „danymi osobowymi".

Należy też zauważyć, że ten konstytucyjny nakaz nie jest w żaden sposób ograniczony podmiotowo – dotyczy każdej osoby, oraz przedmiotowo – dotyczy **wszelkiego rodzaju informacji osobowych**, nie zawężając ochrony do wybranej grupy o szczególnym charakterze, czy dotyczącej szczególnych kwestii, np. wygląd, zdrowie, majętność, itp.[30].

Zagwarantowana konstytucyjnie „autonomia informacyjna jednostki", to nie tylko prawo do „samostanowienia" o ujawnianiu informacji na swój temat, ale także bardzo szerokie uprawnienia do **sprawowania kontroli** nad tymi informacjami, które oznaczają:

- prawo dostępu do dotyczących nas urzędowych dokumentów i zbiorów danych (art. 51 ust. 3);
- prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą (art. 51 ust. 4).

Dyspozycje te mogą wywoływać kilka praktycznych wątpliwości, w zakresie ich jurysdykcji poza obszarem administracji publicznej; chodzi o to, czy dotyczą również „danych osobowych" zbieranych i przetwarzanych przez podmioty prywatne, fundacje, stowarzyszenia, itp.

W pierwszym przypadku istnieje bezpośrednie odesłanie do „urzędu", czyli organu publicznego. Nie oznacza, to jednak, że nie mamy prawa nadzoru nad naszymi informacjami osobowymi posiadanymi przez podmioty prywatne, a jedynie tyle, że przepis ten odnosi się do administracji[31], która jest zobowiązana udostępnić nam **wgląd** do zebranych o nas informacji bezpośrednio w urzędowych dokumentach i zbiorach danych[32].

---

[26] (Dz.U. nr 78, poz. 483, z późn. zm.).

[27] J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 94.

[28] J. Oniszczuk: Konstytucja Rzeczpospolitej Polskiej w orzecznictwie Trybunału Konstytucyjnego, Kraków: ABC, 2000, s. 398.

[29] J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 95.

[30] J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 94-95.

[31] J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 95.

[32] Organizacje niepubliczne na podstawie innych przepisów także zobowiązane są udzielić informacji o przetwarzaniu naszych „danych osobowych", z tym zastrzeżeniem, że nie istnieje obowiązek udostępnienia dokumentów i zbiorów.

W drugim przypadku jest niemal oczywiste, że zapewnienie wskazanych uprawnień dotyczy **wszelkich podmiotów**, które w swojej działalności zbierają „dane osobowe".

Reasumując należy jeszcze zauważyć, że samo posiadanie ustawowej zgody na przetwarzanie „danych osobowych" nie określa jeszcze jego konstytucyjnej zgodności. Ograniczenie prawa do „autonomii informacyjnej" musi mieć charakter wyjątkowy, szczegółowo wyznaczony podmiotowo i przedmiotowo, tak by nie naruszać jego istoty, (tzw. **klauzula konieczności** w demokratycznym społeczeństwie)[33].

1.2.2. USTAWA O OCHRONIE DANYCH OSOBOWYCH

Wykonaniem konstytucyjnego obowiązku ustawowej regulacji dopuszczalności zbierania i przetwarzania danych osobowych jest **Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych** (dalej: Ustawa)[34].

W praktyce nie jest ona jednak bezpośrednim następstwem przyjęcia zaledwie miesiąc wcześniej Konstytucji RP, ale przede wszystkim ponad 6-letniego procesu legislacyjnego wynikającego z powszechnej potrzeby dostosowania polskiego prawodawstwa do standardów demokratycznej Europy. Jednocześnie zapoczątkowany już proces integracji z Unią Europejską skutkował obowiązkiem implementacji Dyrektywy 95/46/WE.

Ustawa w swoim pierwszym zdaniu powtarza konstytucyjną gwarancję autonomii informacyjnej dającą **każdemu** prawo do ochrony dotyczących jego danych osobowych (art. 1 ust. 1), bez względu na jego przymioty prawne czy faktyczne, o których była już mowa w poprzednim podrozdziale.

1.2.3. AKTY WYKONAWCZE

Uszczegółowienie regulacji ustawowych dla kilku ważnych obszarów znajduje swoje miejsce w wydanych przez upoważnionych ministrów **rozporządzeniach wykonawczych**. Chociaż są to akty niższego rzędu, doprecyzowujące a nie tworzące nowe reguły, to jednak w polskim systemie prawnym stanowią zazwyczaj wyznaczniki praktycznej realizacji wielu ogólnych wymagań zawartych w ustawie. Nie inaczej jest w omawianym zakresie.

Najważniejszym przepisem wykonawczym wydanym zgodnie z dyspozycją ustawy jest Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku **w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych**[35].

Zgodnie z dyspozycją tytułu w zakresie regulacji przedmiotowego Rozporządzenia znajdują się takie obszary, jak:

1) podstawowe wymogi bezpieczeństwa dla systemów informatycznych służących do przetwarzania danych osobowych;
2) wymagania w zakresie minimalnej funkcjonalności systemów informatycznych, w szczególności w zakresie odnotowywania udostępniania danych osobowych;
3) zakres dokumentacji opisującej:
   a) sposób przetwarzania danych osobowych,
   b) środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.

Efektem ostatniej nowelizacji Ustawy[36] jest zbiór rozporządzeń dotyczących wyznaczania i wypełniania zadań przez „**Administratora bezpieczeństwa informacji**":

1) Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 roku **w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji**[37].
2) Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji[38].
3) Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych[39].

Rozporządzeniem o charakterze technicznym jest Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 roku **w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony**

---

33 Szerzej: B. Banaszak: *Konstytucja Rzeczpospolitej Polskiej.* …, s. 309 i nast..

34 (Dz.U. nr 133, poz. 883; tekst jedn. Dz.U. 2014, poz. 1182).

35 (Dz.U. nr 100, poz. 1024).

36 Ustawa z dnia 7 listopada 2014 roku *o ułatwieniu wykonywania działalności gospodarczej*, (Dz.U. 2014, poz. 1662).

37 (Dz.U. 2014, poz. 1934).

38 (Dz.U. 2015, poz. 745).

39 (Dz.U. 2015, poz. 719).

Danych Osobowych[40]. Nie określa ono zasad rejestracji „zbiorów danych osobowych", a jedynie prezentuje wzór druku, na którym dokonuje się zgłoszenia rejestracyjnego.

W praktyce jest to rozporządzenie zupełnie nieprzydatne, gdyż proces wypełniania wniosku o rejestracje „zbioru danych osobowych" jest zautomatyzowany i dokonuje się go w gotowym formularzu elektronicznym znajdującym się na specjalne stronie internetowej Generalnego Inspektora Danych Osobowych (GIODO)[41].

Ostatnia grupa rozporządzeń dotyczy organizacji pracy **Biura Generalnego Inspektora**:

1) Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 10 października 2011 roku **w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych**[42].
2) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 roku w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych[43].

Praktyczne wymagania powyższych aktów wykonawczych zostaną szczegółowo omówione w kolejnych rozdziałach.

1.2.4. WYŁĄCZENIE STOSOWANIA USTAWY

Ustawodawca przyjął kilka **szczególnych sytuacji** prawnych i faktycznych, które pozwalają na wyłączenie stosowania Ustawy. Może to dotyczyć zarówno jej całości, jak również odnosić się do określonych rozdziałów, czy nawet pojedynczych przepisów. Są to klauzule szczególne – ograniczające prawo podstawowe, a zatem nie mogą być interpretowane rozszerzająco, w szczególności w celu ominięcia wymogów ustawowych gwarantujących istotę ochrony „danych osobowych".

Podstawowym wyłączeniem stosowania całości Ustawy jest wykorzystywanie „danych osobowych" przez **osoby fizyczne**, ale także tylko w sytuacji gdy jego celem są **czynności osobiste lub domowe** (art. 3a ust. 1 pkt 1). Mamy więc tutaj do czynienia z dwoma warunkami wyłączającymi – podmiot i cel, które muszą zaistnieć równocześnie.

Dla spełnienia pierwszego kryterium „dane osobowe" muszą być przetwarzane przez „osobę fizyczną", a więc nie może to być żadna zbiorowość czy podmiot, tj. przedsiębiorstwo, spółka (nawet osobowa), korporacje, stowarzyszenia czy kluby, bez względu na ich wielkość. Może to być jednak grupa osób fizycznych, pozostająca w wyraźnym związku osobistym, w szczególności pokrewieństwa lub powinowactwa. Wyjmując tym samym spod restrykcji ustawowych **wspólnoty rodzinne**[44].

Drugim kryterium jest cel przetwarzania. Chociaż determinanty są nieostre i trudno jest znaleźć granicę pomiędzy czynnościami „osobistymi lub domowymi", a tymi, które już takiego waloru nie mają, to jednak nie napotyka się tutaj na nadużycia tego wyjątku. Powszechnie przyjmuje się nawet, że takim rodzajem działalności może być nawet taka, która ma cechy **czynności zarobkowych**, np. działalność kolekcjonerska czy udział w aukcjach elektronicznych. Z tym podstawowym zastrzeżeniem, że osoba fizyczna nie realizuje tego w ramach prowadzonej działalności gospodarczej[45].

Studium przypadku:
Za cel osobisty lub domowy należy uznać przechowywanie danych teleadresowych, nawet w dostępnym dla wszystkich domowników notatniku papierowym czy elektronicznym.

Ważnym wyłączeniem stosowania ustawy jest wykonywanie szczególnych grup **działalności zawodowej**:

- dziennikarskiej;
- literackiej;
- artystycznej (art. 3a ust. 2.).

Pierwsza jest wyznaczona przepisami prawa prasowego[46], natomiast pozostałe nie mają swojej jednoznacznej definicji, czy umocowania ustawowego[47]. Bez względu jednak na nieostrość tych pojęć – nawet w przypadku działalności dziennikarskiej – najistotniejszym elementem decydującym o wyłączeniu stosowania ustawy jest **bezpośrednie wykonywanie tej działalności**, a nie działalności wspierającej te zawody, np. marketing, skład czy sprzedaż dzieła.

---

[40] (Dz.U. nr 229, poz. 1536).
[41] Moduł internetowej rejestracji „zbiorów danych osobowych" znajduje się pod adresem: https://egiodo.giodo.gov.pl/index.dhtml.
[42] (Dz.U. nr 225, poz. 1350).
[43] (Dz.U. nr 94, poz. 923, zm. Dz.U. 2011, nr 103, poz. 601).
[44] J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 322-323.
[45] A. Drozd: Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy, Wydanie 3, Warszawa: LexisNexis, 2007, s. 29.
[46] Patrz: Ustawa z dnia 26 stycznia 1984 roku – *Prawo prasowe*, (Dz.U. nr 5, poz. 24, z późn. zm.), art. 7 ust. 2 pkt. 1.
[47] Można ją identyfikować jednakże jako działalność twórczą, której wynikiem jest przedmiot praw autorskich określonych w Ustawie z dnia 4 lutego 1994 roku *o ochronie praw autorskich i praw pokrewnych*, (Dz.U. nr 24, poz. 83, z późn. zm.).

Nie ma natomiast znaczenia czy czynności te są wykonywane jako działalność *stricte* zawodowa – członek redakcji telewizyjnej, profesjonalny aktor, czy jako rodzaj aktywności amatorskiej – bloger internetowy, twórca ludowy[48].

Studium przypadku:
Ustawa ma zastosowanie do zbierania, opracowania i publikowania materiałów prasowych, ale nie obejmuje działań związanych z procesem sprzedaży czasopisma przez wydawnictwo.

Powyższe wyłączenie **nie jest jednak zupełne**. Nadal zastosowanie mają obowiązki związane z właściwym zabezpieczeniem „danych osobowych"(art. 36 ust. 1). Nie są też ograniczone uprawnienia kontrolne Generalnego Inspektora (art. 14-19). W tym drugim przypadku istnieją jednak wątpliwości czy takie działania nie mogłyby pociągać za sobą naruszenia „tajemnicy dziennikarskiej"[49].

Innego rodzaju powodem wyłączenia stosowania Ustawy jest kryterium „**doraźności zbioru**", do którego są zbierane informacje o osobach (art. 2 ust. 3). Przez „doraźność" należy rozumieć szczególny **cel** jego utworzenia:

- techniczny;
- szkoleniowy;
- związany z dydaktyką w szkołach wyższych,

po którego ustaniu następuje niezwłoczne usunięcie lub anonimizacja „danych osobowych".

Determinantem uznania „doraźności" **nie jest czas przetwarzania** „danych osobowych" w konkretnym zbiorze. Przede wszystkim nie jest to warunek decydujący, choćby z uwagi na brak jego ustawowego określenia, tj. jakie mają być czasowe granice „doraźności". Kluczowa jest tu okoliczność tworzenia takiego zbioru, a więc jego faktyczne **przeznaczenie**. Przede wszystkich charakteru technicznego nie będzie miało przetwarzanie „danych osobowych" w obszarze statutowych zadań przedsiębiorstwa, np. marketing własnych produktów[50].

Studium przypadku:
Zbiorem „doraźnym" nie jest kartoteka dokumentów CV osób ubiegających się o przyjęcie do pracy, nawet w przypadku jej prowadzenia wyłącznie przez kilkudniowy proces naboru, a po nim zniszczona.
Rekrutacja jest ustawowo określonym, typowy celem każdej organizacji.

Wśród najważniejszych wyłączeń należy jeszcze wskazać na przyjętą przez ustawodawcę **wyższość przepisu szczegółowego** nad ogólnym (łac.: „*lex specialis derogat legi generali*"), zawężając ją jednak wyłącznie do tych przypadków, w których akt szczegółowy przewiduje wyższy poziom ochrony dla „danych osobowych" (art. 5).

W bardzo wielu przypadkach istnienie „dalej idącej ochrony" będzie praktycznie niemożliwe do jednoznacznego stwierdzenia. Właściwym wtedy będzie określenie, że mamy do czynienia z ochroną „inaczej ukształtowaną". Najważniejsze wtedy będzie ustalenie czy wskazane w innym akcie prawnym rangi ustawy wymogi bezpieczeństwa informacji zapewniają **minimalny poziom ochrony**, przynajmniej równoważny temu, który wynika z Ustawy[51].

Przedmiotowa reguła nie dotyczy jednak bezwzględnej relacji pomiędzy całymi ustawami, a najczęściej jedynie tych obszarów, w których **przepisy szczegółowe** innych aktów odnoszą się do ochrony „danych osobowych" [52]. Wyłączenie dyspozycji Ustawy będzie w takim przypadku dotyczyło tylko odmiennych wymogów w konkretnej sytuacji, procesie czy terminie, dla jednoznacznie wskazanego podmiotu[53].

Studium przypadku:
Przedsiębiorca świadczący usługi detektywistyczne może przetwarzać bez wiedzy i zgody osoby jej dane osobowe.
Może to robić jednak tylko za pośrednictwem pracowników mających „Licencję Detektywa", z zachowaniem wszelkich środków bezpieczeństwa, w sposób nie naruszający istoty praw i wolności obywatelskich.
Dodatkowo tego rodzaju przedsiębiorca nie ma prawa udostępnić komukolwiek poza zlecającemu usługę detektywistyczną zebranych w toku czynności danych osobowych.

---

[48] J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 324-325.
[49] M. Sakowska, A. Młynarska-Sobaczewska: *„Klauzula prasowa" z ustawy o ochronie danych osobowych*, „Prokuratura i Prawo", nr 1, 2005, s. 74.
[50] P. Barta, P. Litwiński: *Ustawa o ochronie* …, s. 30-31.
[51] J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 334.
[52] A. Drozd: *Ustawa o ochronie* …, s. 37.
[53] Wykaz najważniejszych aktów prawnych zawierających przepisy odnoszące się do przetwarzania „danych osobowych" można znaleźć w: J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 105-123.

Zbliżonym do powyższego, powodem wyłączającym stosowanie Ustawy jest sytuacja, w której **umowa międzynarodowa** zawarta przez Rzeczpospolitą Polską wyraźnie odnosi się do przetwarzania i ochrony „danych osobowych", zakładając jednocześnie odmienne standardy niż te przyjęte w ustawie (art. 4). Ważnym jednocześnie warunkiem dla możliwości wyłączenia Ustawy jest poprawna ratyfikacja takiej umowy międzynarodowej, a następnie jej publikacja w Dzienniku Ustaw[54].

Podsumowując analizę wyłączeń należy zwrócić uwagę na dwa kluczowe dla praktycznego ich stosowania aspekty.

Po pierwsze, ustawodawca **nie uzależnia** dopuszczalności żadnego z przedstawionych wyłączeń od:

- zawartości informacyjnej przetwarzanych „danych osobowych", tj. ewentualnej „wrażliwej" ich treści;
- sposobu przetwarzania „danych osobowych", tj. kartoteka papierowa czy system informatyczny.

Po drugie, nie istnieje jednocześnie żadna przesłanka prawna czy formalna pozwalająca na automatyczne wykluczenie stosowania całości Ustawy w odniesieniu do obszarów regulowanych przepisami dotyczącymi **innych tajemnic**, np. informacji niejawnych[55], tajemnicy bankowej[56] czy tajemnicy przedsiębiorstwa[57].

Studium przypadku:
Przedsiębiorca mający „Świadectwo Bezpieczeństwa Przemysłowego", oznaczające jego pełną zdolność do ochrony informacji niejawnych o klauzuli „Tajne", nie może na podstawie tego uprawnienia uznać, że nie obowiązują go przepisy ustawy o ochronie danych osobowych. Nawet w odniesieniu do „zbiorów danych osobowych" stanowiących tą tajemnicę i przetwarzanych w „Kancelarii Tajnej".

[54] A. Drozd: *Ustawa o ochronie* …, s. 33.

[55] Patrz: G. Sibiga: Ochrona informacji niejawnych i ochrona danych osobowych. Wybrane zagadnienia wzajemnych relacji, (w:) Gajos M. (red. nauk.): Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały V Kongresu, Katowice: KSOIN, 2009, s. 155-162.

[56] Patrz: M. Krzysztofek: *Tajemnica bankowa i ochrona danych osobowych w praktyce bankowej*, Warszawa: LexysNexis, 2010, s. 17-38.

[57] Patrz: E. Nowińska, M. du Vall: *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz*, Wydanie 5, Warszawa: LexisNexis, 2010, s. 163-179.

2. PRZEDMIOT OCHRONY – PODSTAWOWE POJĘCIA

mgr Bartosz Mendyk

Prawidłowe wykonywanie obowiązków związanych z przetwarzaniem danych osobowych wymaga zrozumienia najważniejszych definicji.

Pojęcia użyte w ustawie nie są terminami prostymi. Jak zostanie przedstawione poniżej, niektóre informacje w poszczególnych sytuacjach mogą zostać uznane za **dane osobowe**, a w innych sytuacjach tak się nie stanie. Celem autorów niniejszej publikacji nie jest wyłącznie przedstawienie definicji ustawowej lub przywołanie bez kontekstu orzeczeń sądowych, ale pokazanie odpowiednich mechanizmów, które pozwolą samodzielnie rozpoznać, w których przypadkach mamy do czynienia z danymi osobowymi, a w których nie.

Dopiero zrozumienie wszystkich powyższych terminów pozwoli skutecznie zarządzać danymi osobowymi i wdrożyć procedury zabezpieczające zbiory danych osobowych.

2.1. POJĘCIE DANYCH OSOBOWYCH

Pojęcie danych osobowych zostało zawarte w Ustawie. Zgodnie z przywołanym aktem prawnym danymi osobowymi są „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej".

Powyższa definicja składa się zatem z kilku elementów, które należy doprecyzować. Są to:

1) **„Wszelkie informacje dotyczące**…". Ten element należy rozumieć szeroko – od wyglądu osoby, poprzez jej imię i nazwisko[58], numery PESEL, kolor oczu, odciski palców, nawyki ubraniowe, aż po pozycję społeczną.
2) **„…zidentyfikowanej lub możliwej do zidentyfikowania...".** Ten element oznacza możliwość ustalenia w sposób niebudzący wątpliwości czyjejś tożsamości na podstawie informacji, o których mowa we wcześniejszym punkcie.
3) **„…pośrednio lub bezpośrednio…".** Pośrednia identyfikacja dotyczy wykorzystania kilku zbiorów danych, których odpowiednie powiązanie pozwala zidentyfikować, tj. ustalić tożsamość osoby. (Może to być np. lista zatrudnionych pracowników w przedsiębiorstwie X oraz lista kart ewidencjonujących czas pracy w przedsiębiorstwie X). Bezpośrednia identyfikacja wykorzystuje tylko jeden zbiór danych. (Może to być np. teczka osobowa pracownika przedsiębiorstwa X).
4) **„...osoby fizycznej**…". Definicja dotyczy wyłącznie żyjących osób fizycznych. Tym samym nie dotyczy osób prawnych, spółek prawa handlowego, stowarzyszeń itp.[59]. Warto też pamiętać, że od 16 maja 2016 r. będzie ułatwione przetwarzanie danych osobowych osób fizycznych prowadzących działalność gospodarczą, bowiem Centralna Ewidencja i Informacja o Działalności Gospodarczej (CEIDG) została wyłączona z Ustawy.

Informacji **nie uważa** się za umożliwiające określenie tożsamości osoby, jeżeli wykorzystanie tych informacji w powyższym celu **wymagałoby poniesienia nadmiernych kosztów, poświęcenia zbyt dużo czasu lub podjęcia zbyt wielu działań**[60]. Powyższe elementy występują zawsze w określonym kontekście, czyli w pewnych sytuacjach informacje będą uznane za dane, zaś w innych – nie.

Co do zasady daną osobową **nie będzie też pojedyncza** informacja o dużym stopniu ogólności, np. nazwa ulicy, numer domu czy wysokość wynagrodzenia. Taka informacja **będzie** jednak stanowić daną osobową wówczas, gdy zostanie ona zestawiona z innymi dodatkowymi informacjami, które w konsekwencji będzie można odnieść do konkretnej osoby.

Studium przypadku 1:
Numer PESEL dla administracji publicznej będzie stanowił daną osobową, gdyż pracownicy urzędu, mając dostęp do innych baz, są w stanie zidentyfikować osobę za pomocą tego numeru. Natomiast dla małego przedsiębiorcy, który nie ma dostępu do żadnych baz i zbiera wyłącznie numery PESEL (bez zestawiania ich z imieniem i nazwiskiem), będą to wyłącznie ciągi nic niemówiących cyfr.

Studium przypadku 2:
Numer rejestracyjny samochodu dla przedsiębiorcy niemającego dostępu do odpowiednich baz danych nie pozwoli na identyfikację właściciela pojazdu. (Może najwyżej dać wiedzę, że właściciel auta zarejestrował pojazd w określonej miejscowości). Ale dla firmy detektywistycznej, która na podstawie numeru jest w stanie zidentyfikować właściciela za pomocą odpowiednich instrumentów, numer rejestracyjny będzie stanowić daną osobową.

[58] Zob. A. Mączyński, Uznanie nazwiska w świetle konwencji nr 31 Międzynarodowej Komisji Stanu Cywilnego z 2005, [w:] Ochrona danych osobowych, wczoraj, dziś, jutro, Warszawa 2006,wyd. GIODO, s. 242.
[59] Decyzja Generalnego Inspektora z dnia 11-06-2012 o sygn. (DOLiS/DEC-520/12/35884).
[60] Wyrok Naczelnego Sądu Administracyjnego z dnia 19-05-2011 o sygn. (I OSK 1086/10).

Studium przypadku 3:
Wewnętrzne legitymacje w przedsiębiorstwie dla pracodawcy oraz innych pracowników będą stanowić daną osobową, bowiem każdy zatrudniony bez większego trudu zidentyfikuje pracownika posługującego się legitymacją nr 175. Natomiast dla osób spoza przedsiębiorstwa będzie to nic niemówiąca cyfra na wewnętrznym identyfikatorze.

Adresy poczty elektronicznej (e-mail) w części przypadków są danymi osobowymi w rozumieniu Ustawy. Zazwyczaj bowiem są w nich umieszczone takie informacje jak:

- imię,
- nazwisko,
- dodatkowa informacja

które w połączeniu pozwalają na identyfikację właściciela adresu poczty elektronicznej w sposób pośredni lub bezpośredni.

Studium przypadku
Na liście subskrybentów newslettera sklepu internetowego są zarówno adresy e-mail, które stanowią dane osobowe (np. jan_stanislaw_kowalski@nazwafirmy.com.pl), jak i takie, które ich nie stanowią (lewapiksrokis@gxm.net).

Inną kwestią jest to, czy **adres IP** (z ang. *Internet Protocol Adddress*) stanowi daną osobową. Adres IP jest to numer porządkowy przypisany urządzeniu, które jest elementem sieci informatycznej. Sam numer nie pozwala w sposób bezpośredni zidentyfikować osoby fizycznej, która użytkuje urządzenie. Zakwalifikowanie adresu IP jako danej osobowej wiąże się z koniecznością posiadania dodatkowych informacji umożliwiających identyfikację osoby użytkującej urządzenie. Niezwykle istotne jest również to, aby adres IP miał charakter stały.

Jeżeli zatem adres IP jest przyporządkowany do lokalnej sieci internetowej (z ang. *Local Area Network* – LAN), z której korzysta wielu współużytkowników, nie będzie daną osobową[61].

Adres IP będzie natomiast stanowić daną osobową, jeżeli:

- **jest on na stałe przypisany do konkretnego urządzenia,**
- **urządzenie to jest przypisane konkretnemu użytkownikowi**.

W powyższym przypadku jest bowiem możliwość identyfikacji konkretnej osoby fizycznej[62].

Szczególną kwestią, której nie można pominąć przy okazji rozważań na temat danych osobowych, jest **wizerunek osoby fizycznej**. Coraz więcej przedsiębiorców zwłaszcza z branży usługowej (np. szkoły językowe lub szkoły aktywnego wypoczynku) prowadzi własne strony internetowe bądź tzw. *fun page* na portalach społecznościowych. Często umieszczają tam wizerunki ludzi korzystających z oferowanych przez nich usług.

Wykorzystanie wizerunku oraz jego ochrona jest przewidziana w:

- Ustawie o ochronie danych osobowych;
- Kodeksie cywilnym[63];
- Ustawie o prawie autorskim i prawach pokrewnych[64].

Wizerunek to wygląd człowieka bez względu na technikę jego utrwalenia, czyli:

- fotografia,
- rysunek,
- wycinanka,
- sylwetka,
- film,
- przekaz telewizyjny,
- przekaz wideo[65].

Zezwolenie na rozpowszechnianie wizerunku może być udzielone w dowolnej formie[66]. Bez zezwolenia jest dozwolone wykorzystanie wizerunku w dwóch sytuacjach:

---

61 P. Barta, P. Litwiński,„Ustawa o ochronie danych osobowych. Komentarz…, s. 100–101.
62 Wyrok Naczelnego Sądu Administracyjnego z 19 maja 2011 roku, sygn. (I OS K 1079/1021).
63 (Dz.U. 1964 nr 16 poz. 93).
64 (Dz.U. 1994 nr 24 poz. 83).
65 Wyrok Sądu Apelacyjnego w Katowicach z dnia 28-05-2015 o sygn. (I ACa 158/15).
66 Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 27-06-2014 o sygn. (I ACa 633/14).

- chodzi o osobę powszechnie znaną, jeżeli jej wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych[67]; dotyczy to polityków, sportowców, aktorów, dziennikarzy lub osoby powszechnie nieznanej, która urządza happening[68];
- chodzi o osobę stanowiącą jedynie szczegół większej całości, czyli np. zgromadzenie publiczne, krajobraz itd.

Osoba decydująca się na udział w zgromadzeniu publicznym wyraża w sposób dorozumiany zgodę na upublicznienie jej wizerunku[69].

Studium przypadku 1
Na pierwszym planie plakatu szkoły językowej stoi trzech klientów trzymając kciuki w górze. Ich twarze stanowią dane osobowe.

Studium przypadku 2
Przedsiębiorca prowadzący szkołę prawa jazdy fotografuje w pełni wyposażoną salę wykładową. Na zdjęciu występuje jeden klient, który studiuje planszę dotyczącą pierwszeństwa na skrzyżowaniu. Na zdjęciu można rozpoznać klienta. Jednakże jego twarz jest szczegółem całości – zdjęcie ma bowiem pokazać wyposażoną salę. W tym wypadku twarz klienta nie będzie stanowić danych osobowych.

Ważną podkategorią danych osobowych są tzw. **dane wrażliwe (sensytywne)**. Są one zdefiniowane w Ustawie na zasadzie wyjątku. Oznacza to, że **danymi wrażliwymi będą tylko i wyłącznie te, które ustawodawca bezpośrednio przewidział w Ustawie (art. 27)**. Będą to:

- dane ujawniające pochodzenie rasowe lub etniczne (czyli np. zbieranie informacji dotyczących tego, kto jest Żydem, Arabem, etc.[70]);
- dane ujawniające poglądy polityczne (czyli np. zbieranie informacji na temat preferencji wyborczych danej osoby przy okazji wyborów prezydenckich, czy parlamentarnych, jak również tego, czy ktoś brał udział w referendum, a jeżeli tak, to w jaki sposób głosował);
- dane ujawniające przekonania religijne lub filozoficzne, przynależność wyznaniową (czyli np. zbieranie informacji na temat tego, czy dana osoba przynależy lub nie przynależy do jakiegoś związku wyznaniowego);
- dane ujawniające przynależność partyjną lub związkową; w przypadku przedsiębiorców (pracodawców) zbieranie informacji o przynależności ich podwładnych do związków zawodowych jest możliwe wyłącznie na podstawie specjalnych ustaw[71];
- dane o stanie zdrowia; tylko określony przepis konkretnej ustawy uprawnia pracodawcę do uzyskania informacji o stanie zdrowia pracownika[72]; uważa się, że informacja o ciąży lub jak często określona osoba choruje również jest daną wrażliwą;
- dane o kodzie genetycznym (czyli np. wzory linii papilarnych, wizerunek twarzy, geometria ust, odcisk dłoni, zapis głosu); zbieranie powyższych danych przez pracodawców jest zabronione (nawet wtedy, kiedy pracownicy wyrażą na to zgodę), a przedsiębiorcy mogą zbierać takie dane od klientów po spełnieniu dodatkowych kryteriów[73];
- dane o nałogach (czyli np. zbieranie informacji o czyimś uzależnieniu od alkoholu, środków odurzających, hazardu itd.);
- dane o życiu seksualnym (czyli np. zbieranie informacji o preferencjach seksualnych innej osoby); takie informacje są zbierane zazwyczaj w serwisach randkowych;
- dane dotyczące skazań (zatarcia skazań), orzeczeń o ukaraniu i mandatach karnych;
- dane dotyczące innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

---

[67] W zakresie pojęcia osób publicznych zob. B. Banaszak, K. Wygoda, Pojęcie Funkcji Publicznej jako przesłanka modyfikująca zakres ochrony danych osobowych, [w:] Ochrona danych osobowych, wczoraj, dziś, jutro, Warszawa 2006,wyd. GIODO, 59 i n.

[68] Wyrok Sądu Apelacyjnego w Poznaniu z dnia 02-09-2010 o sygn. (I ACa 620/10).

[69] wyrok Sądu Apelacyjnego w Łodzi z dnia 06-10-2014 o sygn. (I ACa 429/14).

[70] Por. A. Gajda, Ochrona danych osobowych i kierunki zmian w tej dziedzinie w prawie Unii Europejskiej, Kwartalnik Kolegium Ekonomiczno-Społecznego, nr 4, vol. 20, 2014, s. 61.

[71] W szczególności ustawa z dnia 23 maja 1991r. o związkach zawodowych (Dz.U. z 2001r. Nr 79, poz. 854) oraz ustawa z dnia 13 marca 2003 r. o szczególnych zasadach rozwiązywania z pracownikami stosunków pracy z przyczyn niedotyczących pracowników (Dz.U. 2003 nr 90 poz. 844) (tzw. ustawa o zwolnieniach grupowych).

[72] Np. art. 57 ust. 1 ustawy z 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa).

[73] L. Kępa, Dane osobowe w firmie. Praktyczny poradnik przedsiębiorcy, Warszawa, Diffin, 2011.

Przetwarzanie danych podlegających szczególnej ochronie (wrażliwych) **co do zasady jest zabronione.** Ustawa wprowadza od tego kilka wyjątków ujętych w zamknięty katalog[74].

Studium przypadku:
Przedsiębiorca w celu zapewnienia pracownikom palarni zbiera informacje, którzy pracownicy palą papierosy. Następuje proces zbierania danych osobowych wrażliwych.

2.2. PRZETWARZANIE DANYCH W ZBIORZE

Co do zasady przepisy Ustawy dotyczą przede wszystkim danych, które są przetwarzane w zbiorze. Jednakże dane osobowe korzystają z ochrony przewidzianej Ustawą już wówczas, jeżeli tylko **mogą** znaleźć się w zbiorze danych osobowych, bez względu na to, czy się w nim ostatecznie znalazły[75]. Przedsiębiorca musi więc przyjąć, że niezależnie od tego, czy dane osobowe są przetwarzane w zbiorze czy poza nim, podlegają pod przepisy Ustawy.

Przez pojęcie **zbiór danych** rozumie się „każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnym według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie" (Art. 7 ust. 1). Definicja zbioru składa się zatem z wielu elementów, które należy doprecyzować.

1) **„Każdy posiadający strukturę zestaw danych…".** Oznacza to konieczność zawarcia w zestawie kryteriów umożliwiających odnalezienie w nim danych osobowych. Uważa się, że powinny być to co najmniej dwa kryteria[76]:
   a) **osobowe** (np. imię, nazwisko, data urodzenia, PESEL);
   b) **nieosobowe** (np. data zamieszczenia danych w zbiorze)[77].
2) **„…o charakterze osobowym…".** Oznacza to, że dotyczy to tylko osób fizycznych (chodzi np. o rejestr osób wchodzących do budynku).
3) **„…niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie…".** Zebrane dane mogą znajdować się w jednym skoroszycie, w drugim natomiast mogą znajdować się inne dane związane z tymi pierwszymi; rozproszenie ma miejsce niezależne od tego, czy występuje w systemie informatycznych, czy w formie papierowej.

Studium przypadku 1:
Aplikacje do pracy są przechowywane w systemie informatycznym, przy czym kryterium umożliwiającym odszukanie osoby to numer referencyjny bądź nazwa stanowiska, na które dana osoba złożyła aplikację. Występują więc określone kryteria, które umożliwiają odnalezienie konkretnych danych osobowych.

Studium przypadku 2:
Dane osobowe zawarte w umowach sprzedaży i dane osobowe zawarte w systemie informatycznym o nazwie „Symfonia", trzeba traktować jako zbiór danych w rozumieniu ustawy (…) wówczas, gdy zawierają te same, wspólne dane klientów, posiadają strukturę uporządkowaną w programie informatycznym oraz więcej niż jedno kryterium dostępu (imię, nazwisko, adres zamieszkania)[78].

Ustawodawca zdefiniował również pojęcie **„przetwarzania danych""**, przez co **rozumie się jakiekolwiek operacje wykonywane na danych osobowych**, w szczególności:

- zbieranie,
- utrwalanie,
- przechowywanie,
- opracowywanie,
- zmienianie,

[74] Zob. Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 23-09-2010 o sygn. (II SA/Wa 666/10).
[75] Postanowienie Sądu Najwyższego z dnia 2000-12-11 o sygn. (II KKN 438/00.)
[76] Wyrok Naczelnego Sądu Administracyjnego z dnia 12-01-2007 r o sygn.(I OSK 218/06).
[77] Por. J. Barta, Komentarz…, który również zwraca uwagę, że „to bowiem struktura zbioru danych osobowych powinna zapewnić dostęp do danych zawartych w zbiorze." Ten sam autor zwraca jednak uwagę, że „nie można utożsamiać dostępności informacji w zbiorze z ich uporządkowaniem – o uporządkowaniu można bowiem mówić jedynie w znaczeniu posiadania przez zbiór odpowiedniej struktury, co nie oznacza jednak uporządkowania poszczególnych elementów, ale jedynie ich dostępność". por. *P. Fajgielski*, Ochrona danych osobowych w telekomunikacji – aspekty prawne, Lublin, wydawnictwo: „Lubelskie Towarzystwo Naukowe", 2003, s. 47.
[78] Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 13-03-2008 o sygn. (II SA/Wa 143/08).

- udostępnianie,
- usuwanie

a **zwłaszcza te operacje, które wykonuje się w systemach informatycznych (art. 7 ust. 2)**[79]**.**

Trudno w prawie znaleźć szerszą definicję. Użycie określenia „jakiekolwiek" oznacza, że **faktycznie każda czynność, jakiej zostały poddane dane osobowe, będzie oznaczać ich przetwarzanie (art. 7 ust 2 ustawy).**

Studium przypadku 1:
Przedsiębiorca zakupił nowe nośniki informacji (twarde dyski). Stare nośniki zawierające dane osobowe musi zniszczyć. Niszczenie dysków twardych zawierających dane osobowe oznacza przetwarzanie danych osobowych.

Studium przypadku 2:
Przedsiębiorca postanowił zarchiwizować dane osobowe swoich pracowników. Oddanie dokumentów do archiwum zakładowego stanowi przetwarzanie danych osobowych.

2.3. WARUNKI OGÓLNE POZYSKIWANIA I PRZETWARZANIA DANYCH OSOBOWYCH

Pozyskiwanie danych osobowych i przechowywanie plików z danymi w opisany sposób ma istotne znaczenie dla działalności zarówno sektora prywatnego, jak i państwowego. Akty prawne i zasady dotyczące ochrony danych mają na celu ustalenie sposobów rozwiązania konfliktu między ochroną prywatności a potrzebą posiadania informacji o innych członkach społeczeństwa, a także osiągnięcia zadowalającej równowagi między poszczególnymi stronami[80].

2.3.1. Przesłanki ogólne

Administrator danych osobowych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest zobowiązany zapewnić, aby dane te były:

1) przetwarzane zgodnie z prawem na każdym etapie ich przetwarzania;
2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu, które jest niezgodne z tymi celami; wykorzystanie pozyskanych danych osobowych do innych celów będzie oznaczać konieczność spełnienie nowych warunków ustawowych (w szczególności zebranie nowych zgód na przetwarzanie danych osobowych);
3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Niezależnie od podstawy prawnej, każdy Administrator danych osobowych powinien przestrzegać zasad ogólnych dotyczących przetwarzania danych.

1) **Zasada celowości,** która przewiduje, że dane osobowe są pozyskiwane dla dokonywania określonych, oznaczonych i zgodnych z prawem celów. Oznacza to, że nie można ich poddawać dalszemu przetwarzaniu, w nowym celu. W praktyce oznacza to, że cel:
   a) **nie może zostać zatajony**;
   b) **powinien być określony precyzyjnie**.

Ponadto:

c) **o celu zbierania danych trzeba poinformować jeszcze przed zbieraniem danych;**
d) **kategorycznie niedopuszczalne jest uzależnianie zawarcia umowy od równoległego wyrażenie zgody na przetwarzanie danych** w innym celu niż zawarcie umowy, zwłaszcza w celu marketingowym i reklamowym.

[79] Zob. Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 05-09-2013 o sygn. (II SA/Wa 764/13), który zauważa, że kolejność operacji na danych osobowych nie jest przypadkowa. Wskazuje ona na dwa skrajne etapy takich działań. O przetwarzaniu danych można mówić począwszy od zbierania danych, a skończywszy na ich usunięciu. W konsekwencji należy przyjąć, że ochrony danych osobowych, a tym samym stosowaniu przepisów ustawy o ochronie danych osobowych nie można rozciągać poza wskazane ramy czasowe. Zbieranie danych osobowych nie stanowi jeszcze przetwarzania danych osobowych, a tym samym nie jest to czynność objęta działaniem ustawy o ochronie danych osobowych.

[80] R. Aarnio, Ochrona danych w życiu zawodowym…, s. 34.

Od zasady celowości przewidziano kilka wyjątków, które przewidują, że jest dopuszczalne przetwarzanie danych w celu innym niż ten, w którym zostały zebrane w sytuacji kiedy:

- nie narusza to praw i wolności osoby, której dane dotyczą;
- następuje to w celach badań naukowych, dydaktycznych, historycznych lub statystycznych z zachowaniem przepisów z zachowaniem przepisów art. 23 Ustawy (podstawy prawne pozyskiwania danych) oraz art. 25 Ustawy (obowiązki informacyjne).

2) **Zasada prawdziwości (lub merytorycznej poprawności),** która przewiduje, że Administrator danych osobowych powinien zapewnić warunki, aby dane były zgodne z prawdą, pełne (kompletne) i aktualne. Zasad ta nakłada na Administratora danych osobowych konkretne obowiązki. Przede wszystkim powinien on::
   a) każdorazowo oceniać wiarygodność źródła pozyskania danych;
   b) wypracować tryb weryfikacji pozwalający stwierdzić, czy zbierane dane są prawdziwe (jest to zasadne zwłaszcza w sytuacji, kiedy zbiera wrażliwe dane osobowe);
   c) ustalić procedurę uaktualnienia lub sprostowania danych (w takich przypadkach Administrator danych osobowych musi poinformować inne podmioty, którym udostępnił taki zbiór danych, czyli np. przedsiębiorstwa, którym zlecono marketing).
3) **Zasada adekwatności,** która mówi, że Administrator danych osobowych powinien przetwarzać **tylko takie dane i tylko dane o takiej treści, które są dla niego niezbędne ze względu na cel ich zbierania**. Moment zbierania jest więc najważniejszy – oznacza to, że Administrator danych osobowych powinien wcześniej się zastanowić, jakich danych klienta rzeczywiście potrzebuje.
4) **Zasada ograniczenia czasowego**, która często jest łączona z zasadą adekwatności. Oznacza ona, że po osiągnieciu celu (np. wykonanie umowy przez przedsiębiorcę) dane powinny zostać:
   a) usunięte,
   b) zanonimizowane,
   c) lub, jeśli tak nakazują przepisy, przekazane do archiwum państwowego.

Dlatego Administrator danych osobowych powinien stale nadzorować zawartość swoich zbiorów, pod kątem obowiązku usunięcia danych[81].

2.3.2. Obowiązki informacyjne i rektyfikacyjne

Na Administratora danych osobowych został nałożony specjalny obowiązek informacyjny. Istotnym jest, aby osoba zainteresowana (np. klient, beneficjent, pracownik) miał możliwość właściwego ocenienia sytuacji i podjęcia decyzji co do udostępnienia danych. Obowiązek informacyjny musi być wypełniony **bez względu** na to, w jaki sposób dane zostały zebrane, czyli:

1) drogą pisemną,
2) telefonicznie,
3) w kontaktach bezpośrednich.

Nieistotny jest również sposób utrwalenia, czyli to, czy zbiór będzie miał postać papierową czy elektroniczną[82].

Administrator danych osobowych jest zobowiązany poinformować osobę, której to bezpośrednio dotyczy o:

1) adresie siedziby swojego przedsiębiorstwa i jego pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku;
2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców pozyskiwanych danych;
3) prawie dostępu do treści swoich danych oraz ich prawie do ich poprawiania;
4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Nie wolno powyższego obowiązku poinformowania zastępować odesłaniem np. do regulaminu konkursu, jeżeli osoba zainteresowana nie ma możliwości bezpośredniego zapoznania się nim.

Powyższy obowiązek może być spełniony w formie:

- ustnej – w takim wypadku powyższy obowiązek powinien być wykonany jeszcze przed rozpoczęciem zbierania danych (np. w przypadku utrwalenia rozmowy telefonicznej należy poinformować rozmówcę o tym fakcie i poprosić go o zgodę na tę czynność);

[81] M. Krasińska, S. Mizerek (opr.), ABC wybranych zagadnień z ustawy …, s. 11-18.
[82] Zob. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, …, s.493–494.

- pisemnej np. na formularzu zgłoszeniowym lub zakupowym; z punktu widzenia dowodowego jest to forma preferowana.

W przypadku sporu to Administrator danych osobowych będzie musiał udowadniać wypełnienie obowiązku informacyjnego.

Wyłączenie obowiązku informacyjnego jest dozwolone wyłącznie wtedy, kiedy przepis innej ustawy na to zezwala lub osoba której dane dotyczą, wie, który podmiot przetwarza jej dane.

Administrator danych osobowych musi więc przyjąć, że prawie zawsze będzie musiał spełniać obowiązek informacyjny[83].

Studium przypadku:
Przykładowa klauzula informacyjna
Na podstawie art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych informuję, że:
1) administratorem Pani/Pana danych osobowych jest Spółka XXX Sp. z o.o. z siedzibą w Krakowie (00-111), ul. 3 maja 2, lok. 1, zwana dalej Spółką,
2) Pani/Pana dane osobowe będą przetwarzane w celu marketingu produktów i usług Spółki i nie będą udostępniane innym odbiorcom,
3) przysługuje Pani/Panu prawo dostępu do treści swoich danych oraz ich poprawiania,
4) podanie Spółce danych osobowych jest dobrowolne.

Ustawa nakłada na Administratora danych osobowych również **obowiązki rektyfikacyjne**. W przypadku gdy administrator danych zbiera dane osobowe nie bezpośrednio od osoby, której dane dotyczą (np. dokonał zakupu bazy danych osobowych od innego podmiotu), jest zobowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych o:
1) **adresie swojej siedziby i pełnej nazwie**, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku;
2) **celu i zakresie zbierania danych**, a w szczególności o odbiorcach lub kategoriach odbiorców danych;
3) źródle danych;
4) **prawie dostępu do treści swoich danych** oraz prawie do ich poprawiania;
5) **prawie do złożenia sprzeciwu** wobec przetwarzania danych w celach marketingowych lub wobec przekazywania ich innym podmiotom;
6) **prawie do żądania zaprzestania** przetwarzania danych ze względu na szczególną sytuację osoby, której dane są przetwarzane.

Studium przypadku:
Przykładowa klauzula informacyjna:
Zgodnie z art. 25 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2002 r. nr 101, poz. 926 ze zm.) informuję, iż:
1) administratorem Pani/Pana danych osobowych jest XXX Sp. z o.o. z siedzibą w Krakowie (00-111), ul Warszawska 1, zwana dalej Spółką,
2) Pani/Pana dane osobowe będą przetwarzane w celu marketingu produktów i usług Spółki i nie będą udostępniane innym odbiorcom,
3) Spółka pozyskała Pani/Pana dane osobowe od YYY Sp. z o.o. z siedzibą w Warszawie (10-001), ul. Zwycięzców 100,
4) posiada Pani/Pan prawo dostępu do treści swoich danych oraz ich poprawiania,
5) na podstawie art. 32 ust. 1 pkt 7 ustawy o ochronie danych osobowych przysługuje Pani/Panu prawo wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania Pani/Pana danych ze względu na Pani/Pana szczególną sytuację, jak również – na podstawie art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych – ma Pani/Pan prawo wniesienia sprzeciwu wobec przetwarzania Pani/Pana danych w celach marketingowych lub wobec przekazywania ich innemu administratorowi danych.

Studium przypadku:
Niedopuszczalne jest działanie przedsiębiorcy, który kupił dane osobowe od innego podmiotu, a następnie przesłał informację o tym fakcie osobie, której te dane dotyczą, wraz z własną ofertą marketingową[84]. Na początku powinien przesłać informację o zakupie danych osobie, której te dane dotyczą, a dopiero następnie przesłać ofertę marketingową.

[83] M. Krasińska, S. Mizerek (opr.), ABC wybranych zagadnień z ustawy o ochronie danych osobowych, , Warszawa,„Wydawnictwo Sejmowe", 2011, s. 20.

2.4. Przesłanki szczególne pozyskiwania danych osobowych zwykłych

Prawo określa pięć niezależnych i autonomicznych podstaw przetwarzania danych osobowych:

1) **osoba, której dane dotyczą, wyrazi na to zgodę** (art. 23 1. 1. Ustawy);
2) **jest to konieczne do realizacji umowy**, gdy osoba, której dane dotyczą, jest stroną umowy lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą (art. 23 ust. 1. 3 Ustawy)[84];
3) **jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa** (art. 23 ust. 1. 2 Ustawy);
4) **jest to niezbędne do wykonania określonych prawem zadań realizowanych** dla dobra publicznego (art. 23 ust. 1. 4 Ustawy);
5) **jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanyc**h (art. 23 ust. 1. 5). Problematyka zostanie omówiona w podrozdziale Marketing i Reklama**.**

Poniżej zostaną omówione **najczęściej spotykane** w obrocie gospodarczym podstawy prawne pozyskania danych osobowych.

Ad. 1) W zakresie przetwarzania zwykłych danych osobowych zgoda może być wyrażona w dowolny sposób. Oznacza to, że **jest dopuszczalne** uzyskiwanie zgody na ich przetwarzanie w postaci elektronicznej np. poprzez zaznaczenie *check box'a*. Nie jest konieczne opatrywanie zgody na przetwarzanie danych osobowych bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu. Ze względów dowodowych rekomenduje się archiwizowanie uzyskanych zgód na przetwarzanie danych osobowych[85].

Nie wystarczy tylko samo powiadomienie klienta o zamiarze przetwarzania danych i brak jego sprzeciwu[86]. Klient musi **wyraźnie** określić swoje zdanie. Każdorazowe wyrażenie zgody powinno być dobrowolne.

W oświadczeniach, które są zamieszczane w formularzu, **jest niedopuszczalne łączenie** w jednym oświadczeniu:

- zgody na przetwarzanie danych osobowych w celach marketingowych,
- oraz zgody na przesyłanie informacji handlowych drogą elektroniczną.

Oświadczenie klienta musi być tak skonstruowane, aby mógł on zgodzić się na przetwarzanie jego danych dla celów marketingowych, a jednocześnie nie zgodzić się na przesyłanie mu informacji handlowej drogą elektroniczną.

Zgoda na przetwarzanie danych osobowych **nie może** być domniemana lub dorozumiana z oświadczeniem woli o innej treści.

Oznacza to, że wyrażający zgodę musi mieć w momencie jej zawarcia świadomość tego, co kryje się pod tym pojęciem[87].

Udzielenie[88] zgody do przetwarzania danych osobowych w ramach procesu rekrutacyjnego, a tym bardziej w ramach zatrudnienia czy nawiązanej współpracy, nie wymaga wyraźnej zgody kandydata czy pracownika[89]. Niemniej jednak dla celów dowodowych zwłaszcza w procesie rekrutacyjnym przyjęła się praktyka żądania zamieszczenia stosownej klauzuli o wyrażeniu zgody na przetwarzanie danych osobowych kandydata do pracy.

Ad. 2) Przedsiębiorcy zawierają umowy cywilnoprawne (o dzieło, zlecenie, sprzedaży itd.), co jest ściśle związane z przetwarzaniem danych osobowych. Wymogiem ustawowym jest sytuacja, aby przedsiębiorca mógł dostarczyć produkt lub należycie wykonać usługę, jeżeli przetworzy dane osobowe klienta, a bez podania tych danych usługa nie mogłaby zostać świadczona, lub produkt nie spełniałby oczekiwań klienta i umowa nie zostałaby w sposób należyty wykonana.

---

[84] W zakresie pozycji klientów oraz dyskusji w ramach Unii Europejskiej Zob. M. Boni, Nowe ramy ochrony danych osobowych w Unii Europejskiej – ważne wyzwanie dla Polski, dodatek „Monitor Prawniczy", nr. 8 2013

[85] Zob. J. Byrski, Odwołanie zgody na przetwarzanie danych osobowych. Wybrane zagadnienia, dodatek do „Monitor Prawniczy" nr 3, 2011.

[86] Zastrzeżenia te dotyczą tylko danych osobowych zwykłych. Zob. J. Byrski, Odwołanie zgody na przetwarzanie danych osobowych. Wybrane zagadnienia, dodatek do „Monitor Prawniczy" nr 3, 2011, s. 1014.

[87] Wyrok Naczelnego Sądu Administracyjnego z dnia 2003-04-04 o sygn. (II SA 2135/02).

[88] Podstawową zasadą jest dobrowolność udzielenia takiej zgody, szerzej na temat autonomii zob. R. Aarnio, Ochrona danych w życiu zawodowym, [w] *Ochrona danych osobowych, wczoraj, dziś, jutro*, Warszawa 2006,wyd. GIODO, s. 27.

[89] Por. M. Gersdorf, Ochrona danych osobowych kandydata do pracy – problem stale dyskusyjny, (w:) Ochrona danych osobowych, wczoraj, dziś, jutro, Warszawa 2006,wyd. GIODO, s. 107 i n.

Studium przypadku1:
Przedsiębiorca prowadzi szkołę językową. Przygotowanie kursów specjalistycznych jest związane z zebraniem danych osobowych klienta, tak aby dobrać odpowiedni rodzaj kursu.

Studium przypadku 2:
Przedsiębiorca prowadzi zakład krawiecki, w którym szyje garnitury na miarę. Tylko pobranie danych klienta sprawi, że będzie mógł dostarczyć towar, który zamawia klient.

2.5. PRZETWARZANIE DANYCH OSOBOWYCH WRAŻLIWYCH

Wśród danych osobowych wyróżniono również dane o szczególnym charakterze, tzw. dane wrażliwe. Zrobiono to, aby zapewnić im wyższy poziom ochrony[90].

Należy mieć na względzie, że dane wrażliwe muszą **również** spełniać wymogi ogólne dla uznania ich za dane osobowe „zwykłe". W szczególności muszą dotyczyć zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Przetwarzanie danych osobowych wrażliwych **każdorazowo wymaga spełnienia warunków ustawowych** (wymienione w art. 27 ust. 2). Zostaną przedstawione te mające znaczenie dla przedsiębiorców:

1) osoba, której dane dotyczą, **wyrazi zgodę na piśmie na ich przetwarzanie**, chyba że chodzi o usunięcie dotyczących jej danych; zgoda wyrażona w sposób inny niż na piśmie jest nieskuteczna (art. 27 ust. 2, pkt 1);
2) **przepis szczególny innej ustawy zezwala na przetwarzanie takich danych** bez zgody osoby, której te dane dotyczą; takimi ustawami mogą być Ustawa o usługach detektywistycznych[91], Ustawa o zwalczaniu chorób zakaźnych[92] (art. 27 ust. 2, pkt. 2);
3) **jest to niezbędne** (…) **do wykonania statutowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji**, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych (art. 27 ust. 2, pkt. 4);
4) **przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem** (art. 27 ust. 2, pkt 5);
5) **przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób**, a zakres przetwarzanych danych jest określony w ustawie, pracodawca pragnący zebrać takie dane, powinien mieć zawsze na względzie postanowienia ustawy szczególnej (np. o związkach zawodowych, o ustawie o rozwiązaniu umowy o pracę z przyczyn nie leżących w winie pracownika, itd. (art. 27 ust. 2, pkt 6);
6) przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych (art. 27 ust. 2, pkt 7);

Studium przypadku:
Niepubliczny zakład ochrony zdrowia przetwarza dane osobowe wrażliwe swoich pacjentów, dotyczące stanu zdrowia. Jednostka powinna jednak gwarantować właściwe zarządzanie ochroną danych osobowych.

7) przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym (art. 27 ust. 2, pkt 10).

[90] J. Barta, P. Fajgielski, R. Markiewicz, Ochrona danych osobowych: Komentarz ..., s. 548.
[91] Ustawa z dnia 6 lipca 2001 r. o usługach detektywistycznych. Dz.U. 2002 Nr 12 poz. 110.
[92] Zob. Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 19 kwietnia 2013 r. w sprawie ogłoszenia jednolitego tekstu ustawy o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi, Dz.U. 2013 poz. 947.

3. ZARZĄDZANIE BEZPIECZEŃSTWEM DANYCH OSOBOWYCH

mgr Bartosz Mendyk

Prawidłowe zarządzanie systemem bezpieczeństwa w przedsiębiorstwie jest ściśle związane z podziałem kompetencji pomiędzy osobami odpowiedzialnymi za przetwarzanie danych osobowych. Ustawa definiuje podmioty, wskazując ich prawa oraz obowiązki. Dopiero należyte zrozumienie podziału pozwoli przedsiębiorcy wprowadzić odpowiednie procedury oraz podjąć działania.

3.1. ADMINISTRATOR DANYCH OSOBOWYCH

W Ustawie **podmiot administrujący danymi**[93] jest jednym z kluczowych pojęć. **Administratorem danych osobowych** (ADO) jest **organ, jednostka organizacyjna, podmiot lub osoba samodzielnie decydująca o celach i środkach przetwarzania danych osobowych**. To na nim ciąży odpowiedzialność za należyte przetwarzanie danych oraz prowadzenie odpowiedniej polityki bezpieczeństwa informacji. Administratorem danych mogą być podmioty publiczne (organy państwowe, samorządu terytorialnego oraz państwowe i samorządowe jednostki organizacyjne), oraz podmioty prywatne, czyli np.:

- spółki jawne,
- spółki partnerskie,
- spółki komandytowe,
- spółki komandytowo–akcyjne,
- spółki z ograniczoną odpowiedzialnością,
- spółki akcyjne,
- osoby fizyczne prowadzące działalność gospodarczą,
- osoby, które nie prowadzą działalności gospodarczej.

Administratorem danych osobowych **nie będą organy** wcześniej wspomnianych podmiotów, czyli np.:

- zarząd i poszczególni członkowie zarządu,
- rada nadzorcza i członkowie rady nadzorczej,
- dyrektorzy departamentów,
- wspólnicy,
- partnerzy,
- komplementariusze,
- itd.

Uznanie podmiotu za Administratora danych osobowych, przesądza, że musi on wypełniać określone ustawowe obowiązki:

- **informacyjny** wypełniany przy zbieraniu danych osobowych (musi poinformować o fakcie zbierania danych osobę, której dane zbiera);
- **zachowania szczególnej staranności** przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane przetwarza;
- **udzielania** informacji o zakresie przetwarzanych danych osobowych;

[93] Pojęcia „administrujący zbiorem", „administrujący danymi" i „administrator danych" nie są tożsame. Ustawodawca nie używa bowiem w tym samym akcie prawnym różnych określeń dla wskazania tego samego podmiotu. Analizując przedstawione zwroty, należy przyjąć, że na gruncie ustawy o ochronie danych osobowych administratorem danych osobowych jest jedynie ten podmiot, który decyduje o celach i środkach przetwarzania danych (art. 7 pkt 4 ustawy), natomiast administrującym – także taki podmiot, który zarządza, zawiaduje zbiorem danych (art. 50, art. 51, art. 54 ustawy) lub danymi (art. 52 ustawy) w procesie ich przetwarzania, w tym i powierzonego mu w trybie wskazanym w art. 31 tej ustawy. Mimo że co do zasady administrującym zbiorem i administratorem danych. Zob. Orzeczenie Naczelnego Sądu Administracyjnego z dnia 08-09- 2009, o sygn. **(**I OSK 1379/08**).**

- **uzupełniania, uaktualnienia, sprostowania danych**, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, gdy zażąda tego osoba, której dane są przetwarzane;
- **stosowania środków technicznych** (np. szafy zamykane na klucz) **i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych** (zasady wydawania kluczy do pokoi);
- **kontroli które dane, kiedy i przez kogo zostały wprowadzone do zbioru** oraz komu są one przekazywane;
- **prowadzenia ewidencji osób upoważnionych** do przetwarzania danych osobowych;
- **zgłaszania zbioru do rejestracji** Generalnemu Inspektorowi w przypadkach przewidzianych prawem[94].

Studium przypadku:
Przy wejściu do siedziby przedsiębiorstwa X znajduje się portiernia obsługiwana przez pracowników zewnętrznej firmy ochroniarskiej, która prowadzi rejestr osób wchodzących do budynku. Jednakże to przedsiębiorstwo X jest Administratorem danych osobowych, gdyż to ono a nie przedsiębiorstwo ochroniarskie decyduje o celach lub środkach zbierania danych.

Należy mieć na względzie, że:
- w sytuacji, w której **Administrator danych osobowych utraci prawo do przetwarzania danych osobowych** (np. zostanie wycofana zgoda osoby zainteresowanej), **utraci je** również podmiot, któremu powierzono przetwarzanie tych danych;
- **firma outsourcingowa nie jest odbiorcą danych, a zatem nie przejmuje obowiązków administratora** (np. obowiązku informacyjnego)[95].

3.2. ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

Jak wspomniano, to na Administratorze danych osobowych spoczywa obowiązek zapewnienia zgodnej z prawem ochrony danych osobowych. Aby robić to we właściwy sposób, Administrator danych osobowych może wybrać jedną z poniższych opcji:

1) Administrator danych osobowych może powołać Administratora bezpieczeństwa informacji (ABI) – czyli osobę nadzorującą z jego upoważnienia przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych – **poprzez powierzenie zadań z zakresu ochrony danych osobowych swojemu pracownikowi.** Wybór ten wiąże się z przeszkoleniem pracownika w zakresie wymagań przepisów prawa (Ustawa o ochronie danych osobowych, przepisy sektorowe czyli np. aspekty prawa telekomunikacyjnego itd.), ale przede wszystkim z zapoznaniem go z zasadami ochrony, które będzie potrafił wprowadzać w życie. Administrator danych osobowych **może powierzyć** Administratorowi bezpieczeństwa informacji wykonywanie innych obowiązków, **jeżeli nie naruszy to prawidłowego wykonywania zadań.** Powierzenie funkcji Administratora bezpieczeństwa informacji już zatrudnionemu pracownikowi oznacza konieczność zmiany struktury organizacyjnej – chodzi o bezpośrednią podległość Administratora bezpieczeństwa informacji pod kierownika jednostki.
2) Administrator danych osobowych może powołać Administratora bezpieczeństwa informacji **poprzez zawarcie umowy** powierzenia danych (outsourcing), czyli skorzystanie z usług profesjonalisty mającego doświadczenie w pełnieniu obowiązków Administratora bezpieczeństwa informacji. Jest to sytuacja najbardziej optymalna, jakkolwiek wiąże się z dodatkowymi kosztami.
3) Administrator danych osobowych może **nie powoływać** Administratora bezpieczeństwa informacji. Sytuacja ta występuje wtedy, kiedy administrator danych uznaje, że sam jest w stanie spełnić wszystkie obowiązki z zakresu ochrony danych osobowych. Jest to opcja, która wydaje się najtańsza. Wiąże się jednak z koniecznością samodzielnego przeszkolenia się przez przedsiębiorcę w zakresie ochrony danych osobowych, wdrożenia stosownej dokumentacji, przy jednoczesnym prowadzeniu działalności gospodarczej.

Trzeba zatem pamiętać, że kwestia powołania lub niepowołania administratora bezpieczeństwa jest indywidualnym wyborem każdego przedsiębiorcy, który w każdej chwili może zostać zmieniony.

[94] Zob. K. Sadło, Ochrona danych osobowych w organizacjach pozarządowych, Warszawa, wydawnictwo „Fundacja Rozwoju Społeczeństwa Obywatelskiego" 2013, s. 13-14.
[95] Zob. E. Śleszyńska, Administrowanie danymi osobowymi przez zarządców i właścicieli nieruchomości, Chotomów, wydawnictwo „MINI GO", 2009, s. 14.

3.2.1.POWOŁANIE ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

W ustawie wymagania stawiane Administratorowi bezpieczeństwa informacji nominalnie nie są wysokie[96]. Administrator:

1) musi mieć **pełną zdolność do wykonywania czynności prawnych** oraz **korzystać z pełni praw publicznych**[97].
2) nie może być **osobą karaną za przestępstwo z winy umyślnej**.
3) powinien **mieć odpowiednią wiedzę z zakresu ochrony danych osobowych**[98].

Oznacza to, że wbrew opiniom, na które często można natknąć się w internecie, Administrator bezpieczeństwa informacji **nie ma obowiązku** legitymować się wykształceniem wyższym, w szczególności wykształceniem prawniczym.

Od stycznia 2015 roku nastąpiło wzmocnienie funkcji Administratora bezpieczeństwa informacji (nowelizacja Ustawy o ochronie danych osobowych). Konieczność wprowadzenia zmian wynikała m.in. z faktu, że wcześniej w wielu spółkach Administratorzy bezpieczeństwa informacji nie byli odpowiednio wysoko w hierarchii spółki, wobec czego ich wpływ na bezpieczeństwo przetwarzanych danych był nieznaczny. Obecnie wymaga się, aby Administratorzy bezpieczeństwa informacji mieli na tyle znaczącą pozycję w przedsiębiorstwie, aby rzeczywiście mogli wdrażać odpowiednie praktyki.

W przypadku średnich przedsiębiorców, które w ramach swojej działalność przetwarzają znaczną liczbę danych osobowych w kilku siedzibach, administrator danych **może powołać zastępców Administratora bezpieczeństwa informacji.** Muszą oni spełniać takie same warunki, jak sam Administrator bezpieczeństwa informacji.

Jeżeli Administrator danych osobowych skorzysta z przysługującego mu uprawnienia i powoła Administratora bezpieczeństwa informacji, ma 30 dni na zgłoszenie tego faktu do rejestracji Generalnemu Inspektorowi Danych Osobowych. Administratorzy bezpieczeństwa informacji zgłoszeni do rejestracji Generalnego Inspektora są wpisywani do ogólnokrajowego, jawnego rejestru, który jest dostępny na stronach e–GIODO[99].

Administrator danych osobowych, który zgłosił Administratora bezpieczeństwa informacji do rejestracji, jest zobowiązany zgłaszać Generalnemu Inspektorowi każdą zmianę informacji objętych zgłoszeniem powołania Administratora bezpieczeństwa informacji.

Zgłoszenia powołania Administratora bezpieczeństwa informacji oraz zgłoszenia odwołania należy dokonać przy użyciu wzorów zgłoszeń powołania i odwołania.

Wypełnienie wzoru nie jest rzeczą skomplikowaną i przedsiębiorcy nie mają z tym problemów. Ta czynność nie powinna zająć dłużej niż kilka minut. Istotne jest, aby dokładnie czytać pola formularza.

Jeżeli przedsiębiorca dysponuje podpisem elektronicznym, może podpisać formularz za pomocą tego podpisu.

Do najpopularniejszy błędów należy:

- niedokonanie zgłoszenia z użyciem formularza zgłoszenia;
- przesłanie zgłoszenia w formie jego skanu;
- brak podpisu osoby upoważnionej (osób upoważnionych) do reprezentowania administratora danych; często zdarza się, że pracownik, który ma być powołany jako Administrator bezpieczeństwa informacji, z rozpędu podpisuje wniosek zamiast Administratora danych osobowych;
- zgłoszenie powołania na funkcję Administratora bezpieczeństwa informacji kierownika jednostki organizacyjnej (prezesa lub członka zarządu spółki z ograniczoną odpowiedzialnością lub spółki akcyjnej);
- zgłoszenie powołania zastępcy Administratora bezpieczeństwa informacji mimo braku takiego obowiązku[100].
- Odwołanie Administratora Bezpieczeństwa oznacza również, że zostaje on wykreślony z rejestru prowadzonego przez Generalnego Inspektora. Powinno ono nastąpić w przypadku, gdyby Administrator bezpieczeństwa informacji utraci cechy, jakie stawia ustawa, np. został skazany za przestępstwo z winy umyślnej.
- Odwołanie takie również jest związane z wypełnieniem formularza. Dlatego dla skutecznego odwołania trzeba również wypełnić stosowny formularz i przesłać go do Generalnego Inspektora.

---

[96] Por. P. Fajgielski, Pozycja prawna i zadania administratora bezpieczeństwa informacji po nowelizacji ustawy o ochronie danych osobowych , dodatek „Monitor Prawniczy" nr 6, 2015.

[97] P. Fajgielski, Ustawowe wymogi wobec administratora bezpieczeństwa informacji, „Informacja w administracji publicznej", nr 3, 2015.

[98] P. Tobiczyk, *Odpowiednia wiedza z ochrony danych – nowy wymóg*, „Ochrona danych osobowych", nr 4, 2015, s. 23. Z powyższego wynika, że Administratorem Bezpieczeństwa może być wyłącznie osoba fizyczna, spółki i inne jednostki organizacyjne zostały wyłączone.

[99] D. Karwala, *Rejestracja ABI w GIODO – pytania o „trzecią drogę"*, „Ochrona danych osobowych", nr 4, 2015, s. 9.

[100] Informacja GIODO http://www.giodo.gov.pl/1520228/id_art/8527/j/pl/ (dostęp na dzień 08-12-2015).

3.2.2. OBOWIĄZKI ABI

Z punktu widzenia wymogów ustawowych Administrator bezpieczeństwa informacji ma następujące obowiązki:

- prowadzenie rejestru zbiorów danych osobowych;
- opracowywanie dokumentacji z zakresu ochrony danych osobowych (np. Polityka Bezpieczeństwa Informacji);
- rejestracja określonych zbiorów u Generalnego Inspektora;
- nadzorowanie dokumentacji dotyczącej;
- dokonywanie sprawdzeń zgodności przetwarzania danych z przepisami;
- opracowywanie sprawozdań na podstawie dokonanych sprawdzeń.

Administrator bezpieczeństwa informacji (profesjonalista lub wyszkolony pracownik) musi przedstawić Administratorowi danych osobowych **plan sprawdzeń**[101]. Dzięki temu administrator danych będzie wiedział, kiedy i jakie czynności będą w tym zakresie wykonywane. Zanim sprawdzenie zostanie przeprowadzone, Administrator bezpieczeństwa informacji powinien:

1) **opracować plan sprawdzeń**,
2) **przedstawić** Administratorowi danych osobowych **plan sprawdzeń**,
3) **zawiadomić** Administratora danych osobowych **o rozpoczęciu sprawdzenia doraźnego** (przed podjęciem pierwszej czynności w sprawdzeniu),
4) **zawiadomić kierownika jednostki organizacyjnej objętej sprawdzeniem o zakresie planowanych czynności**[102].

Administrator danych osobowych powinien oczekiwać, że w planie sprawdzeń zostaną przedstawione następujące elementy:

1) **przedmiot –** czyli określenie, które elementy polityki bezpieczeństwa będą sprawdzane (np. dokumentacja dotycząca osób upoważnionych do przetwarzania danych itd.);
2) **zakres** – czyli określenie, które zbiory danych będą przedmiotem kontroli;
3) **termin przeprowadzenia poszczególnych sprawdzeń** – czyli ustalenie planu działań tak, żeby administrator danych wiedział, kiedy mogą odbywać się poszczególne sprawdzenia i miał czas na przygotowanie do nich pracowników;
4) **sposób i zakres dokumentowania przetwarzania i zabezpieczania danych osobowych.**

Administrator bezpieczeństwa informacji w planie sprawdzeń uwzględnia:

1) **zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych** – sprawdzenie zbiorów danych jest podstawą dokonania każdego sprawdzenia;
2) **konieczność weryfikacji zgodności przetwarzania danych osobowych z obowiązkami ustawowymi**.

Należy pamiętać, że plan sprawdzeń:

1) **jest przygotowywany** przez Administratora bezpieczeństwa informacji **na okres nie krótszy niż kwartał i nie dłuższy niż rok**;
2) **jest przedstawiany** Administratorowi danych **nie później niż na dwa tygodnie** przed dniem rozpoczęcia okresu objętego planem;
3) **obejmuje co najmniej jedno sprawdzenie**.

Ponadto zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych powinny być objęte sprawdzeniem co najmniej raz na pięć lat[103].

Administrator bezpieczeństwa informacji dokumentuje czynności przeprowadzone w toku sprawdzenia w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania[104].

Dokumentowanie czynności w toku sprawdzenia może polegać na:

- **utrwaleniu danych z systemu informatycznego** służącego do przetwarzania lub zabezpieczania danych osobowych na informatycznym nośniku danych lub dokonaniu wydruku tych danych;

---

[101] Por. szczegółowo G. Sibiga, Sposób i tryb wykonywania zadań ABI na podstawie nowych przepisów wykonawczych, „Informacja w administracji publicznej", nr 3, 2015.

[102] G. Sibiga, Sposób i tryb wykonywania zadań ABI na podstawie nowych przepisów wykonawczych, „Informacja w administracji publicznej" nr 3, 2015, s. 12.

[103] P. Kowalik, Czynności sprawdzające ABI – zgodnie z nowymi obowiązkami, „Informacja w administracji publicznej" nr 2, 2015

[104] Szczegółowe obowiązki nakładają wydane rozporządzenia zob. G. Sibiga, Stan prawny dotyczący ABI kompletny – nowe przepisy wykonawcze do ustawy o ochronie danych osobowych, „Informacja w administracji publicznej", nr 3, 2015.

- **sporządzeniu notatki z czynności** – w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
- **odebraniu wyjaśnień osoby**, której czynności objęto sprawdzeniem – w szczególności tych, które bezpośrednio przetwarzają dane osobowe; ma to tym większe znaczenie, że największe faktyczne zagrożenie w zakresie bezpieczeństwa informacji stanowi czynnik ludzki;
- **sporządzeniu kopii otrzymanego dokumentu**;
- **sporządzeniu kopii obrazu wyświetlonego** na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych (*printscreen*);
- **sporządzeniu kopii zapisów rejestrów systemu informatycznego** służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu – tworzenie kopii zapasowych wszelkich plików powinno już dawno być praktyką przedsiębiorców; w przypadku awarii, zniszczenia systemu etc. szybko można odtworzyć potrzebne rejestry lub zapisy konfiguracji.

Materiały sporządzone w wyniku sprawdzenia mogą być sporządzane w postaci:
- papierowej,
- elektronicznej.

Administrator bezpieczeństwa informacji zawiadamia Administratora danych osobowych o zakresie planowanych czynności w terminie co najmniej **7 dni przed dniem przeprowadzenia czynności**.

Zawiadomienia nie przekazuje się w poniższych przypadkach.

1) **Sprawdzenie doraźne** – czyli wtedy, kiedy niezwłoczne rozpoczęcie sprawdzenia jest niezbędne do przywrócenia stanu zgodnego z prawem lub w przypadku weryfikacji, czy naruszenie faktycznie miało miejsce (np. na podstawie skargi klienta lub artykułu w prasie).
2) **Sprawdzenie doraźne, o którego dokonanie zwrócił się Generalny Inspektor** a wyznaczony przez niego termin sprawdzenia nie pozwala na zawiadomienie o tym administratora danych.

Po zakończeniu sprawdzenia Administrator bezpieczeństwa informacji **przygotowuje sprawozdanie[105].** Jest ono sporządzane w dwóch postaciach:
- elektronicznej,
- papierowej.

Ponieważ Administrator danych osobowych ma obowiązek wiedzieć, w jaki sposób Administrator bezpieczeństwa wypełnia swoje zadanie, ten ostatni musi co najmniej raz do roku przekazywać sprawozdania ze swojej działalności. Do Administratora danych osobowych powinny więc być przedkładane sprawozdania:
- **ze sprawdzenia planowego** – nie później niż w terminie 30 dni od jego zakończenia;
- **ze sprawdzenia doraźnego** – niezwłocznie po jego zakończeniu.

Sprawozdanie ze sprawdzeń, o których dokonanie zwrócił się Generalny Inspektor, należy jemu przedłożyć. Wydaje się jednak naturalne, że zostanie ono przedstawione również Administratorowi danych osobowych.

Dokonanie sprawdzenia ma być własną **wewnętrzną inspekcją** – **audytem,** które powinno być dokonane w celu wykrycia zagrożeń i ich eliminowania. Jeżeli w trakcie audytu zostanie wykryta nieprawidłowość Administrator bezpieczeństwa informacji:
- **zawiadamia administratora danych o nieopracowaniu lub brakach w dokumentacji** przetwarzania danych lub jej elementach; przede wszystkim powinien poinformować, o działaniach podjętych w celu doprowadzenia dokumentacji do wymaganego stanu;
- **przedstawia** administratorowi danych **projekty dokumentów** usuwające stan niezgodności; o ile administrator bezpieczeństwa jest pracownikiem, to powinien bezzwłocznie przedstawić stosowne dokumenty i procedury do wdrożenia (wdrożenia rzeczywistego, a nie formalnego – „na papierze"); o ile jest to podmiot zewnętrzny – podejmuje działania na podstawie przepisów zawartej umowy;
- **zawiadamia** administratora danych **o nieaktualności dokumentacji** oraz może przedstawić mu projekty dokumentów aktualizujących do wdrożenia;

[105] Szerzej o nowej roli Administratora Bezpieczeństwa Informacji por. X. Konarski, Nowe zasady organizacji ochrony danych osobowych, „Prawo Asekuracyjne", nr 2, vol. 83, 2015, s. 85.

- **poucza lub instruuje osobę nieprzestrzegającą zasad określonych** w dokumentacji przetwarzania danych o prawidłowym sposobie ich realizacji.

Powyższe zawiadomienia mogą być zawarte:
- w sprawozdaniu,
- w odrębnym dokumencie, jeżeli dotyczy osoby nieprzestrzegającej zasad określonych w dokumentacji przetwarzania danych.

Wady i zalety powołania Administratora Bezpieczeństwa Informacji

Na koniec warto rozważyć zalety i wady powołania lub niepowołania Administratora bezpieczeństwa informacji. Do pierwszych z nich można zaliczyć:
- **mniejsze obciążenie obowiązkami** – Administrator danych osobowych nie musi zaprzątać sobie głowy przygotowaniem szczegółowej dokumentacji, wdrażaniem polityki bezpieczeństwa itd.; swój czas i energię może poświęcić na prowadzenie działalności gospodarczej; jest to tym bardziej istotne, że zapewnienie bezpieczeństwa nie jest czynnością jednorazową – cały czas zmieniają się przepisy, jedni klienci odchodzą a inni przychodzą, są kupowane nowe systemy komputerowe itd.;
- konieczność rejestracji **mniejszej liczby** zbiorów danych; ustawodawca pozostawił wymóg rejestrowania u Generalnego Inspektora zbiorów zawierających dane osobowe wrażliwe, ale inne zbiory zostaną zwolnione z obowiązku rejestracyjnego, jeżeli został powołany Administrator bezpieczeństwa informacji[106];
- powołanie Administratora bezpieczeństwa spowoduje **mniejszą liczbę** kontroli Generalnego Inspektora, który, w razie powzięcia informacji o ewentualnych naruszeniach przepisów z zakresu danych osobowych, w pierwszej kolejności zwróci się do Administratora bezpieczeństwa informacji o zbadanie sprawy[107];
- wzrost wiarygodności w oczach klientów; dostają oni czytelny znak, że podmiot dba o ochronę ich danych.

Wady powoływania Administratora bezpieczeństwa informacji to:
- zmiany organizacyjne oraz koszty; Administrator bezpieczeństwa informacji musi podlegać bezpośrednio kierownikowi jednostki, dlatego jeżeli do sprawowania funkcji zostanie oddelegowany pracownik przedsiębiorstwa, będą konieczne zmiany organizacyjne; jeżeli natomiast przedsiębiorca zdecyduje się na outsourcing – oznacza to kolejne koszty;
- zapewnienie niezależności i środków dla wykonywania funkcji ABI; pracownicy muszą być gotowi na przyjmowanie uwag i zaleceń odnoszących się do ich działań związanych z przetwarzaniem danych osobowych.

Powołanie ABI sprawi, że:
- Administrator danych osobowych nie **będzie** odpowiadał z tytułu nieumyślnego naruszenia przepisów dotyczących ochrony danych osobowych;
- Administrator bezpieczeństwa informacji może zostać pociągnięty do odpowiedzialności pracowniczej, administracyjnej lub nawet karnej, jeżeli nienależycie zarządza zbiorem danych.

3.3. Administrator systemu informatycznego

Zapewnienie należytego poziomu ochrony systemów informatycznych z każdym rokiem staje się coraz ważniejszym elementem polityki bezpieczeństwa informacji[108]. Do tego stopnia, że na podmiot, który przetwarza dane osobowe w systemie informatycznym, nałożono obowiązek opracowania Instrukcji Zarządzania Systemów Informatycznych[109]. Nakłada ona na Administratora danych osobowych szereg obowiązków począwszy od czuwania nad automatycznym wylogowywaniem z systemu, jeżeli użytkownik urządzenia jest nieaktywny, poprzez utworzenie dla każdego użytkownika

[106] Por. X. Konarski, Organizacja ochrony danych osobowych po nowelizacji, (w:) Ochrona danych osobowych, (red.) Szczygielska , wyd. „Oficyna Prawa Polskiego", Warszawa 2015.

[107] Ma to zapewnić realizację unijnego założenia, że nie tylko kontroli instytucjonalnej w zakresie ochrony danych, sprawowanej Generalnego Inspektora Ochrony Danych Osobowych, ale także kontroli funkcjonalnej, realizowanej w ramach struktury wewnętrznej administratora danych. Zob. P. Fajgielski, Administrator bezpieczeństwa informacji – geneza, stan obecny i perspektywy zmian – „Dodatek Monitora Prawniczego nr 9, 2004.

[108] Do tego stopnia, że wydano rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024 z późn. zm.).

[109] Źródeł tego obowiązku należy upatrywać w art 36 ust. 2 Ustawy. W rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych … (Dz.U. Nr 100 poz. 1024) wskazane są szczegółowe elementy takiej instrukcji.

własnego konta, z poziomu którego może zalogować się do komputera (lub całego systemu), a skończywszy na okresowej zmianie haseł i dbaniu o ich odpowiednią siłę.

Ponieważ Administrator bezpieczeństwa informacji nie zawsze będzie potrafił wypełnić obowiązki związane z zapewnieniem bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych, Administrator danych osobowych może powołać Administratora systemu informatycznego (ASI). Potrzeba powołania tego ostatniego wynika bardziej z praktyki niż z samych przepisów prawa. Zawsze jednak będzie to informatyk, który zajmuje się zarządzaniem systemem informatycznym i odpowiada za jego sprawne działanie.

W hierarchii podmiotu Administrator systemów informatycznych **musi podlegać Administratorowi bezpieczeństwa informacji**, który może delegować na Administratora systemów informatycznych część swoich obowiązków.

Studium przypadku:
Administrator bezpieczeństwa informacji upoważnił nowozatrudnionego pracownika do przetwarzania danych osobowych w określonym zbiorze (np. do obsługi listy mailingowej). Administrator systemów informatycznych przydziela mu login oraz hasło tymczasowe.

Wiedza Administratora systemu informatycznego wykracza zazwyczaj poza znajomość administrowania powierzonym mu oprogramowaniem lub siecią i dotyczy wielu innych kategorii. W zależności od potrzeb Administratora danych osobowych, Administrator systemu informatycznego powinien odznaczać się znajomością:

- elektroniki,
- wielu różnych języków programowania,
- kryptografii i kryptoanalizy.

Z powyższego względów zwłaszcza średni przedsiębiorcy, którzy pracują w przestrzeni internetowej, wyodrębniają nawet administratorów:

- baz danych,
- serwerów,
- sieci,
- poszczególnych usług typu fora dyskusyjne, czaty itp.

3.3.1. POWODY POWOŁYWANIA ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH

Można wyodrębnić dwie przyczyny, które sprawiają, że powołanie administratora systemu informacji staje się praktycznie niezbędne.

1) Wzrost informatyzacji przedsiębiorstw.

O tej tendencji świadczą następujące dane:

- wartość przychodów sektora IT w Polsce w 2011 r. wyniosła 31,3 mld PLN[110];
- sektor usług IT daje zatrudnienie na poziomie ok. 400 tys. osób[111];
- w 2013 r. sprzedaż komputerów w Polsce wyniosła 5 mln sztuk[112].

2) Wzrost zagrożeń związanych ze złośliwym oprogramowaniem.

O wzroście zagrożenia świadczą:

- straty powstałe w wyniku działalności cyberprzestępców na świecie wyniosły w 2011 r. 388 mld USD;
- 69% dorosłych użytkowników internetu przynajmniej raz w życiu było ofiarami przestępczości internetowej (44 proc. w 2011 r.);
- 41% użytkowników nie ma aktualnego oprogramowania zabezpieczającego systemy komputerowe[113].

Zagrożenia nie dotyczą już tylko instalacji wirusów, ale i *phishingu* (wyłudzenia poufnych informacji)[114].

---

[110] Raport Polskiej Agencji Informacji i Inwestycji Zagranicznych, Sektor Technologii Informatycznych w Polsce, dostępny na stronie paiz.gov.pl

[111] Zob. Raport przedsiębiorstwa PMR, Rynek IT w Polsce 2014 Prognozy rozwoju na lata 2014-2018, 2014.

[112] Na marginesie warto zauważyć, że **małe przedsiębiorstwa stanowią 90% polskich firm IT,** Por. raport PMR, *Rynek IT w Polsce 2014*...

[113] Symantec Cybercrime Report 2011, http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrime/assets/downloads/en-us/NCR-DataSheet.pdf (dostęp: 24 kwietnia 2012 r.).

[114] M. Grzelak, K. Liedel, Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski– zarys problemu, „Bezpieczeństwo Narodowe" nr 22, 2012, s. 126.

3.3.2. ZADANIA I OBOWIĄZKI ASI

Ponieważ w prawie nie ma zdefiniowanego stanowiska Administratora systemów informatycznych, a potrzeba ich powołania wynika przede wszystkim z praktyki, w każdym przedsiębiorstwie ma on zakres obowiązków, który jest ściśle dostosowany do określonych potrzeb firmy.

Do najważniejszych obowiązków administratora systemu informatycznego należy:

- zapewnienie bezpieczeństwa systemu informatycznego,
- zapewnienie ciągłości działania systemu,
- zapewnienie sprawnego realizowania procedur tworzenia kopii zapasowych.

Powyższe jest realizowane poprzez konkretne działania:

- ogólny nadzór nad prawidłowym przebiegiem procedury sporządzania kopii zapasowych przetwarzanych zbiorów danych osobowych oraz kopii systemów informatycznych używanych do ich przetwarzania – kopie są tworzone zazwyczaj w sposób automatyczny, a rolą Administratora systemów informatycznych jest nadzór nad tym procesem; dane powinny być zapisywane na serwerze oraz zewnętrznym dysku twardym znajdującym się w siedzibie przedsiębiorcy;
- wdrożenie procedury oraz oprogramowania, które chronią dane osobowe przed nieuprawnionym dostępem, zmianami, usunięciem lub uszkodzeniem oraz szkodliwym oprogramowaniem – użyte programy antywirusowe (firewalle i inne) mają chronić przed programami zawierającymi złośliwy kod (wirusy), tzw. koniami trojańskimi oraz atakami hakerów;
- nadzór, aby pracownicy przetwarzający dane osobowe bez wiedzy Administratora systemów informatycznych nie pobierali oraz nie instalowali na komputerach jakichkolwiek programów służących do przetwarzania danych osobowych;
- pouczenie osób przetwarzających dane osobowe, aby nie używały nośników informacji niepochodzących ze źródeł Administratora systemów informatycznych;
- instalowanie wygaszaczy ekranów na stanowiskach, na których są przetwarzane dane osobowe – zastosowanie mechanizmu automatycznej blokady dostępu do systemu informatycznego;
- przeglądanie i konserwacje systemów oraz nośników informacji służących do przetwarzania danych;
- dbałość, aby system spełniał wymogi rozporządzenia[115] (np. system powinien rejestrować datę wprowadzenia danych do systemu).

Dodatkowo do dobrych praktyk należy prowadzenie tzw. „Dziennika Administratora systemów informatycznych", czyli rejestrowania bieżących zdarzeń mających miejsce w systemie informatycznym i pośrednio lub bezpośrednio dotyczą danych osobowych.

Administrator danych osobowych nie musi zatrudniać nowej osoby na stanowisko Administratora systemów informatycznych. Byłoby to niecelowe, zwłaszcza dla mniejszych przedsiębiorstw, ze względu na zbyt duże koszty. Ale nawet średni przedsiębiorcy powinni – podobnie jak w przypadku powołania Administratora bezpieczeństwa informacji – przemyśleć, czy taniej i efektywniej jest przeszkolić informatyka już zatrudnionego w przedsiębiorstwie, czy wynająć profesjonalistę zewnętrznego.

[115] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024 z późn. zm.).

4. SYSTEM ZABEZPIECZEŃ DANYCH OSOBOWYCH

dr Łukasz Kister

Zabezpieczenie danych osobowych pozostających w dyspozycji firmy jest kolejnym krokiem w procesie zbudowania całościowego i poprawnego systemu ich ochrony. Choć nie jest to element najważniejszy jeżeli patrzymy na ten system przez pryzmat jego istoty – ochrona osób przed bezprawnym wykorzystaniem ich danych osobowych, to staje się takim na poziomie przetwarzania danych osobowych w praktyce codziennej działalności.

Jak już zostało to wskazane w poprzednim rozdziale, najważniejszą rolę w systemie ochrony danych osobowych odgrywa **Administrator danych osobowych** (ADO). Odpowiada on za całość działań podejmowanych w stosunku do danych osobowych, w tym także w zakresie ich **zabezpieczenia przed działaniami niepożądanymi**:

- udostępnieniem osobom nieupoważnionym;
- zabraniem przez osobę nieuprawnioną;
- przetwarzaniem z naruszeniem ustawy;
- nieuprawnioną zmianą[116];
- utratą, uszkodzeniem lub zniszczeniem (art. 36 ust. 1).

W tym celu Administrator danych osobowych ma obowiązek zastosowania środków technicznych i organizacyjnych, otrzymując w tym względzie prawie całkowitą dowolność, zwłaszcza w obszarze doboru rozwiązań technicznych. Generalnie przyjmuje się, że system zabezpieczeń stworzony zgodnie z wymogami Ustawy musi spełniać takie podstawowe cele, jak:

1) **rozliczalność** – właściwość systemu zapewniająca, że działania podmiotu posiadającego dostęp do danych osobowych mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (§2 pkt 7);
2) **integralność danych** – właściwość systemu zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany (§2 pkt 8);
3) **poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom (§2 pkt 10); oraz dodatkowo – nie wymieniony wprost w Rozporządzeniu ws. warunków technicznych – wymóg decydujący o normalnym funkcjonowaniu organizacji, czyli:
4) **dostępność danych** – właściwość systemu zapewniająca niezakłócony dostęp do danych osobowych, ograniczony wyłącznie wymogami rozliczalności, integralności i poufności[117].

W niniejszym rozdziale zostaną przedstawione najważniejsze wskazane w Ustawie i Rozporządzeniu ws. warunków technicznych wymagania w zakresie zabezpieczenia procesu przetwarzania danych osobowych, wraz z próbą ich praktycznego omówienia. W szczególności poniżej znajdą się te zabezpieczenia, których obowiązek stosowania jest nienaruszalny z uwagi na ich prawne umocowanie. W bardzo wielu przypadkach specyfika działalności Administratora danych osobowych będzie wymagała także innych systemów ochrony przetwarzanych danych osobowych.

4.1. BEZPIECZEŃSTWO OSOBOWE

Powszechnie przyjmuje się, że największym zagrożeniem dla bezpieczeństwa jakichkolwiek zasobów informacyjnych jest człowiek. To jego działania lub zaniechania stanowią przyczynę ponad **80% wszelkich sytuacji kryzysowych**[118]. Żadne nawet najwyższej klasy zabezpieczenia techniczne czy informatyczne nie są w stanie sprostać ludzkiej pomysłowości[119]. Stąd tak wielkie znaczenie dla praktycznej sprawności systemu ochrony danych osobowych ma obszar, tzw. „bezpieczeństwa osobowego". Można nawet przyjąć, że jest on warunkiem decydującym o jego skuteczności.

Obszar procedur „bezpieczeństwa osobowego" powinien składać się z wielu bardzo różnorodnych elementów, których wspólnym celem jest osiągnięcie faktycznego ograniczenia możliwości wystąpienia **błędu ludzkiego** lub zdolności do minimalizacji jego skutków. Nie powinny to być wyłącznie procedury nakazów i zakazów, ale kompleksowe podejście

---

[116] W ustawie nie występuje wskazanie na „nieuprawnioną" zmianę. Niemniej jednak w praktyce możemy mówić, że tylko taka jest działaniem niepożądanym, gdyż „zmiana" danych osobowych, jest jednym z elementów normalnego procesu przetwarzania, np. aktualizacja.

[117] Polska Norma: PN-I-13335-1/1999, Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych, PKN: Warszawa, 1999.

[118] Patrz: K. Mitnick, W. Simon: *Sztuka podstępu. Łamałem ludzi nie hasła*, Gliwice: Helion, 2003.

[119] Patrz: Ł. Kister: *Wikiekcja dla biznesu*, „Bussines Security Magazine", nr 1, 2011. s. 12-13.

do całej aktywności pracownika[120] i jego roli w organizacji – od momentu pierwszego kontaktu z firmą[121], aż do chwili ustania wzajemnych zobowiązań.

Reasumując, należy jednoznacznie stwierdzić, że „bezpieczeństwo osobowe" jest **najtańszym i najprostszym z zabezpieczeń**, a jednocześnie gwarantującym najwyższą skuteczność całego systemu ochrony danych osobowych. Jego pomijanie lub bagatelizowanie skutkuje coraz częściej występującymi sytuacjami kryzysowymi i wyciekami danych osobowych.

4.1.1. SYSTEM UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

Administratora danych osobowych przed dopuszczeniem pracownika do możliwości przetwarzania danych osobowych musi nadać mu „**Upoważnienie do przetwarzania danych osobowych**" (art. 37).

Upoważnienie do przetwarzania danych osobowych nadaje się każdej osobie, która może mieć dostęp do danych osobowych, **bez względu na**:

1) **rodzaj danych osobowych** – „zwykłe" czy „wrażliwe";
2) **sposób prowadzenia zbioru danych osobowych** – kartoteka papierowa czy system informatyczny;
3) **zakres dostępu do danych osobowych** – zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie czy usuwanie;
4) **rodzaj dostępu** – jednorazowy czy stały;
5) **rodzaj stosunku prawnego łączącego osobę z Administratorem danych osobowych** – umowa o pracę, umowa cywilno-prawna, staż, praktyka czy wolontariat[122].

Studium przypadku:
Upoważnienie do przetwarzania danych osobowych należy nadać studentowi, który na podstawie jednorazowej umowy-zlecenia prowadzi marketing bezpośredni produktów firmowych, zapisując wyłącznie dane kontaktowe zainteresowanych nimi klientów w papierowym rejestrze, który następnie przekazuje bezpośrednio do działu sprzedaży.

Ponadto istnienia bezwzględnego „upoważnienia" nie można wywodzić z faktu wykonywania przez osobę **określonego zawodu**. Nawet wtedy, kiedy gdy regulująca go ustawa wskazuje na konieczność lub możliwość przetwarzania danych osobowych, np. lekarz, adwokat czy pracownik ochrony[123].

Najważniejszym celem nadawania „Upoważnień do przetwarzania danych osobowych" jest wypełnienie kluczowego standardu dostępu do informacji chronionych – zasady „wiedzy koniecznej" (ang. „*need to know*"). Oznacza to, że dla każdej osoby Administrator danych osobowych wyznacza **indywidualny zakres dostępu** do danych osobowych, dostosowany do potrzeb na zajmowanym stanowisku pracy:

1) wskazanie „zbioru danych osobowych" lub jego części;
2) szczegółowe określenie dopuszczalnych czynności na danych osobowych, tj. zbieranie, przeglądanie, aktualizowanie, kopiowanie, udostępnianie, anonimizowanie, usuwanie, itp.;
3) wyznaczenie czasu obowiązywania.

Studium przypadku:
Pracownik sekretariatu adresujący korespondencję kadrowo-płacową kierowaną do Zakładu Ubezpieczeń Społecznych lub Urzędu Skarbowego nie powinien mieć nadanego „upoważnienia" do dostępu do zbioru „kadrowo-płacowego", ani tym bardziej faktycznego dostępu do jego zawartości.

Co do zasady „Upoważnienia do przetwarzania danych osobowych" winien nadawać **osobiście** Administrator danych osobowych. Niemniej jednak nie istnieje przeszkoda prawna, która pozbawiała by możliwości **delegowania tego uprawnienia** na inną osobę. Umocowanie wybranej osoby musi jednak zostać przeprowadzone z zachowaniem wszelkich zasad nadawania pełnomocnictw, czyli:

- jednoznacznym wskazaniem osoby uprawnionej;
- precyzyjnym określeniem celu i zakresu uprawnienia;
- sporządzeniem na piśmie.

---

[120] W naszym przypadku przez termin „pracownik" rozumieć będziemy wszelkie osoby wykonujące pracę dla lub na rzecz firmy, bez względu na rodzaj łączącego strony stosunku prawnego.

[121] Patrz: Ł. Kister: Proces rekrutacji jako czynnik bezpieczeństwa informacyjnego organizacji, „Ochrona mienia i informacji", nr 3, 2010.

[122] A. Drozd: *Ustawa o ochronie* …, s. 265-266.

[123] W tym miejscu należy zauważyć, że takie podejście może w przyszłości ulec zmianie. Przykładem może być tutaj orzeczenie Naczelnego Sądu Administracyjnego w sprawie dostępu Prokuratorów, które uznaje, że ustawowe zakres czynności prokuratorskich w postępowaniu karnym zezwala niejako „z urzędu" na przetwarzanie danych osobowych, zwalniając z odrębnego upoważnienia, (NSA, I OSK 1279/05).

Ponadto uprawnienie do ich wydawania w imieniu Administratora danych osobowych **nie może być domniemane**, tj. nie można go wywieść z faktu posiadania innych pełnomocnictw czy piastowania jakiegokolwiek stanowiska[124].

Studium przypadku:
Posiadane przez kierownika komórki kadrowo-płacowej pełnomocnictwa zarządu spółki do zawierania umów o pracę, nie upoważnia do wydawania „upoważnień do przetwarzania danych osobowych" dla pracowników spółki.

Ustawodawca nie określił wprost treści i formy, jaką ma przybrać „Upoważnienie", niemniej jednak powszechnie uznaje się, że wymagana w tym względzie jest postać pisemna[125].

Rozwiązanie umowy z pracownikiem – bez względu na jej rodzaj – oznacza jednocześnie natychmiastową **utratę uprawnień** do przetwarzania danych osobowych.

W praktyce należy to fizycznie zagwarantować poprzez niezwłoczne:
- odebranie prawa swobodnego dostępu do pomieszczeń, w których przetwarzane są dane osobowe;
- zablokowanie możliwości dostępu do systemu informatycznego, w tym do służbowej poczty e-mail;
- odebranie wszystkich służbowych komputerowych nośników informacji, na których mogą znajdować się dane osobowe;
- rozliczenie całej posiadanej przez pracownika dokumentacji mogącej zawierać dane osobowe.

Nie ma konieczności, aby Administrator danych osobowych wydawał dodatkową decyzję o cofnięciu wydanego uprzednio „Upoważnienia do przetwarzania danych osobowych" w związku z zakończeniem współpracy. „Upoważnień do przetwarzania danych osobowych" **nie wydaje się**:
- pracownikom, którzy w sposób przypadkowy – nie wynikający z ich obowiązków służbowych, mogą uzyskać dostęp do danych osobowych (np. personel sprzątający);
- funkcjonariuszom publicznym, którym z racji nadanych im przez ustawę uprawnień, udzielamy dostępu do posiadanych „zbiorów danych osobowych" (np. kontrolerzy skarbowi);
- inspektorom Generalnego Inspektora Ochrony Danych Osobowych, którzy wykonują swoje obowiązki kontrolne.

4.1.2. ZOBOWIĄZANIE DO ZACHOWANIA POUFNOŚCI

Kluczowym elementem systemu bezpieczeństwa osobowego w procesie przetwarzania danych osobowych jest **obowiązek zachowania tajemnicy** przez osoby, którym nadano „Upoważnienia do przetwarzania danych osobowych". Ustawodawca określił tym samym odrębną „tajemnicę funkcyjną"[126], której przedmiotem ochrony są:
- dane osobowe;
- sposoby zabezpieczenia danych osobowych (art. 39 ust. 2).

Należy w tym miejscu wskazać na kilka kluczowych **determinantów** tej tajemnicy, które warunkują praktyczne jej stosowanie i respektowanie.

Po pierwsze, obowiązuje ona wyłącznie **określone osoby**, tj. te, które zostały „upoważnione do przetwarzania danych osobowych" przez Administratora danych osobowych. Bez znaczenia jest tu rodzaj łączącego strony stosunku prawnego[127].

Po drugie, obejmuje **wszelkie rodzaje danych osobowych** – „zwykłe" i „wrażliwe", bez znaczenia na sposób ich przetwarzania.

Po trzecie, dotyczy także danych osobowych, które **nie zostały** uwzględnione w zakresie nadanego „Upoważnienia", a mimo tego zostały osobie udostępnione[128].

Po czwarte. Obowiązek zachowania tajemnicy trwa **bezterminowo**, również po ustaniu „Upoważnienia", czy stosunku prawnego łączącego osobę z Administratorem danych osobowych[129].

Po piąte, zakresem tajemnicy są objęte, poza samymi „danymi osobowymi", także wszelkie informacje wskazujące na zastosowane przez Administratora danych osobowych **zabezpieczenia** procesu przetwarzania danych osobowych. Będzie to dotyczyło nie tylko „Polityki bezpieczeństwa danych osobowych", ale również wszelkich innych procedur, instrukcji, regulaminów, itp.[130].

---

124 P. Barta, P. Litwiński: *Ustawa o ochronie* …, s. 418.

125 Patrz: P. Fajgielski: *Obowiązki związane z zabezpieczeniem danych osobowych*, (w:) P. Fajgielski (red.): *Ochrona danych* …, s. 149; A. Drozd: *Ustawa o ochronie* …, s. 266. Zakres i forma „Upoważnienia do przetwarzania danych osobowych" zostanie szczegółowo omówiona w kolejnym Rozdziale.

126 Przez niektórych wskazywana jako „tajemnica zawodowa" – P. Fajgielski: *Obowiązki związane z zabezpieczeniem* …, s. 149; choć w zasadzie nie jest związana z żadnym zawodem, a właśnie z funkcją i jej zakresem obowiązków – J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 637.

127 P. Fajgielski: Obowiązki związane z zabezpieczeniem …, s. 151.

128 A. Drozd: *Zabezpieczenie danych osobowych*, Wrocław: Presscom, 2008, s. 27.

129 A. Drozd: *Ustawa o ochronie* …, s. 272.

130 Por.: Ł. Kister: *Polityka bezpieczeństwa danych osobowych*, „Ochrona Mienia i Informacji", nr 6, 2009, s. 16.

Studium przypadku:
Pracownik zewnętrznego serwisu informatycznego, któremu Administrator danych osobowych nadał „Upoważnienie do przetwarzania danych osobowych", w związku z koniecznością obsługi aplikacji kadrowo-płacowej, jest zobowiązany do zachowania w tajemnicy nie tylko poznanych w ten sposób informacji osobowych, ale również wszelkich zasad bezpieczeństwa tej aplikacji i całego systemu informatycznego firmy.
Obowiązek poufności nie ustanie nawet w chwili zakończenia współpracy, a nawet w sytuacji, gdy informatyk ten posiądzie wiedzę o upadłości swojego byłego już klienta.

Ustawa nie określa, w jaki sposób osoba, która otrzymała „Upoważnienie do przetwarzania danych osobowych", ma potwierdzić swoje zobowiązanie do zachowania poufności. W piśmiennictwie wskazuje się, że podobnie jak w przypadku samego „Upoważnienia", winno to być pisemne „oświadczenie"[131]. Nie ma przeszkód, aby takie „oświadczenie woli" znalazło się w szczegółowej umowie regulującej szersze kwestie nieuczciwej konkurencji i poufności[132], zawartej pomiędzy pracodawcą, a pracownikiem, np. umowa o zakazie konkurencji w trakcie trwania stosunku pracy[133].

4.1.3. SZKOLENIA PRACOWNIKÓW

Pomimo braku jednoznacznego ustawowego nakazu, powszechnie przyjmuje się, że nadanie osobie „Upoważnienia do przetwarzania danych osobowych" oraz odebranie od niej „Oświadczenia woli – zobowiązania do zachowania poufności" powinno zostać poprzedzone **obowiązkowym szkoleniem**[134].

Tematyka takiego szkolenia powinna obejmować w szczególności:

- aktualny system prawny ochrony danych osobowych w Polsce i UE;
- wewnętrzne regulacje związane z bezpieczeństwem informacji w firmie, w szczególności te, które odnoszą się do przetwarzania danych osobowych;
- zagrożenia dla bezpieczeństwa przetwarzanych danych osobowych, w odniesieniu do specyfiki działalności firmy;
- role i zadania poszczególnych osób odpowiedzialnych za ochronę danych osobowych;
- zasady udzielania dostępu do zbiorów danych osobowych;
- prawa i obowiązki osób upoważnionych do dostępu do danych osobowych;
- zasady przetwarzania danych osobowych w systemach informatycznych;
- procedury postępowania w sytuacji naruszenia bezpieczeństwa przetwarzanych danych osobowych;
- odpowiedzialność dyscyplinarna i karna za nieprzestrzeganie zasad ochrony danych osobowych.

Zapoznanie pracownika z aktami prawnymi – powszechnymi i zakładowymi – musi przybrać formę udostępnienia tych dokumentów na czas niezbędny do osobistego zapoznania z ich treścią.

Szkolenie, o którym jest mowa wyżej, przygotowuje Administrator bezpieczeństwa informacji lub inna osoba wyznaczona do nadzoru nad obszarem ochrony danych osobowych w firmie. Może ono być przeprowadzane w formie **tradycyjnego wykładu** czy konwersatorium, ale może także przybrać formę **kursu e-learningowego**. Ważne jest jednak, by udział w takim szkoleniu był potwierdzony własnoręcznym podpisem uczestnika lub innym niezaprzeczalnym dowodem jego odbycia, np. indywidualne konto w internetowym systemie szkoleniowym.

Zupełnie należy natomiast odrzucić spotykane dosyć często sytuacje, w których szkolenie polega wyłącznie na zapoznaniu się osoby z aktami prawnymi, gdyż bez jakiegokolwiek ich objaśnienia, czy odniesienia do specyfiki przetwarzania jest ono całkowicie nieskuteczne.

Studium przypadku:
Pracodawca ma znikome środki egzekucji od pracownika odpowiedzialności za wyrzucenie przez niego do kosza na śmieci niepotrzebnych już wydruków z danymi osobowymi klientów, jeżeli nie poinformował go wcześniej o obowiązku niszczenia dokumentacji zawierającej takie informacje w niszczarce.

Szkolenia te powinny być uzupełniane indywidualnymi **szkoleniami stanowiskowymi**, przeprowadzanymi przez bezpośrednich przełożonych. Pozwalają one zdobytą ogólną wiedzę przełożyć na szczególną specyfikę własnego zakresu zadań. Jednocześnie ważnym elementem utrzymania wysokich kwalifikacji pracowników w zakresie ochrony danych oso-

[131] Zakres i forma „Oświadczenia woli – Zobowiązania do zachowania poufności" zostanie szczegółowo omówiona w kolejnym Rozdziale.
[132] Patrz: Ustawa z dnia 26 czerwca 1974 roku – *Kodeks pracy*, (Dz.U. nr 24, poz. 141, z późn. zm) – art. 101[1].
[133] Szerzej: R. Sadlik: Zakaz konkurencji jako sposób ochrony interesów pracodawcy, Warszawa: Difin, 2007, s. 9-30.
[134] Por.: P. Fajgielski: *Obowiązki związane z zabezpieczeniem* …, s. 151; A. Krasuski, D. Skolimowska: *Dane osobowe* …, s. 203.

bowych jest to, by swoją wiedzę i umiejętności podnosili w sposób systematyczny, tj. szkolenia powinny być powtarzane co najmniej **raz w roku** oraz w sytuacji:

- znaczących zmian ustawowych;
- zmiany wewnętrznego systemu zarządzania bezpieczeństwem danych osobowych;
- zmian organizacyjnych wpływających na sposób przetwarzania danych osobowych;
- zaistnienia sytuacji kryzysowej naruszającej bezpieczeństwo przetwarzanych danych osobowych.

Na koniec należy pamiętać, by także osoby odpowiedzialne za zarządzanie przetwarzaniem i ochroną danych osobowych – Administrator danych osobowych, Administrator bezpieczeństwa informacji oraz Administrator systemu informatycznego, regularnie podnosili swoje **kwalifikacje specjalistyczne**.

4.2. BEZPIECZEŃSTWO FIZYCZNE

Dane osobowe są przykładem dobra niematerialnego, którego istotą jest przede wszystkim zawartość informacyjna, a nie fizyczny obiekt. To ich treść wyznacza obowiązek ochrony, jej zakres i odpowiedzialność. Niemniej jednak musimy pamiętać o tym, że **proces przetwarzania danych osobowych dokonuje się poprzez ich materialne nośniki – papierowe czy elektroniczne**. Stąd ochrona danych osobowych przed działaniami niepożądanymi musi uwzględniać także kwestie fizycznego dostępu do tych nośników. Niestety prawie zupełne pominięcie przez ustawodawcę kwestii „bezpieczeństwa fizycznego" powoduje, że w większości publikacji książkowych kwestia ta jest nadmiernie bagatelizowana. W praktyce można więc spotkać się z takim podejściem, że Administrator danych osobowych nie ma żadnych obowiązków w tym zakresie. Nic bardziej mylnego. Wystarczy przypomnieć sobie nakazy „**szczególnej staranności**" (art. 26), oraz „**odpowiedniej ochrony**" (art. 36 ust. 1), które nie mają ograniczenia rzeczowego. Dotyczą on bezwzględnego **obowiązku zabezpieczenia przetwarzanych danych osobowych w odniesieniu do wszystkich rodzajów zagrożeń**, dając Administratorowi danych osobowych swobodę **wyłącznie** w kwestii doboru środków bezpieczeństwa[135].

Zabezpieczenia, a przede wszystkim ich poziom, należy dobierać opierając się na zasadzie **adekwatności** w stosunku do istniejących zagrożeń, wynikających z:

- specyfiki działalności firmy;
- lokalizacji „strefy przetwarzania";
- kategorii przetwarzanych danych osobowych, tj. zwykłych czy wrażliwych;
- sposobu przetwarzania danych osobowych, tj. wielkości zbiorów tradycyjnych oraz budowy systemu informatycznego.

4.2.1. WYZNACZENIE STREFY PRZETWARZANIA DANYCH OSOBOWYCH

Podstawowym środkiem bezpieczeństwa decydującym o skuteczności ochrony przetwarzanych danych osobowych przed dostępem do nich osób nieuprawnionych jest wyznaczenie miejsc podlegających **obowiązkowemu nadzorowi**. Administrator danych osobowych zobowiązany jest do określenia „**strefy przetwarzania**", tj. obszaru administracyjnego:

- w których jest możliwy bezpośredni lub pośredni dostęp do danych osobowych;
- dostępnego w sposób nieograniczony wyłącznie dla osób posiadających „Upoważnienia do przetwarzania danych osobowych" (pkt I).

W skład „obszaru przetwarzania" powinny więc wejść **wszystkie pomieszczenia** biurowe i techniczne, w których są przetwarzane dane osobowe. Nie są to jednak tylko te pomieszczenia, w których wykonuje się bieżące operacje na danych osobowych, tj. stanowiska pracy biurowej, ale także te miejsca, gdzie są przechowywane nośniki tych danych osobowych, np. szafy dokumentacji papierowej, jak również te odpowiadające za funkcjonowanie systemu informatycznego, np. serwerownia[136]. W związku z koniecznością zapewnienia dostępu do „strefy przetwarzania", ograniczonego wyłącznie do osób mających „Upoważnienia do przetwarzania danych osobowych" lub pod ich bezpośrednim nadzorem, jest zasadnym, żeby **nie uogólniać jej granic** do całego budynku biurowego. Takie pozornie upraszczające podejście może spowodować konieczność zabezpieczenia także tych pomieszczeń, w których nie jest realizowany proces przetwarzania danych osobowych, tj. pokoi socjalnych, łazienek czy całych ciągów komunikacyjnych.

[135] A. Drozd: Zabezpieczenie danych …, s. 44.
[136] A. Drozd: *Ustawa o ochronie* …, s. 252-253.

Studium przypadku:
Przedsiębiorca prowadzący aptekę nie powinien wskazywać całego jej pomieszczenia przeznaczonego do sprzedaży leków jako „obszaru przetwarzania", gdyż w części dostępnej dla klientów nie są przetwarzane dane osobowe, a ponadto nie ma on nad całością bezpośredniego nadzoru.

W praktyce przyjmuje się ponadto, że w „strefie przetwarzania" powinny zostać dodatkowo wydzielone pomieszczenia, których znaczenie dla procesu przetwarzania danych osobowych ma charakter krytyczny – tzw. „**strefa specjalna**". W jej składzie powinny się znaleźć:

- pomieszczenia serwerowni – głównej i zapasowej;
- pomieszczenia specjalnych urządzeń sieciowych;
- magazyn wycofanych z eksploatacji komputerowych nośników danych i urządzeń systemu informatycznego;
- pomieszczenie systemu wydruków zbiorowych;
- miejsce przechowywania kopii bezpieczeństwa systemu informatycznego;
- miejsce przechowywania akt osobowych pracowników;
- pomieszczenie archiwum lub inne miejsce przeznaczone do przechowywania tradycyjnej dokumentacji zawierającej dane osobowe[137].

4.2.2. ZABEZPIECZENIE POMIESZCZEŃ BIUROWYCH

Pierwszym z zabezpieczeń jest **system kontroli dostępu**, który, w odniesieniu do wskazanego uprzednio obowiązku zabezpieczenia „strefy przetwarzania" przed dostępem osób nieuprawnionych, uchodzi w istocie za najważniejszy. Zasadniczo przyjmuje się, że obiekt biurowy powinien mieć, o ile jest to fizycznie możliwe, wydzielone **obszary**: **ogólnodostępny i kontrolowany**, a przejście między nimi powinno być właściwie nadzorowane. Nie ma konieczności stosowania elektronicznego systemu kontroli dostępu, wystarczy właściwie prowadzona „książka wejść i wyjść"[138]. Natomiast nieograniczony dostęp do pomieszczeń biurowych mogą mieć wyłącznie osoby „Upoważnione do przetwarzania danych osobowych", wykonujące w nich swoje obowiązki służbowe. Na nich też ciąży obowiązek kontroli dostępu do tych pomieszczeń, tj. inne osoby mogą w nich przebywać **tylko pod nadzorem** (pkt I.2.).

Studium przypadku:
Pracownik marketingu przyjmując klienta, nie może pozostawić go samego w pomieszczeniu biurowym, w sytuacji konieczności udania się do magazynu po materiały reklamowe. Nie może tego zrobić nawet wtedy, kiedy stanowisko komputerowe jest wyłączone, a dokumentacja papierowa umieszczona w zamkniętej szafie.

Z kontrolą dostępu jest nieodzownie związany problem **zarządzania kluczami**. Powinny być one dostępne wyłącznie dla osób pracujących w konkretnym pomieszczeniu biurowym, a jednocześnie przechowywane w sposób uniemożliwiający ich zabranie przez osoby nieuprawnione[139]. W przypadku zabezpieczeń przed zagrożeniami związanymi z nieuprawnionym dostępem do „strefy przetwarzania", ale będącym skutkiem działań o charakterze przestępczym (np. **włamanie)**, należy przeanalizować ich ryzyko i dobrać odpowiednie środki, np.: drzwi i okna o podwyższonej odporności na włamanie lub elektroniczny system alarmowy.

Ponadto należy zabezpieczyć pomieszczenia „strefy przetwarzania" przed działaniami spowodowanymi **siłami przyrody** oraz **awariami technicznymi**, tj.: pożar czy zalanie. W pierwszym przypadku będzie to **przynajmniej** właściwe rozmieszczenie ręcznego sprzętu gaśniczego. W drugim zaś unikanie lokalizacji pomieszczeń biurowych w bezpośredniej bliskości instalacji wodociągowych i kanalizacyjnych. Dobór zabezpieczeń jest autonomiczną decyzją Administratora danych osobowych, za którą ponosi on samodzielną odpowiedzialność. **Niedopuszczalne** jest jednak przetwarzanie danych osobowych w pomieszczeniach niemających żadnych, chociażby najbardziej podstawowych, zabezpieczeń fizycznych uniemożliwiających dostęp do nich osób nieuprawnionych oraz ochrony przed skutkami innych działań niepożądanych[140].

[137] Patrz: Ł. Kister: Ochrona danych osobowych – zabezpieczenia organizacyjno-techniczne. Część II, „Ochrona Mienia i Informacji", nr 3, 2009, s. 22.
[138] Patrz: Ł. Kister, M. Gaśpierik: *Polityka kontroli dostępu do obiektów biurowych*, „Ochrona Mienia i Informacji", nr 2, 2012, s. 87-89.
[139] Ł. Kister: Ochrona danych osobowych ... Część II, s. 22.
[140] Ł. Kister: Ochrona danych osobowych ... Część II, s. 21.

4.2.3. ZABEZPIECZENIE POMIESZCZEŃ SPECJALNYCH

W przypadku pomieszczeń„specjalnych" ich zabezpieczenia powinny być adekwatne do ich roli w procesie przetwarzania danych osobowych. Przede wszystkim muszą cechować się **wyższym poziomem ochrony** dla znajdujących się w nich zasobów, niż te stosowane dla zwykłych pomieszczeń biurowych.

Pomieszczenie **serwerowni** to najbardziej newralgiczny punkt systemu informatycznego. Znajdują się w nim wszystkie zbiory danych osobowych oraz urządzenia i aplikacje pozwalające na ich przetwarzania.

Mając na uwadze znaczenie serwera dla całokształtu ochrony danych osobowych oraz jego podatność na różnego rodzaju zagrożenia, należy przyjąć, że pomieszczenie serwerowni powinno być wyposażone w:

1) **specjalne drzwi i okna**:
   a) antywłamaniowe;
   b) ognioodporne;
2) **elektroniczne systemy** wspomagające:
   a) kontroli dostępu;
   b) sygnalizacji włamania i napadu;
   c) dozoru wizyjnego;
   d) sygnalizacji pożarowej;
   e) automatycznego gaszenia pożaru;
   f) sygnalizacji zalania;
3) **zabezpieczenie przed silnym polem elektromagnetycznym**;
4) **klimatyzację i wentylację**;
5) **podłogę techniczną**[141].

Szczegółowy rodzaj i klasę wskazanych zabezpieczeń należy dostosować do oceny zagrożeń i wartości przetwarzanych danych osobowych. Zbliżony poziom zabezpieczeń – dostosowany do innej specyfiki zagrożeń – należy zastosować względem pomieszczeń, w których znajdują pozostałe kluczowe elementy systemu informatycznego tzn. uszkodzone komputery, dyski i innego rodzaju nośniki, które mogą zawierać nieusunięte bazy danych, a przede wszystkim **kopie bezpieczeństwa** zbiorów danych osobowych i aplikacji służących do ich przetwarzania.

Studium przypadku:
Przedsiębiorca naruszy obowiązek„szczególnej staranności" wtedy, kiedy serwer systemu informatycznego służącego do przetwarzania danych osobowych umieści w pomieszczeniu pozbawionym jakichkolwiek zabezpieczeń antywłamaniowych.

W przypadku pomieszczeń „specjalnych", w których jest przechowywana dokumentacja tradycyjna, możemy posłużyć się obowiązkowymi wymaganiami odnoszącymi się do zabezpieczenia dokumentacji osobowej i płacowej pracowników[142]. Na tej podstawie możemy przyjąć, że pomieszczenie **archiwum** powinno być wyposażone przede wszystkim w:

1) **specjalne drzwi i okna**:
   a) antywłamaniowe;
   b) ognioodporne;
2) **elektroniczne systemy** wspomagające:
   a) sygnalizacji włamania i napadu;
   b) sygnalizacji pożarowej;
   c) pomiaru i rejestracji temperatury i wilgotności powietrza;
3) **zabezpieczenie przed promieniowaniem UV**;
4) **klimatyzację i wentylację**.

Ponadto dokumentację papierową należy odpowiednio chronić przed kurzem, infekcją grzybów pleśniowych oraz uszkodzeniami spowodowanymi przez owady i gryzonie. Nadto pomieszczenia te nie mogą znajdować się w nieprzystosowanej piwnicy i na strychu budynku. Nie mogą być przez nie prowadzone instalacje wodociągowe, kanalizacyjne i gazowe.

Ważne jest także, żeby „pomieszczenia specjalne" **nie były szczególnie oznaczone** w sposób identyfikujący ich przeznaczenie i nie prowokowały w ten sposób ewentualnych działań sabotażowych lub przestępczych.

---

[141] Ł. Kister: Zabezpieczenia „Data Center" – Wymagania prawa i praktyki, (w:) Praktyczne aspekty funkcjonowania serwerowni. Centra przetwarzania danych – dostosowanie do potrzeb organizacji, Warszawa: Centrum Promocji Informatyki, 2011.

[142] Rozporządzenie Ministra Kultury z dnia 15 lutego 2005 roku *w sprawie warunków przechowywania dokumentacji osobowej i płacowej pracowników*, (Dz.U. nr 32, poz. 283).

4.2.4. PRZECHOWYWANIE DOKUMENTACJI TRADYCYJNEJ

Podobnie jak w przypadku zabezpieczeń pomieszczeń „strefy przetwarzania", tak również w kwestii przechowywania dokumentacji tradycyjnych, tj. akta, księgi, kartoteki, Administrator danych osobowych otrzymał całkowitą swobodę w zakresie doboru sposobu ich ochrony **przed działaniami niepożądanymi**:

- nieuprawnionym przejęciem;
- nieuprawnioną modyfikacją ich zawartości;
- uszkodzeniem uniemożliwiającym odczytanie;
- całkowitym zniszczeniem fizycznym.

W związku z powyższym całkowicie **niedopuszczalne** jest przechowywanie dokumentacji zawierającej dane osobowe bez jakiegokolwiek ich zabezpieczenia, np. na otwartych regałach[143]. Przyjmuje się powszechnie, że dla zachowania ustawowych wymogów oraz faktycznego jej bezpieczeństwa, dokumentację tradycyjną wystarczy umieszczać w **zamykanych na klucz szafach** i szufladach mebli biurowych. Niemniej jednak część akt papierowych z uwagi na wrażliwość zawartych w nich danych osobowych, np. dokumentacja medyczna, powinna być przechowywana w szafach metalowych o podwyższonej klasie odporności na włamanie oraz ognioodpornych[144].

Studium przypadku:
Jest dopuszczalne przechowywanie nawet wrażliwej dokumentacji pracowniczej w otwartych regałach, w sytuacji gdy całe pomieszczenie archiwum akt osobowych jest zbudowane z zachowaniem podwyższonych standardów zabezpieczeń.

Niezbędnym uzupełnieniem omawianego obszaru jest postępowanie z dokumentacją tradycyjną **po ustaniu jej przydatności** do bieżącego przetwarzania oraz braku obowiązku prawnego jej dalszego archiwizowania. Jest **zakazane** wyrzucanie do koszy na śmieci jakiejkolwiek dokumentacji zawierającej dane osobowe, bez względu na jej zawartość informacyjną czy upływ czasu od jej wytworzenia.

Studium przypadku:
Administrator danych osobowych, którego dokumentacja pracownicza została znaleziona w kontenerze ze śmieciami, jeżeli tylko jest możliwe jej odczytanie, ponosi odpowiedzialność za umyślne niedopełnienie obowiązku należytego zabezpieczenia przetwarzanych danych osobowych.

Wszelkie dokumenty tradycyjne zawierające dane osobowe przeznaczone do utylizacji należy **bezwzględnie niszczyć** w przeznaczonych do tego urządzeniach, tzw. niszczarkach, spełniających co najmniej wymagania poziomu P-3 według normy technicznej DIN 66399[145].

4.3. BEZPIECZEŃSTWO SYSTEMU INFORMATYCZNEGO

Informatyzacja wszelkich dziedzin aktywności biznesowej dotyczy także procesu przetwarzania danych osobowych. Ponad **70% wszelkiej dokumentacji** przetwarzanej w systemach informatycznych nigdy nie jest drukowana. Nawet dokumenty kadrowo-płacowe, które ustawodawca nakazał przechowywać w formie tradycyjnej – papierowej, prawie w całości mają swoje odpowiedniki w formie elektronicznej[146]. W związku z powyższym systemy informatyczne stały się szczególnym punktem zainteresowania ustawodawcy, który w każdym możliwym artykule akcentuje ich rolę oraz zagrożenia, które wiążą się z ich wykorzystaniem. Ponadto z jego nakazu wydane zostało **Rozporządzenie ws. warunków technicznych**, które w znacznej części odnosi się wyłącznie do kwestii bezpieczeństwa procesu przetwarzania danych osobowych w systemach informatycznych. Zgodnie z dyspozycją ustawową powyższe rozporządzenie wyznacza **trzy poziomy bezpieczeństwa** dla systemów informatycznych (§6). Niemniej jednak przyjęty przez jego autorów warunek podłączenia systemu informatycznego do sieci publicznej – **Internet**, jako kluczowy determinant klasyfikacji – powoduje, że w praktyce każdy z Administratorów danych osobowych jest zobowiązany do stosowania „**wysokiego poziomu bezpieczeństwa**"[147]. Zwracając uwagę, że

[143] A. Drozd: Zabezpieczenie danych …, s. 46.
[144] Ł. Kister: Ochrona danych osobowych ... Część II, s. 20.
[145] Norma techniczna określająca wymogi w zakresie bezpiecznego niszczenia dokumentów i nośników danych.
[146] Ł. Kister: Ochrona danych osobowych …. Część II, s. 19.
[147] Nie znam przypadku, w którym jakakolwiek instytucja publiczna czy prywatna posiadała by system informatycznych zupełnie pozbawiony dostępu do Internetu. Patrz: Ł. Kister: *Bezpieczeństwo danych osobowych w systemach informatycznych*, „Ochrona Mienia i Informacji", nr 5, 2009, s. 12-13.

ustawodawca oraz autorzy rozporządzenia nie wskazali szczegółowych rozwiązań technologicznych, ważnym problemem praktycznym jest obowiązek dostosowania zabezpieczeń do **aktualnego stanu techniki informatycznej**. Zgodnie z dyspozycją Dyrektywy 95/46/WE Administrator danych osobowych nie ma obowiązku korzystania z najnowszych urządzeń czy oprogramowania, a jedynie takich, które zapewnią ochronę przetwarzanych danych osobowych **adekwatną do zagrożeń**, uwzględniając przy tym koszty ich realizacji (art. 17 ust. 1). Jednakże kryterium kosztów nie może być powodem całkowitego odstąpienia przez Administratora danych osobowych od zastosowania wymaganych środków zabezpieczeń technicznych[148].

4.3.1. NADAWANIE DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

Ustawodawca bezwzględnie nakazał kontrolę nad tym, kto ma dostęp do danych osobowych (art. 38). W przypadku jego realizacji za pośrednictwem systemu informatycznego ten **wymóg rozliczalności**, można spełnić z całą starannością i pełnym zakresem kontroli. Przyznanie osobie możliwości dostępu do danych osobowych przetwarzanych w systemie informatycznym jest procesem dwustopniowym.

1) Nadanie przez Administratora danych osobowych „**Upoważnienia do przetwarzania danych osobowych**"[149], które musi zawierać:
   a) wskazanie, że uprawnienie ma być realizowane przy pomocy systemu informatycznego,
   b) wskazanie zbioru danych, do którego ma być udzielony dostęp,
   c) określenie dopuszczalnych czynności przetwarzania w systemie informatycznym, np.: wprowadzanie, przeglądanie, modyfikowanie, drukowanie, udostępnianie, anonimizowanie, usuwanie, itp.
2) Utworzenie przez Administratora systemu informatycznego indywidualnego konta „użytkownika systemu informatycznego"[150], które charakteryzuje się:
   a) niepowtarzalnym „identyfikatorem", stanowiącym ciąg znaków literowych, cyfrowych lub innych, jednoznacznie pozwalającym na identyfikację osoby upoważnionej do przetwarzania danych osobowych w systemie informatycznym (§2 pkt 2),
   b) zakresem dostępu do określonych baz danych oraz uprawnień do ich przetwarzania nie mogącym wykraczać poza ten wyznaczony przez „Upoważnienie do przetwarzania danych osobowych".

Studium przypadku:
Nieprecyzyjne „Upoważnienie do przetwarzania danych osobowych" wydane dla stażysty w komórce marketingu, może skutkować nadaniem mu zbyt szerokich uprawnień dostępu do systemu informatycznego, np. pozwalających na kopiowanie całej bazy danych.

Sposób tworzenia „**identyfikatorów**" dla osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym należy do indywidualnej decyzji organizacji. Musi on jednak zapewniać możliwość jednoznacznej identyfikacji każdego użytkownika systemu informatycznego, w tym także Administratora systemu informatycznego. W praktyce może to polegać na kompilacji pierwszych liter imienia i nazwiska, wykorzystaniu nadawanych przy zatrudnianiu numerów ID lub innych jednolitych dla całej instytucji metod[151]. Jest **zakazane** nadawanie użytkownikowi „identyfikatora" identycznego z wcześniej występującym w systemie informatycznym, nawet w przypadku, kiedy identyfikator został już z wyrejestrowany z systemu (pkt IV.2.).

Studium przypadku:
Jest niedopuszczalne, aby kolejni następujący po sobie Administratorzy systemu informatycznego mieli ten sam identyfikator, np. „Admin".
Każdy z nich powinien przydzielić sobie indywidualny wyróżnik dla swoich działań w systemie informatycznym.

Dostęp do systemu informatycznego, w którym będzie istniała możliwości przetwarzania danych osobowych, musi być zabezpieczony procesem **uwierzytelnienia** użytkownika, tj. potwierdzeniem tożsamości wskazanej w indywidualnym „identyfikatorze".

---

[148] Patrz: Wyrok Naczelnego Sądu Administracyjnego z dnia 4 marca 2002 roku, (II SA 3144/01).

[149] System nadawania „Upoważnień do przetwarzania danych osobowych" został omówiony w pierwszej części niniejszego Rozdziału.

[150] Przez „użytkownika systemu informatycznego" określa się każdą osobę posiadającą dostęp do systemu informatycznego, w naszym przypadku będzie to termin oznaczający jednocześnie, że osoba ta posiada właściwe „Upoważnienie do przetwarzania danych osobowych".

[151] Ł. Kister: *Ochrona danych osobowych – funkcjonalność systemu informatycznego*, „Ochrona Mienia i Informacji", nr 4, 2009, s. 12-13.

Najpopularniejszą metodą weryfikacji praw dostępu do systemu informatycznego, jedyną wskazaną bezpośrednio przez Rozporządzenie ws. warunków technicznych, jest użycie „**hasła**" (pkt II.2.), tj. unikalnego i poufnego ciągu znaków literowych, cyfrowych lub innych (§2 pkt 3).

Siła „hasła" wykorzystywanego do uwierzytelnianie użytkowników w systemie informatycznym jest jedynym szczegółowo określonym wymogiem zabezpieczeń:

- długość: co najmniej **8 znaków**;
- budowa: **małe i wielkie litery oraz cyfry lub znaki specjalne**;
- ważność: maksymalnie **30 dni** (pkt IV.2., VIII).

Nie ma obowiązku, żeby system informatyczny automatycznie wymuszał na użytkownikach te wymagania, jednak taka funkcjonalność pozwala na skuteczne zarządzanie ich realizacją, uniemożliwiając jawne lub przypadkowe łamanie tego nakazu.

Należy w tym miejscu wskazać również, że o **poufności hasła** nie decyduje wyłącznie jego nieudostępnianie innym osobom, ale również jego treść. Stąd też użytkownik systemu informatycznego ma obowiązek stosować hasła trudne do odgadnięcia. W szczególności **nie mogą nimi być**:

- nazwisko, imię, adres, numer rejestracyjny prywatnego samochodu, PESEL, NIP, numer telefonu, itp.;
- słowo w żadnym popularnym języku;
- nazwa geograficzna, termin techniczny lub określenie potoczne;
- sekwencja kolejnych znaków na klawiaturze;

  a także dowolny spośród wymienionych uzupełnionym na początku lub końcu cyfrą lub znakiem specjalnym.

Studium przypadku:
Za zupełnie niedopuszczalne należy uznać hasło: „Kadrowa34", ale można je prosto zmodyfikować w taki sposób by spełniało wymogi poufności: „K@dr0wA#4".

Ponadto przyjmuje się także, że **ponowne użycie** tego samego hasła może nastąpić dopiero po okresie 6 miesięcy[152].

Poza opisanym w Rozporządzeniu ws. warunków technicznych wykorzystaniem „hasła" – metoda „co wiem", jest dopuszczalne również użycie innych środków identyfikacji uprawnień dostępu do systemu informatycznego:

- **urządzenia**, np. karty mikroprocesorowe, tokeny – metoda „co mam";
- **biometria**, np. odcisk linii papilarnych, mapa siatkówki oka, kształt twarzy, barwa głosu – metoda „kim jestem"[153].

Niemniej jednak warunkiem zastosowania takiego systemu uwierzytelniania jest jego poziom zabezpieczenia przed nieuprawnionym dostępem, który winien być przynajmniej równy temu z wykorzystaniem hasła.

Studium przypadku:
Użycie kart mikroprocesorowych jako narzędzia weryfikacji uprawnień musi uwzględniać mechanizm odporności systemu na ich wykorzystanie przez osoby nieuprawnione, np. w wyniku zagubienia czy kradzieży.

Omawiając zasady udzielania dostępu do systemu informatycznego nie można pominąć kwestii odbierania tych praw, choć nie została ona wprost opisana w Rozporządzeniu ws. warunków technicznych.

Zablokowanie konta użytkownika uniemożliwiające mu jakikolwiek dostęp do systemu informatycznego lub wykonywanie w nim czynności przetwarzania danych osobowych może mieć charakter:

1) trwały, w sytuacji ustania ważności „Upoważnienia do przetwarzania danych osobowych", np. rozwiązanie stosunku pracy;
2) czasowy, w sytuacjach szczególnych, np.:

a) nieobecności użytkownika w pracy trwającej dłużej niż 1 miesiąc;
b) zawieszeniu użytkownika w pełnieniu obowiązków służbowych;
c) wypowiedzenia użytkownikowi umowy o pracę;
d) wszczęcia wobec użytkownika postępowania dyscyplinarnego.

Należy jednak pamiętać, by z przyczyn dowodowych **nie usuwać** niezwłocznie zablokowanego konta, wraz z informacjami o zarejestrowanych na nim aktywnościach związanych z procesem przetwarzania danych osobowych. **Wyjąt-**

[152] Ł. Kister: Ochrona danych osobowych – funkcjonalność …, s. 13.
[153] A. Drozd: *Zabezpieczenie danych* …, s. 49-50.

kiem od obowiązku wdrożenia procedur uwierzytelniania użytkowników systemu informatycznego jest sytuacja – prawie wyłącznie hipotetyczna – w której dostęp do niego ma tylko jedna osoba (pkt II.2.).

4.3.2. KONTROLA PRZETWARZANIA DANYCH OSOBOWYCH

Jednym z najważniejszych elementów systemu ochrony danych osobowych jest wymóg **kontroli procesu przetwarzania**. Ustawodawca nakazał Administratorowi danych osobowych zapewnienie możliwości ustalenia takich informacji, jak:

- jakie dane osobowe zostały wprowadzone do zbioru;
- kiedy dane osobowe zostały wprowadzone do zbioru;
- kto wprowadził dane osobowe do zbioru;
- komu są przekazywane dane osobowe (art. 38).

Wymóg ten obejmuje obie formy przetwarzania danych osobowych, tj. tradycyjną (papierową) oraz informatyczną (komputerową). Wydaje się jednak, że wypełnienie tego obowiązku w pierwszym przypadku może być praktycznie nieosiągalne[154]. Dlatego też jest on prawie wyłącznie odnoszony do wymaganej **funkcjonalności systemów informatycznych**. Zgodnie z dyspozycją Rozporządzenia ws. warunków technicznych system informatyczny służący do przetwarzania danych osobowych powinien **dla każdej osoby**, której dane dotyczą, odnotować:

- **datę pierwszego wprowadzenia** danych osobowych do systemu;
- **identyfikator użytkownika** wprowadzającego dane do systemu, chyba, że dostęp do tego systemu posiada wyłącznie jedna osoba;
- szczegółowe informacje identyfikujące **źródło danych osobowych**, w przypadku zbierania danych nie od osoby, której dane dotyczą;
- szczegółowe **informacje o odbiorcach danych**, w tym data i zakres udostępnienia;
- **informacji o sprzeciwie** wobec przetwarzania danych dla celów marketingowych lub przekazywania ich innemu podmiotowi, zgłoszonym przez osobę, której dane dotyczą (§7 ust. 1).

Istotny jest tu jednak wymóg takiej funkcjonalności aplikacji obsługującej zbiór danych, aby pierwsze dwie informacje **zapisywały się automatycznie** po zatwierdzeniu przez użytkownika operacji wprowadzenia danych (§7 ust. 2), bez możliwości ingerencji kogokolwiek w te metadane[155]. Pozostałe informacje mogą być umieszczane ręcznie przez użytkownika, ale musi to następować w systemie informatycznym, nie zaś w podręcznej ewidencji papierowej czy innej aplikacji, np. arkuszu kalkulacyjnym czy pliku tekstowym[156].

Studium przypadku:
Przedsiębiorca pozyskując od innej firmy bazę danych teleadresowych potencjalnych klientów musi odnotować w systemie służącym do jej przetwarzania dokładne informacje identyfikujące tę firmę – nazwa, adres, numer identyfikacyjny (NIP, REGON, KRS).

W świetle wymogów Rozporządzenia ws. warunków technicznych, system informatyczny nie musi odnotowywać innych informacji niż wskazane powyżej. Niemniej jednak praktyka wskazuje, że utrwalanie także innych informacji związanych z przetwarzaniem danych jest **przydatne** dla wykonywania pozostałych obowiązków Administratora danych określonych w ustawie. Dlatego też jest celowe, aby system umożliwiał dodatkowo **odnotowywanie informacji** o:

- **przesłankach**, na podstawie których są przetwarzane dane osobowe (art. 23), szczególnie w przypadku przetwarzania „wrażliwych" danych osobowych (art. 27 ust. 2) oraz gdy przetwarzanie jest legalizowane przez więcej niż jedną przesłankę;
- **dacie zebrania danych**, gdyż sam fakt wprowadzenia danych do systemu informatycznego nie jest datą faktycznego rozpoczęcia przetwarzania;
- **udostępnienia danych podmiotom uprawnionym z mocy prawa**, np. Sąd czy Policja;
- **realizacji szczególnych uprawnień osoby**, której dane dotyczą (art. 24, 25, 32, 33)[157].

---

154 J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 634.

155 Metadane to inaczej „dane o danych", czyli informacje określające atrybuty innych informacji, pozwalające na zarządzanie nimi, np. katalog biblioteczny.

156 Patrz: Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 17 listopada 2004 roku, (II SA/Wa 887/04).

157 A. Drozd: *Zabezpieczenie danych* …, s. 37-38.

W tym miejscu należy jednocześnie zaznaczyć, że wymuszona przez ustawodawcę kontrola procesu przetwarzania danych osobowych nie ma służyć celom ewidencyjno-dokumentacyjnym. Jej zadaniem jest przede wszystkim działanie **prewencyjne**, tj. ograniczenie możliwości przyzwolenia na naruszanie zasad, jak również **dowodowe**, w sytuacji wystąpienia sytuacji niepożądanej[158]. System informatyczny **nie musi umożliwiać odnotowywania** w/w informacji, jeżeli jest wykorzystywany jedynie do edycji tekstu w celu udostępniania go na piśmie (§7 ust. 1). Wyłączenie to można zastosować jedynie w takim przypadku, kiedy aplikacja służy wyłącznie do wytworzenia dokumentu mogącego zawierać dane osobowe, a po jego wydrukowaniu nie jest on zapisywany (np. edytor tekstu)[159]. Szczególnym przypadkiem realizacji wymogu odnotowywania operacji na danych osobowych jest sytuacja, w której informacje dotyczące tych samych osób są przetwarzane jednocześnie **w dwóch aplikacjach**. Wówczas odnotowywanie może być realizowane tylko w jednym z nich lub w odrębnym systemie informatycznym, który jest przeznaczony tylko do tej czynności (§7 ust. 4).

Studium przypadku:
Jeżeli dane kadrowo-płacowe są przetwarzane przy wykorzystaniu kilku różnych aplikacji, to obowiązkowe informacje kontrolne mogą być odnotowywane tylko w jednym z nich.

Właściwie prowadzona ewidencja metadanych kontrolnych, pozwala na wypełnienie obowiązku przygotowania i wydrukowania **raportu informacyjnego** dla każdej osoby, której dane osobowe są przetwarzane (§7 ust. 3). Raport ten ma w powszechnie zrozumiałej formie nie tylko przedstawiać obowiązkowe metadane, ale także te wskazane jako zalecane oraz treść przetwarzanych danych osobowych. Dopiero w takiej sytuacji będzie możliwe potwierdzenie zdolności Administratora danych osobowych do wypełniania ustawowego obowiązku informacyjnego względem osoby, której dane dotyczą (art. 32 ust. 1). Nie istnieje wymóg techniczny, by raport generowany był automatycznie z aplikacji, która służy do przetwarzania danych osobowych, np. za pomocą edytora tekstu. Ważna jest tylko jego „**powszechne zrozumienie**", które oznacza konieczność dostosowania zawartych w nim informacji do możliwości potencjalnego czytelnika, np. unikając skrótów innych niż ogólnie znane czy fachowych zwrotów informatycznych. Ponadto należy przyjąć, że powinien on być sporządzony w języku polskim, ponieważ tylko w odniesieniu do niego możemy mówić, że jest on powszechnie zrozumiały w Rzeczpospolitej Polskiej[160].

4.3.3. ZABEZPIECZENIE PRZED ZAGROŻENIAMI Z INTERNETU

Systemy informatyczne w związku z ich powszechnym podłączeniem do sieci publicznej (Internet), w sposób szczególny są podatne na różnego rodzaju niepożądane działania, które mogą bezpośrednio lub pośrednio zagrażać bezpieczeństwu przetwarzanych w nich danych osobowych. W związku z powyższym, zgodnie z dyspozycją Rozporządzenia ws. warunków technicznych, Administrator danych osobowych jest zobowiązany do zabezpieczenia systemu informatycznego przed działaniem **szkodliwego oprogramowania**[161], tzw. „wirusów" (pkt III.1), lub **innego czynnika** – np. *hacking* (pkt XII.1.), których celem jest uzyskanie nieuprawnionego dostępu do procesu przetwarzania danych osobowych.

Za „**działania niepożądane**" w tym obszarze należy uznać m.in. takie, które:

- powodują nieautoryzowaną samoinstalację oprogramowania;
- prowadzą do uszkodzenia lub modyfikacji pamięci komputerowej, plików systemowych lub oprogramowania;
- służą do omijania lub przełamywania zabezpieczeń i/lub praw dostępu;
- wymuszają wykorzystanie większej ilości zasobów niż jest to niezbędne do zapewnienia prawidłowego działania systemu informatycznego;
- powodują zakłócenia w normalnym działaniu systemu informatycznego;
- prowadzą do naruszenia zasad integralności, rozliczalności, dostępności i poufności danych osobowych przetwarzanych w systemie informatycznym[162].

Zabezpieczenie systemu informatycznego przed podatnością na działania niepożądane może składać się z bardzo wielu elementów zabezpieczających – organizacyjnych, programowych i fizycznych. **Dobór środków ochrony** powinien uwzględniać:

- rodzaj przetwarzanych danych osobowych, w tym ich „wrażliwość" informacyjną;
- organizację systemu informatycznego, w tym jego wielkość, skomplikowanie i rozproszenie;

158 J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 634.
159 A. Krasuski, D. Skolimowska: *Dane osobowe* …, s. 232.
160 A. Drozd: *Zabezpieczenie danych* …, s. 39-40.
161 W potocznej dyskusji bardzo często można spotkać się z terminem „oprogramowanie złośliwe".
162 Szerzej w: A. Kaczmarek: ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych, Warszawa: GIODO, 2009.

- sposób podłączenia do Internetu;
- specyfikę procesu przetwarzania, w tym konieczność przesyłania danych za pośrednictwem internetu i wykorzystywanie komputerowych nośników danych;
- dotychczasowe zdarzenia niepożądane, bez względu na to czy pochodziły z internetu.

Podstawowym warunkiem ochrony systemu informatycznego przed możliwością wystąpienia sytuacji niepożądanych jest systematyczna **aktualizacja oprogramowania**. Wszelkie aplikacje informatyczne mają zamierzone lub przypadkowe błędy, luki w oprogramowaniu, które mogą pozwolić na dostęp do danych bez uwierzytelniania, tzw. „**wejście tylnymi drzwiami**". Szczególnie w przypadku oprogramowania pochodzącego z nieznanego źródła może ono zawierać dodatkowo niebezpieczne kody lub ukryte szpiegowskie funkcjonalności[163]. W związku z powyższym jest niezbędne, aby do przetwarzania danych osobowych wykorzystywać wyłącznie **legalne oprogramowanie**, gdyż tylko takie umożliwia uzyskiwanie zatwierdzonych przez producenta nowych wersji, poprawek lub aktualizacji usuwających stwierdzone wady i słabości. Za dobrą praktykę należy uznać korzystanie z funkcji **automatycznej aktualizacji** wszystkich aplikacji w systemie informatycznym, nie tylko tych służących bezpośrednio do przetwarzania danych osobowych. W przypadku braku takiej możliwości, należy możliwie regularnie śledzić informacje udostępniane przez producenta oprogramowania i dokonywać jego „ręcznej" aktualizacji[164].

Studium przypadku:
Zainstalowanie w systemie informatycznym chociażby jednej nielegalnej kopii oprogramowania, która nie podlega poprawnej aktualizacji, powoduje obniżenie bezpieczeństwa całego systemu, bez względu na zainstalowanie dodatkowych systemów ochrony.

Niemniej jednak kluczowym zabezpieczeniem systemu informatycznego przed pochodzącymi z Internetu zagrożeniami jest obowiązek zainstalowania **aplikacji monitorująco-zabezpieczającej**, zwanej potocznie **antywirusową**. Jej działanie musi obejmować wszystkie urządzenia systemu informatycznego, zarówno serwery i urządzenia sieciowe, jak również poszczególne stanowiska komputerowe i wszelkie urządzenia mobilne. **Funkcjonalność** takiej aplikacji powinna być maksymalnie szeroka, nieograniczona wyłącznie do wykrywania „wirusów komputerowych", żeby skutecznie chronić system informatyczny przed wszelkimi możliwymi zagrożeniami pochodzącymi z „zewnątrz". Powinna mieć ona zdolność:
- wykrycia i zablokowania każdego rodzaju szkodliwego ataku;
- integracji z systemem operacyjnym i kluczowymi programami;
- ciągłego nadzoru „w tle" nad pracą systemu informatycznego;
- analizy danych przesyłanych w sieci wewnętrznej;
- kontroli przepływu danych do/z sieci Internet;
- kontroli i blokowania niechcianej poczty elektronicznej;
- blokowania dostępu do określonych stron i aplikacji internetowych;
- analizy komputerowych nośników danych[165],

a ponadto powinna umożliwiać rejestrację:
- daty i czasu zalogowania i wylogowania z każdego użytkownika systemu informatycznego;
- danych identyfikujących komputer, z którego następuje dostęp do systemu;
- udanych i nieudanych prób dostępu do systemu informatycznego z wewnątrz sieci oraz przy wykorzystaniu sieci Internet[166].

Najważniejszym jednak determinantem skuteczności działania tego rodzaju aplikacji jest **aktualizacja wzorców wirusów**. Powinien on być tak skonfigurowany, żeby z maksymalną częstotliwością automatycznie pobierał ze strony producenta nowe bazy rozpoznanych wirusów, utrzymując zdolność do reakcji na aktualne zagrożenia. Jednocześnie program ten powinien być **centralnie zarządzany**, przy całkowitym pozbawieniu użytkowników możliwości jego modyfikacji lub wyłączenia na swoich stanowiskach komputerowych.

[163] A. Gałach: *Instrukcja ochrony danych osobowych w systemie informatycznym*, Gdańsk: Ośrodek Doradztwa i Doskonalenia Kadr, 2004, s. 4 (errata).
[164] Ł. Kister: Bezpieczeństwo danych osobowych …, s. 13-14.
[165] A. Gałach: Instrukcja ochrony danych …, s. 52.
[166] Ł. Kister: Bezpieczeństwo danych osobowych …, s. 15.

Studium przypadku:
Bezpieczeństwu systemów informatycznych zagraża obecnie ponad 50 milionów różnych szkodliwych programów; każdego miesiąca liczba ta rośnie o kolejne 500 tysięcy. Każdego dnia w naszym kraju skutecznie zainfekowanych wirusami jest około 280 tysięcy urządzeń komputerowych.

Najbardziej radyklanym z zabezpieczeń – zarówno przed szkodliwym oprogramowaniem, jak również przed innymi zagrożeniami związanymi z dostępem do Internetu – ale w niektórych przypadkach niezbędnym (np. przetwarzanie danych osobowych stanowiących informacje o krytycznym znaczeniu dla firmy), jest **wydzielenie urządzenia komputerowego**:

- fizyczne odseparowanie od sieci Internet, w tym od połączenia z innymi urządzeniami komputerowymi, które mają takie podłączenie;
- blokowanie portów komunikacji zewnętrznej, np. USB;
- blokowanie napędów optycznych, np. CD;
- blokowanie systemów komunikacji bezprzewodowej, np. Bluetooth.

Tego rodzaju działania ograniczają praktycznie całkowicie ryzyko ataku z wykorzystaniem oprogramowania szkodliwego[167].

4.3.4. ZABEZPIECZENIE PRZED AWARIĄ ZASILANIA

Systemy informatyczne są narażone nie tylko na infekcje wirusowe, ale także na negatywne skutki utraty lub niestabilności zasilania w energię elektryczną. Wynikiem takiej sytuacji może być nie tylko czasowe pozbawienie zdolności do przetwarzania danych osobowych, ale przede wszystkim nieodwracalne uszkodzenie pamięci, na której są zapisane zbiory danych osobowych, a tym samym ich utratę. W związku z powyższym Administrator danych osobowych ma obowiązek ochrony systemu informatycznego **przed utratą danych wskutek awarii zasilania** lub zakłóceniami w sieci zasilającej (III.2.). Z uwagi na fakt, że obowiązek ten **nie dotyczy** zabezpieczenia przed samą awarią zasilania, ale przed możliwością jej negatywnych skutków dla przetwarzanych danych osobowych, jego **realizacja może przybrać kilka form**. Ich pojedyncze lub wspólne zastosowanie powinno wynikać ze specyfiki systemu informatycznego, rodzaju przetwarzanych zbiorów danych osobowych, analizy częstotliwości tego rodzaju zdarzeń nadzwyczajnych. Podstawowym działaniem powinno być takie skonfigurowanie aplikacji służących do przetwarzania danych osobowych, by dokonywały **automatycznego zapisywania** wszystkich działań bezpośrednio w zasobach serwera. Zabezpiecza ono jednak wyłącznie stanowiska komputerowe, nie gwarantując w żaden sposób ochrony dla całego zbioru danych osobowych. Jednakże uznaje się, że **niezbędnym minimum** dla spełnienia tego obowiązku jest:

- użycie listew przeciwprzepięciowych dla wszystkich stanowisk systemu informatycznego;
- wyposażenie serwera oraz najważniejszych stanowisk komputerowych w system akumulatorowego zasilania awaryjnego, tzw. UPS.

Optymalnym zaś rozwiązaniem jest utworzenie w strefie przetwarzania danych osobowych **bezpiecznej sieci zasilającej**, której celem nie musi być zagwarantowanie ciągłej dostawy energii i utrzymanie normalnej pracy systemu informatycznego, ale zapewnienie możliwości zapisania wszystkich informacji i bezpieczne wyłącznie urządzeń[168].

Ponadto jest zasadnym, żeby budynki, w których znajdują się urządzenia systemu informatycznego, były wyposażone w **instalację odgromową**, w tym w szczególności elementy linii zewnętrznych sieci telekomunikacyjnej.

4.3.5. KOPIE BEZPIECZEŃSTWA

Zapewnienie „kopii bezpieczeństwa" dla systemów informatycznych jest jednym z podstawowych elementów **zapewnienia ciągłości działania** na wypadek wystąpienia sytuacji kryzysowej, tj.:

- fizycznego zniszczenia infrastruktury systemu informatycznego;
- zniszczenia lub uszkodzenia bazy danych;
- infekcji wirusowej;
- nieuprawnionego usunięcia lub zmodyfikowania bazy danych.

[167] Tego rodzaju zabezpieczenia stosuje się w bezpiecznych stanowiskach komputerowych służących do przetwarzania „informacji niejawnych". Patrz: B. Iwaszko: *Ochrona informacji niejawnych w praktyce*, Wrocław: Presscom, 2012.
[168] A. Drozd: Zabezpieczenie danych …, s. 54.

Rozporządzenia ws. warunków technicznych nakłada także na Administratora danych osobowych obowiązek zabezpieczenia przetwarzanych danych osobowych poprzez wykonanie kopii bezpieczeństwa[169]:

- **zbiorów danych osobowych**;
- **programów** służących do przetwarzania danych osobowych (pkt IV.3.).

Podstawowym wyznacznikiem kopii bezpieczeństwa jest **częstotliwość** ich wykonywania, która powinna uwzględniać, takie determinanty, jak:

- skomplikowanie systemu informatycznego;
- wielkość zbiorów danych osobowych;
- częstotliwość zmian zawartości informacyjnej zbioru danych osobowych;
- ocena ryzyka i analiza dotychczasowych zdarzeń kryzysowych.

Ponadto kopię bezpieczeństwa należy wykonać w przypadku aktualizacji aplikacji o krytycznym znaczeniu dla procesu przetwarzania danych osobowych oraz przed czynnościami serwisowymi obejmującymi urządzenia serwerowe[170]. Jednocześnie nie ma obowiązku, żeby z tą samą częstotliwością wykonywać kopie bezpieczeństwa wszystkich przetwarzanych zbiorów danych osobowych.

Studium przypadku:
Przedsiębiorca prowadzący zbiory danych marketingu internetowego oraz kadrowo-płacowego może sporządzać przyrostową kopię bezpieczeństwa pierwszego z nich z częstotliwością nawet 1 godziny lub jeszcze częściej, natomiast drugiego tylko co miesiąc, gdy nie wykonuje w tym czasie żadnych szczególnych zmian w tym zbiorze.

Każdą kopie bezpieczeństwa należy wykonywać na oddzielnym, specjalnie do tego przeznaczonym i właściwie oznaczonym **zewnętrznym nośniku danych**, tj. płyta DVD, dysk HDD/SSD, taśma magnetyczna. **Niedopuszczalne** jest tworzenie kopii bezpieczeństwa na dysku serwera służącego do bieżącego przetwarzania danych osobowych. Nośniki kopii bezpieczeństwa, z uwagi na swoje krytyczne znacznie dla bezpieczeństwa systemu informatycznego, należy przechowywać w odpowiednio **zabezpieczonych pomieszczeniach**, gwarantujących ochronę przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem (pkt IV.4a.), także z uwagi na działanie sił przyrody czy silnego pola magnetycznego[171]. Ważne jest, żeby nośniki kopii bezpieczeństwa nie były narażone na skutki tych samych działań niepożądanych co zbiory danych osobowych pozostające w bieżącym użytkowaniu. Stąd stanowczo **niedozwolone** jest przechowywanie jej nośników w pomieszczeniu serwerowni, nawet w przypadku zabezpieczenia ich w szafie stalowej.

Studium przypadku:
Producent mebli, którego obiekt biurowy jest narażony na wysokie ryzyko pożaru, powinien przechowywać nośniki kopii bezpieczeństwa w innej lokalizacji.

Istotnym warunkiem przydatności kopii bezpieczeństwa jest ich zdolność do odtworzenia zasobów systemu informatycznego w przypadku wystąpienia sytuacji kryzysowej. Dlatego też jest niezbędne cykliczne **testowanie** wybranych kopii bezpieczeństwa. Stwierdzenie utraty przez kopię bezpieczeństwa waloru przydatności do celu jakiemu ma służyć – uszkodzenie lub istnienie nowszej – wymusza konieczność jej **zniszczenia** (pkt IV.4b.).

4.3.6. UŻYTKOWANIE URZĄDZEŃ MOBILNYCH

Wykorzystanie komputerowych urządzeń mobilnych jest dzisiaj pewnego rodzaju standardem każdego rodzaju organizacji. Już nie tylko komputery przenośne, ale także mniejsze urządzenia są wykorzystywane do zdalnej pracy w systemie informatycznym. Zgodnie z dyspozycją Rozporządzenia ws. warunków technicznych osoba użytkująca urządzenie mobilne[172] służące do przetwarzania danych osobowych jest zobowiązana do zachowania szczególnej ostrożności podczas jego użytkowania (pkt V). Przez **szczególne warunki użytkowania** urządzeń mobilnych należy rozumieć m.in.:

- zakaz ich pozostawiania bez nadzoru, w szczególności w samochodach, hotelach i innych miejscach publicznych;
- zakaz ich używania przez osoby inne niż użytkownicy, którym zostały one powierzone;
- zakaz ich podłączania do otwartych sieci internetowych wi-fi, tzw. „hot spot";

[169] Rozporządzenie ws. warunków technicznych nazywa je „kopiami zapasowymi".
[170] Ł. Kister: Bezpieczeństwo danych osobowych …, s. 13.
[171] A. Krasuski, D. Skolimowska: *Dane osobowe* …, s. 227.
[172] W przedmiotowym rozporządzeniu jest mowa wyłącznie o komputerach przenośnych.

- zakaz ich przechowywania w pamięci urządzenia zbiorów danych osobowych;
- zakaz ich samodzielnej modernizacji oraz zakaz samodzielnej modernizacji użytkowanego przez nie oprogramowania.

Ponadto urządzenia mobilne wykorzystywane do przetwarzania danych osobowych poza „strefą przetwarzania" muszą być **zabezpieczone metodami kryptograficznymi** (pkt V), w tym również proces uwierzytelnienia dostępu zdalnego do systemu informatycznego (pkt. XIII) .

Wypełnieniem tego obowiązku będzie w szczególności:
- **zaszyfrowanie dysku** twardego urządzenia, uniemożliwiającego dostęp osób nieuprawnionych do jego zasobów;
- **wykorzystywanie protokołu SSL** (ang. *Secure Socket Layer*), pozwalającego na bezpieczną transmisję zaszyfrowanego strumienia danych.

Studium przypadku:
Użytkownik urządzenia mobilnego, który wykorzystuje je do dostępu do skrzynki pocztowej e-mail, na którą są przesyłane wiadomości zawierające zestawienia danych osobowych musi już wypełniać szczególne warunki użytkowania tego urządzenia.

4.3.7. ZARZĄDZANIE KOMPUTEROWYMI NOŚNIKAMI DANYCH

Najpopularniejszym narzędziem do przenoszenia i czasowego przechowywania danych osobowych przetwarzanych w systemie informatycznym są komputerowe nośniki danych, np. płyty CD/DVD, dyski HDD/SSD, pamięci typu „pendrive". Z użytkowaniem tego rodzaju nośników wiąże się jednak **największa grupa zdarzeń kryzysowych** związanych z ich utratą, tj. zagubieniem lub kradzieżą. Przyjmuje się, że kluczowymi **warunkami bezpiecznego użytkowania** komputerowych nośników danych w systemie informatycznym jest:
- wykorzystywanie wyłącznie służbowych zarejestrowanych nośników;
- bezwzględne szyfrowanie ich zawartości, nie tylko w przypadku wynoszenia poza „strefę przetwarzania";
- przechowywanie ich w zamkniętych szafach o podwyższonym standardzie ochrony[173].

Studium przypadku:
Komputerowa baza danych klientów banku, zawierające nawet kilka milionów rekordów, mieści się na ogólnie dostępnych nośnikach danych typu „pendrive".
Jej wydruk należałoby przewozić ciężarówką.

Wszelkie komputerowe nośniki danych, w tym także nośniki „kopii bezpieczeństwa" oraz dyski serwera, po ustaniu ich przydatności należy pozbawić zapisu danych osobowych lub **fizycznie zniszczyć**, w sposób uniemożliwiający jakiekolwiek odczytanie (pkt. VI).

[173] Ł. Kister: Ochrona danych osobowych …. Część II, s. 20.

5. DOKUMENTOWANIE SYSTEMU OCHRONY DANYCH OSOBOWYCH

dr Łukasz Kister

Administrator danych osobowych ma **ustawowy obowiązek** opracowania, wdrożenia i prowadzenia dokumentacji systemu ochrony danych osobowych (art. 36 ust. 2).

System ochrony danych osobowych to najogólniej zbiór celowo zdefiniowanych elementów organizacyjnych i technicznych, które wzajemnie ze sobą powiązane funkcjonują jako jedna całość, wspólnie realizując jeden cel – zapewnienie niezakłóconego procesu przetwarzania danych osobowych i minimalnego akceptowalnego poziomu ich odporności na działania niepożądane.

Na wymóg prowadzenia dokumentacji **nie ma wpływu**:

- rodzaj przetwarzanych danych osobowych;
- cel przetwarzania;
- wielkość przetwarzanych zbiorów danych osobowych;
- sposób przetwarzania[174].

Zgodnie z dyspozycją Rozporządzenia ws. dokumentacji w **skład obowiązkowej dokumentacji** systemu ochrony danych osobowych wchodzą:

1) Polityka bezpieczeństwa;
2) Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (§3).

Należy jednak uznać, że nie jest to zbiór zamknięty i powinien być rozszerzony na pozostałe dokumenty określone wprost lub wynikające z przepisów Ustawy:

3) Upoważnienia do przetwarzania danych osobowych (art. 37);
4) Ewidencja upoważnień do przetwarzania danych osobowych (art. 39 ust. 1);
5) Zobowiązania do zachowania poufności (art. 39 ust. 2).

Ponadto ze względów organizacyjnych skład dokumentacji może być jeszcze szerszy i obejmować dokumenty niezbędne do prawidłowego zarządzania procesem przetwarzania danych osobowych w organizacji[175].

Istotna jest przede wszystkim **zawartość merytoryczna dokumentacji**, a nie liczba jej składników.

Przede wszystkim jednak podstawowym wymogiem stawianym dokumentacji systemu ochrony danych osobowych, jest jej **przejrzystość i kompleksowość**, dzięki której osoby zarządzające, nadzorujące i bezpośrednio przetwarzające dane osobowe będą wiedziały, jak wypełniać obowiązki ustawowe na swoim stanowisku pracy[176].

5.1. POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Polityka bezpieczeństwa danych osobowych – jest to zbiór praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych wewnątrz i na zewnątrz organizacji, odnoszących się całościowo do problemu zabezpieczenia danych osobowych przed działaniami niepożądanymi, zarówno tych przetwarzanych tradycyjnie, jak i tych przetwarzanych w systemach informatycznych. Jak już wspomniano we wstępie, Rozporządzenie ws. dokumentacji nakłada obowiązek prowadzenia **dwóch dokumentów** dla systemu ochrony danych osobowych, tj:

- Polityka bezpieczeństwa;
- Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Niemniej jednak z takim wymogiem wiąże się **kilka formalnych i praktycznych problemów**, których usunięcie wydaje się być niezbędne dla stworzenia poprawnej i jednoznacznej dokumentacji systemu ochrony danych osobowych. Po pierwsze, całkowicie niefortunna jest **nazwa** „Polityka bezpieczeństwa" w odniesieniu do dokumentu, który nie ma opisywać zasad całościowej ochrony organizacji, tj. bezpieczeństwa fizycznego, informacyjnego, antyterrorystycznego, itp., a tylko jednego z niematerialnych aktywów – danych osobowych[177]. Po drugie, praktycznie i prawnie niezrozumia-

[174] A. Drozd: Zabezpieczenie danych …, s. 65.
[175] P. Fajgielski: Obowiązki związane z zabezpieczeniem …, s. 144.
[176] M. Byczkowski: Zarządzanie procesami przetwarzania danych osobowych, (w:) X. Konarski, G. Sibiga (red.): Ochrona danych osobowych. Aktualne problemy i nowe wyzwania, Warszawa: Wolters Kluwer Polska, 2007, s. 39.
[177] M. Byczkowski: Zarządzanie procesami przetwarzania …, s. 34.

ła jest konieczność prowadzenia dwóch odrębnych dokumentów wzajemnie dublujących swoje **zadania**[178]. W związku z powyższym istotą poprawności dokumentacji systemu ochrony danych osobowych jest **zawartość merytoryczna**, nie zaś nazwa, czy liczba składających się na nią dokumentów. Przyjmując jednak potrzebę czytelności i jednoznaczności niosącego obowiązki i skutki prawne dokumentu, zasadnym jest, aby nosił on precyzyjną nazwę – **Polityka Bezpieczeństwa Danych Osobowych (dalej: „Polityka")**[179].

5.1.1. ZASADY PRZYGOTOWYWANIA DOKUMENTACJI BEZPIECZEŃSTWA

Dokumentacja określająca zasady bezpieczeństwa przetwarzanych danych osobowych, poza wszelkimi innymi szczegółowymi wymogami, musi być **adekwatna do rzeczywistości**, odnosząc się do stanu faktycznego wdrożonego systemu zabezpieczeń. Punktem wyjścia do wdrożenia w organizacji poprawnych zasad ochrony danych osobowych powinna być **deklaracja woli** w tym zakresie złożona przez ścisłe kierownictwo. Prezentowane dosyć często w Polsce pisanie „Polityki", tylko z uwagi na obowiązek ustawowy i zagrożenie kontrolą, a w jej następstwie karą, jest sytuacją niedopuszczalną, której wynikiem są zawsze dokumenty nieprzystające do specyfiki i charakterystyki Administratora danych osobowych[180]. Oczywiście nie może być mowy o ich stosowaniu w praktyce, a tym samym o właściwej ochronie aktywów informacyjnych[181]. W związku z powyższym przygotowanie „Polityki" to proces, który powinien zostać oparty na poprawnie i skrupulatnie wykonanym **audycie**, który rozpozna i zidentyfikuje:

- zbiory danych osobowych;
- procesy przetwarzania danych osobowych;
- system informatyczny i jego elementy wykorzystywane do przetwarzania danych osobowych;
- obszar przetwarzania danych osobowych;
- ryzyka dla bezpieczeństwa przetwarzanych danych osobowych[182].

Ważna jest także **kolejność tworzenia** poszczególnych procedur i zasad – od ogółu do szczegółu. Jako pierwsze należy określić generalne standardy ochrony danych osobowych, a następnie na tej podbudowie wyznaczyć szczegóły rozwiązań organizacyjnych i technicznych odnoszących się do wszystkich obszarów i sposobów przetwarzania.

Ponadto wśród podstawowych wymogów należy wskazać także na **obowiązek pisemnej formy „**Polityki"[183]. Nie znajduje on jednak potwierdzenia w prawie, co powoduje, że przygotowanie i utrzymywanie dokumentu „Polityki" w formie elektronicznej nie powinno stanowić o jej nieważności. Przygotowanie poprawnej, co nie oznacza wyłącznie zgodnej z wymogami prawa, ale przede wszystkim wspomagającej proces zarządzania przetwarzaniem danych osobowych dokumentacji bezpieczeństwa jest zadaniem wymagającym **profesjonalnego podejścia**. Dlatego też warto zastanowić się czy jego realizacji nie należy powierzyć zewnętrznym konsultantom, ze szczególnym zwróceniem uwagi na ich odpowiednią wiedzę i doświadczenie, które będą gwarantować poziom zaprojektowanego i opisanego systemy zarządzania bezpieczeństwem[184]. Nie oznacza to, że samodzielne przygotowanie „Polityki" jest niemożliwe, czy skazane na niepowodzenie[185].

5.1.2. UKŁAD I ZAWARTOŚĆ MERYTORYCZNA POLITYKI

Określony przez **Rozporządzenie ws. dokumentacji** układ i zawartość merytoryczna dokumentacji systemu zarządzania bezpieczeństwem danych osobowych budzi liczne wątpliwości jakościowe.

Zgodnie z jego treścią, **wymaganymi elementami** „Polityki" są:

1) wykaz budynków pomieszczeń lub części pomieszczeń, tworzących obszar, w którym są przetwarzane dane osobowe;
2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
4) sposób przepływu danych pomiędzy poszczególnymi systemami informatycznymi;
5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych (§4), które w odniesieniu do bezpieczeństwa systemu informatycznego służącego do przetwarzania danych osobowych, powinny zawierać:

---

178 Patrz: Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 8 grudnia 2005 roku (II SA Wa 1539/05).

179 Ł. Kister: Polityka bezpieczeństwa …, s. 14; M. Byczkowski: Zarządzanie procesami przetwarzania …, s. 34.

180 Patrz: P. Kral: *Wzorcowa dokumentacja ochrony danych osobowych z komentarzem*, Gdańsk: Ośrodek Doradztwa i Doskonalenia Kadr, 2007.

181 Ł. Kister: Polityka bezpieczeństwa …, s. 14.

182 Patrz: Ł. Kister: Audyt jako narzędzie oceny bezpieczeństwa informacji w organizacji, (w:) M. Gajos (red.): Ochrona informacji niejawnych, biznesowych i danych osobowych, Katowice: KSOIN – UŚ, 2010. s. 57-62.

183 A. Drozd: *Ustawa o ochronie* …, s. 329.

184 Patrz: Information Security Service – www.bezpieczneinformacje.pl.

185 A. Drozd: *Zabezpieczenie danych* …, s. 73-80.

a) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
b) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
c) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
d) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
e) sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii bezpieczeństwa;
f) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania szkodliwego;
g) sposób realizacji wymogów odnotowywania informacji o odbiorcach danych;
h) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych (§5).

Niemniej jednak „Polityka", jak sama nazwa wskazuje, powinna być **zbiorem zasad**, a nie kolekcją wykazów i spisów uzupełnioną o nie zawsze zrozumiałe procedury informatyczne jak sugeruje Rozporządzenie ws. dokumentacji. Zatem w „Polityce" należy przede wszystkim **jasno i czytelnie** określić zasady dotyczące przetwarzania danych osobowych w organizacji, uwzględniając realizację wszystkich obowiązków ustawowych Administratora danych osobowych, do których to załącznikiem powinny być określone w Rozporządzeniu ws. dokumentacji wykazy[186]. Ponadto należy zauważyć, że opracowanie „Polityki" zawierającej wyłącznie wskazane w Rozporządzeniu ws. dokumentacji elementy składowe **nie wypełnia wymogów ustawowych**, przede wszystkim obowiązku „szczególnej staranności"[187]. Korzystając z międzynarodowych standardów dokumentowania systemów zarządzania bezpieczeństwem informacji[188], zalecanych również przez Generalnego Inspektora[189], przyjąć należy, że całościowa „**Polityka**" powinna składać się z takich generalnych części:
1) Deklaracja Administratora danych osobowych.
2) Wprowadzenie.
3) Struktura zarządzania bezpieczeństwem.
4) Dostęp do zbiorów danych osobowych.
5) Dostęp do strefy przetwarzania.
6) Zabezpieczenia dokumentacji tradycyjnej.
7) Zabezpieczenia systemu informatycznego.
8) Rejestracja zbiorów danych osobowych.
9) Powierzanie danych osobowych do przetwarzania.
10) Zarządzanie incydentami.
11) Audyt i aktualizacja dokumentacji[190].

Dopiero tak stworzony dokument określający wszystkie ustawowo wymagane zasady bezpieczeństwa przetwarzanych danych osobowych pozwala na dołączenie do niego, w formie na bieżąco aktualizowanych załączników, wykazów i spisów wymaganych przez Rozporządzenie ws. dokumentacji[191]. **Deklaracja Administratora danych osobowych** powinna otwierać „Politykę". Oświadczenie kierownictwa organizacji jest zawsze obowiązkowym elementem wszelkich dokumentów związanych z procesem zarządzania. Przedstawia ona intencję Administratora danych osobowych, cele i zasady wprowadzonych regulacji, a także wskazuje na bezpośrednie zaangażowanie całej organizacji w ten proces.

---

186 M. Byczkowski: Zarządzanie procesami przetwarzania …, s. 35.

187 A. Drozd: *Ustawa o ochronie* …, s. 342.

188 Patrz: PN-EN ISO/IEC 27001:2014 – 1/2: Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania, Warszawa: Polski Komitet Normalizacyjny, 2014.

189 A. Kaczmarek (opr.): *Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa*, Warszawa: Biuro Generalnego Inspektora Ochrony Danych Osobowych, bdw. Dostępne pod adresem: http://www.giodo.gov.pl, (10.11.2015); A. Kaczmarek (opr.): *Wskazówki dotyczące sposobu opracowania instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji*, Warszawa: Biuro Generalnego Inspektora Ochrony Danych Osobowych, bdw. Dostępne pod adresem: http://www.giodo.gov.pl (10.11.2015).

190 Ł. Kister: Polityka bezpieczeństwa …, s. 14..

191 Przedstawiony układ „Polityki" jest projektem autorskim, opracowanym na podstawie szerokiej literatury przedmiotu, wytycznych międzynarodowych standardów bezpieczeństwa informacji

Przykładowy fragment treści:
Zarząd Spółki świadomy znaczenia przetwarzanych danych osobowych, przykłada najwyższą wagę do zapewnienia im odpowiedniego poziomu bezpieczeństwa, ponieważ mają one fundamentalne znaczenia dla realizacji misji i celów statutowych, a ich zgodne z prawem wykorzystanie pozwala na budowę przewagi rynkowej.
Dane osobowe stanowią kluczowe zasoby informacyjne Spółki i jako takim zapewnia się odpowiednią ochronę.

Można się spotkać z potocznymi opiniami, że dokument tego rodzaju nie ma żadnego znaczenia dla praktycznej realizacji procesu zarządzania bezpieczeństwem przetwarzanych danych osobowych. Doświadczenie pokazuje, że jest wręcz przeciwnie. **Wprowadzenie** ma za zadanie wskazać podstawy prawne, cel faktyczny oraz określić podstawowe zasady stosowania „Polityki".

Przykładowy fragment treści:
W celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych stosuje się następujące zasady generalne:
- wiedzy koniecznej – każdy pracownik posiada dostęp do danych osobowych ograniczony wyłącznie do tych, które są mu niezbędne do realizacji powierzonych obowiązków służbowych;
- bezwzględnej poufności – każdy pracownik posiadający dostęp do danych osobowych ma obowiązek zachowania w tajemnicy tych danych oraz zasad ich ochrony, także po ustaniu stosunku pracy;
- indywidualnej odpowiedzialności – każdy pracownik posiada jednoznacznie określony zakres indywidualnej odpowiedzialności za przetwarzane dane osobowe;
- czystego biurka – zabronione jest pozostawianie na stanowisku pracy jakichkolwiek dokumentów lub nośników zawierających dane osobowe po zakończeniu dnia pracy lub w trakcie czasowej nieobecności.

Ponadto we wstępie należy **zdefiniować pojęcia** użyte w treści dokumentu. W szczególności powinno to dotyczyć terminów niejasnych lub o odmiennym od potocznego znaczeniu. **Struktura zarządzania bezpieczeństwem**, to ten rozdział „Polityki", którego zadaniem jest wskazanie ról w procesie przetwarzania danych osobowych:
- Administratora danych osobowych;
- Administratora bezpieczeństwa informacji;
- Administratora systemu informatycznego;
- Gestora zbioru danych osobowych, tj. osób odpowiedzialnych za poszczególne zbiory lub procesy przetwarzania.

Należy bezpośrednio zidentyfikować te osoby oraz przypisać im **zakresy odpowiedzialności** i uprawnienia. Pracownicy muszą wiedzieć, kto i w jakim zakresie podejmuje decyzje władcze w procesie przetwarzania danych osobowych[192]. Najobszerniejszy blok „Polityki" odnosi się do **strategii zabezpieczenia** danych osobowych. Powinien on kompleksowo i przystępnie przedstawić środki organizacyjne i techniczne przyjęte przez Administratora danych osobowych w celu zapewnienia integralności, rozliczalności, dostępności i poufności przetwarzanych danych osobowych. Obejmuje on omówione w poprzednim rozdziale procedury opisujące obszary:
1) bezpieczeństwa osobowego,
2) bezpieczeństwa fizycznego,
3) bezpieczeństwa informatycznego.

Ze względów hierarchii oraz chronologii pierwszym z rozdziałów w tym bloku jest „**Dostęp do zbiorów danych osobowych**", który powinien co najmniej określić zasady związane z:
- nadawaniem, ewidencjonowaniem oraz odbieraniem „Upoważnień do przetwarzania danych osobowych";
- potwierdzaniem zobowiązań do zachowania poufności.

Przykładowy fragment treści:
Osoba, dla której wydano upoważnienie, przed uzyskaniem dostępu do danych osobowych zapoznaje się z niniejszą Polityką, a następnie podpisuje oświadczenie potwierdzające zapoznanie się z zasadami bezpieczeństwa oraz składa zobowiązanie dotyczące zachowania poufności.

[192] Dane identyfikujące te osoby, w celu uniknięcia konieczności niepotrzebnej aktualizacji całej „Polityki" w przypadku ich zmiany, należy umieścić w odpowiednim wykazie stanowiącym jeden z załączników.

Ze względów poprawności logicznej w tym miejscu należy zasygnalizować również ogólne zasady udzielania dostępu do zbiorów danych osobowych **przetwarzanych w systemie informatycznym**. Jeżeli nie tworzy się odrębnego rozdziału, zasady **obowiązkowych szkoleń** można umieścić także w tym rozdziale. Następnie umieszczamy procedury **dostępu do strefy przetwarzania**, których zadaniem jest wskazanie zasad uprawnionego przebywania w pomieszczeniach przeznaczonych do przetwarzania danych osobowych.

Przykładowy fragment treści:
Do pomieszczeń strefy przetwarzania nieograniczony dostęp mają wyłącznie pracownicy wykonujący w nich zadania służbowe.
Osoby „trzecie" mogą przebywać w tych pomieszczeniach wyłącznie w obecności osób upoważnionych i tylko w uzasadnionych przypadkach.
Niedopuszczalne jest pozostawianie osób „trzecich" w pomieszczeniach strefy przetwarzania bez nadzoru osób upoważnionych, jak również umożliwianie im dostępu do tych pomieszczeń podczas swojej nieobecności.

Zupełnie pomijanym w większości opracowań jest rozdział dotyczący **zabezpieczenia dokumentacji tradycyjnej**. Jego rolą jest wskazanie podstawowych standardów postępowania z księgami, aktami, rejestrami i wykazami w formie papierowej:

- wytwarzanie;
- przechowywanie;
- archiwizowanie;
- niszczenie.

Przykładowy fragment treści:
Główną zasadą bezpiecznego przetwarzania dokumentacji tradycyjnej jest „zasada czystego biurka", przez którą należy rozumieć bezwzględny zakaz pozostawiania na stanowisku pracy jakichkolwiek dokumentów bez nadzoru.
Po zakończeniu dnia pracy wszystkie dokumenty tradycyjne, które zawierają dane osobowe należy umieścić w zamykanych na klucz szafkach.

Kolejne rozdziały tego bloku odnoszą się już do bardziej szczegółowych zasad związanych z **zarządzaniem systemem informatycznym** służącym do przetwarzania danych osobowych – od tych dotyczących bezpośredniego przetwarzania danych osobowych, po te związane z utrzymaniem systemu informatycznego. Zaczynamy od procedur dostępu do systemu informatycznego, których najważniejszym celem jest wskazanie **zasad uwierzytelniania** i związanych z tym obowiązków.

Przykładowy fragment treści:
Hasło służące do uwierzytelniania w systemie informatycznym stanowi indywidualną własność użytkownika i może być znane wyłącznie jemu.
Bezwzględnie zabrania się ujawniania, udostępniania i zapisywania haseł dostępu.

Ponadto w rozdziale tym można opisać niezrozumiałe już dzisiaj, ale ciągle wymagane przez Rozporządzenie ws. dokumentacji kwestie: rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym. Następnie określa się procedury użytkowania **komputerowych nośników danych**, w tym w szczególności:

- inwentaryzacja nośników;
- wykorzystywanie nośników do przenoszenia danych osobowych;
- przechowywanie nośników;
- niszczenie nośników.

Przykładowy fragment treści:
Komputerowe nośniki danych zawierające dane osobowe należy bezwzględnie przechowywać w zamkniętych na klucz szafach, a po ich wykorzystaniu dane w nich zawarte trwale usuwać lub nośniki te zniszczyć.
Komputerowe nośniki danych, które są przeznaczone do przenoszenia danych osobowych poza „strefę przetwarzania" należy bezwzględnie poddać zaszyfrowaniu.

W rozdziale dotyczącym **urządzeń mobilnych** należy umieścić podstawowe zasady ich bezpiecznego wykorzystywania, w szczególności poza „strefą przetwarzania" i możliwością realizacji zdalnego dostępu do systemu informatycznego.

Przykładowy fragment treści:
Użytkownicy, którym zostały powierzone urządzenia mobilne, powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych.
Urządzenia mobilne wyniesione poza „strefę przetwarzania" nie powinny być pozostawione bez nadzoru, w szczególności w samochodach, hotelach i innych miejscach publicznych.

Ochrona antywirusowa powinna obejmować opis zabezpieczeń systemu informatycznego przed działalnością oprogramowania szkodliwego, którego celem jest zdobycie nieuprawnionego dostępu. W rozdziale tym należy wskazać, że wszelkie procedury antywirusowe dotyczą także urządzeń mobilnych i komputerowych nośników danych.

Przykładowy fragment treści:
W stosunku do urządzeń mobilnych zastosowanie mają wszelkie procedury bezpieczeństwa antywirusowego stosowane wobec stacji roboczych.
Komputerowe nośniki danych pochodzące od podmiotów „zewnętrznych" nie mogą zostać użyte w systemie informatycznym bez wcześniejszego przetestowania oprogramowaniem antywirusowym.

Formalnym opisem podstawowych zadań Administratora danych osobowych związanych z kontrolą procesu przetwarzania danych osobowych powinien być rozdział dotyczący **monitorowania systemu informatycznego**, który określi procedury:
- kontroli dostępu do systemu informatycznego;
- odnotowywania informacji o czynnościach wykonywanych na danych osobowych;
- zarządzania dostępem do sieci publicznej – Internetu.

Przykładowy fragment treści:
System informatyczny jest wyposażony w mechanizmy ograniczające liczbę nieudanych prób rejestracji.
Blokowanie konta użytkownika następuje po przekroczeniu pięciu nieudanych prób rejestracji.

Rozdział dotyczący **kopii bezpieczeństwa** określa procedury:
- częstotliwości tworzenia;
- testowania;
- przechowywania nośników.

W treści tego rozdziału nie należy wskazywać dokładnej lokalizacji miejsca, w którym są przechowywane kopie bezpieczeństwa, a jedynie sposób ich zabezpieczenia.

Przykładowy fragment treści:
Nośniki kopii bezpieczeństwa przechowuje się w odpowiednio zabezpieczonym pomieszczeniu, w warunkach minimalizujących zagrożenie ze strony sił przyrody oraz silnego pola elektromagnetycznego.
Zabrania się przechowywania kopii bezpieczeństwa w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.

Blok ten powinien zamykać rozdział dotyczący **bezpieczeństwa zasobów sprzętowych**, obejmujący przede wszystkim procedury:
- wprowadzania do użytku sprzętu komputerowego;
- zasilania awaryjnego urządzeń;
- przeglądów, konserwacji i napraw sprzętu komputerowego;
- wycofywania z użycia i utylizacji sprzętu komputerowego.

Przykładowy fragment treści:
W celu zapewnienia odpowiedniej poufności, dostępności i integralności przetwarzanych danych osobowych, system informatycznym jest poddawany systematycznym przeglądom.
Czynności wykonywane przez zewnętrznych serwisantów muszą być ściśle nadzorowane i prowadzone w „strefie przetwarzania".
Wszystkie awarie, które miały lub mogłyby mieć wpływ na bezpieczeństwo przetwarzanych danych osobowych muszą być bezwzględnie zgłaszane do Administratora danych osobowych.

Niezbędną w praktyce częścią „Polityki" powinno być określenie zasad i obowiązków związanych z **rejestracją zbiorów danych osobowych**:

- procedury zgłoszenia zbioru danych osobowych do rejestracji;
- sposób prowadzenia rejestru zbiorów danych osobowych.

Przykładowy fragment treści:
Gestor zbioru jest zobowiązany do niezwłocznego informowania Administratora danych osobowych o wszelkich zmianach odnoszących się do przetwarzanych zbiorów danych osobowych, w szczególności dotyczących zawartości informacyjnej i celu przetwarzania.

Szczególnie dla przedsiębiorców jest istotne określenie zasad **powierzania danych osobowych innym podmiotom**, w których powinny znaleźć się wymagania dotyczące:

- zasad zawierania i treści umowy powierzenia danych osobowych do przetwarzania;
- nadzoru nad przetwarzaniem powierzonych zbiorów danych osobowych.

Przykładowy fragment treści:
Przed zawarciem umowy powierzenia danych osobowych do przetwarzania podmiotowi zewnętrznemu, należy bezwzględnie potwierdzić, czy spełnia on wymogi w zakresie zabezpieczeń organizacyjno-technicznych oraz dokumentacji procesu przetwarzania danych osobowych, gwarantując właściwy poziom ochrony interesów osób, których dane dotyczą.

Przedostatnim elementem „Polityki" powinien być opis procedur **postępowania z incydentami** naruszającymi bezpieczeństwa danych osobowych[193]:

- tryb zgłaszania wszelkich naruszeń lub sytuacji nienaturalnych;
- zasady podejmowania działań zabezpieczających dane osobowe;
- dokumentowanie incydentów i prowadzenie czynności wyjaśniających;
- procedury przywracania normalnego przetwarzania danych osobowych;
- zasady powiadamiania właściwych organów państwowych.

Przykładowy fragment treści:
Każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do informowania przełożonego o wszelkich zauważonych lub podejrzanych słabościach procesu przetwarzania danych osobowych, a w szczególności o:

- naruszeniu hasła i identyfikatora, uprawniających do pracy w systemie informatycznym;
- częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień;
- braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera;
- itd.

[193] Obowiązek odrębnej instrukcji w tym zakresie istniał w nieobowiązującym już Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 roku *w sprawie określenia podstawowych warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych*, (Dz.U. nr 80, poz. 521, zm. Dz.U. 2001, nr 121, poz. 1306).

Ostatnią merytoryczną częścią „Polityki" powinny być procedury związane z:

- **audytowaniem procesu przetwarzania danych osobowych**[194];
- **aktualizacją dokumentacji bezpieczeństwa**.

Przykładowy fragment treści:
Administrator bezpieczeństwa informacji wspólnie z Administratorem systemu informatycznego są zobowiązani do cyklicznego przeprowadzania audytów w obszarze wybranych procedur przetwarzania danych osobowych. Częstotliwość audytów nie może być mniejsza niż 6 miesięcy.

Dokument „Polityki" może być zakończony **postanowieniami organizacyjnymi**, np. terminem wejścia w życie, okresem wdrożenia, itp., oraz **rejestrem zmian i aktualizacji**.

Przykładowy rejestr zmian:

Numer wersji	Data zmiany	Zmiany wprowadził	Opis zmian
1.0	20.11.2015	Łukasz Kister	Opracowanie wersji ostatecznej.
1.1	23.11.2015	Łukasz Kister	Uaktualnienie nazw działów.

Podsumowując należy zaznaczyć bardzo ważną kwestię związaną z treścią „Polityki". Zawartość jej nie powinna zawierać żadnych szczegółów technicznych zastosowanych zabezpieczeń, np. nazwy systemu antywirusowego, a jedynie wskazanie zasad bezpieczeństwa i uzasadnienie ich stosowania w odniesieniu do założonych celów[195]. Szczegółowe procedury techniczne dla Administratora bezpieczeństwa informacji, Administratora systemu informatycznego czy innych osób odpowiedzialnych za bezpieczeństwa organizacji powinny znaleźć się w odrębnych instrukcjach oraz dokumentacji systemu informatycznego, niedostępnych dla zwykłych pracowników.

Studium przypadku:
Polityka bezpieczeństwa danych osobowych zawierająca szczegółowy schemat sieci teleinformatycznej oraz jej zabezpieczenia to najlepsze źródło wiedzy dla potencjalnych działań niepożądanych, np. ze strony zwalnianego dyscyplinarnie pracownika.

5.1.3. OBOWIĄZKOWE ZAŁĄCZNIKI

Zgodnie z określonymi w poprzednim podrozdziale warunkami poprawności formy i zawartości „Polityki", obowiązkowymi załącznikami do tego dokumentu winny być **opisy infrastruktury przetwarzania danych osobowych**:

1) Strefa przetwarzania danych osobowych.
2) Zbiory danych osobowych.

Pominięcie tych elementów będzie stanowiło złamanie dyspozycji Rozporządzenia ws. dokumentacji, które uznaje je za podstawowe elementy dokumentacji systemu zabezpieczeń przetwarzanych danych osobowych (§4). Opis „**Strefy przetwarzania danych osobowych**" powinien szczegółowo wskazywać miejsca, w których odbywają się jakiekolwiek procesy przetwarzania danych osobowych, tj.:

- pomieszczenia biurowe;
- pomieszczenia serwerowni i innych elementów systemu informatycznego;
- archiwa i składnice akt;
- szafy do przechowywania dokumentacji tradycyjnej i komputerowych nośników danych, jeżeli znajdują się poza pomieszczeniami biurowymi.

Obowiązek umieszczenia w tym wykazie nie dotyczy wyłącznie pomieszczeń w obiektach należących do Administratora danych osobowych lub przez niego zarządzanych, ale także lokalizacji:

- zewnętrznej serwerowni głównej lub zapasowej;

[194] W tym względzie można skorzystać ze standardu audytowania określonego w międzynarodowej normie: PN-EN ISO 19011:2012 – *Wytyczne dotyczące auditowania systemów zarządzania*, Warszawa: Polski Komitet Normalizacyjny, 2012.
[195] Ł. Kister: Polityka bezpieczeństwa …, s. 16.

- skrytki bankowej, w której są przechowywane kopie bezpieczeństwa;
- punktów dostępowych do systemu informatycznego znajdujących się u innych podmiotów[196].

Przykładowy wykaz:

l.p.	Obiekt	Adres	Pomieszczenia (numer lub inna identyfikacja)
1.	Centrala firmy	Warszawa, ul. Malinowa 12	Parter: 2, 3, szafa nr 1 (korytarz) I piętro: 11, 12, 15, 17. II piętro: 22, 24, szafa nr 2 (korytarz)
2.	Big Data	Wrocław ul. Dyskowa 1	Serwerownia

Praktyka wymusza, by w celu zapewnienia właściwego poziomu bezpieczeństwa krytycznym elementom systemu informatycznego, **zaleca się**, by w wykazie pomieszczeń tworzących „strefę przetwarzania danych osobowych" **nie umieszczać** szczegółowych danych pozwalających na lokalizację serwerowni głównej i zapasowej oraz miejsca przechowywania kopii bezpieczeństwa. Szczególnie w sytuacji gdy dotyczy to obiektu biurowego Administratora danych osobowych.

Drugim załącznikiem winien być opis „**Zbiorów danych osobowych**", na który składają się:

1) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
2) wskazanie struktury informacyjnej zbiorów danych osobowych,
3) opis przepływu danych pomiędzy poszczególnymi elementami systemu informatycznego, służącymi do przetwarzania danych osobowych w zbiorze.

Wykaz „Zbiorów danych osobowych" powinien przede wszystkim zawierać takie informacje, jak:

1) nazwa zbioru danych osobowych;
2) nazwa aplikacji informatycznej służącej do przetwarzania danych osobowych w tym zbiorze.

Generalny Inspektor wymaga ponadto, żeby wykaz ten zawierał dodatkowo lokalizację:

- miejsc, w których znajdują się zbiory danych osobowych;
- stanowisk komputerowych używanych do ich przetwarzania[197].

Dopełniając kompleksowość takiego wykazu, należy rozważyć, by wskazywał on także na inne elementy, dające pełny obraz zbioru danych osobowych, tj.:

1) nazwę ewidencji tradycyjnej, stanowiącej element całego zbioru;
2) lokalizację przechowywania ewidencji tradycyjnych.

Przykładowy wykaz:

l.p.	Zbiór danych osobowych	Lokalizacja Zbioru	Nazwa aplikacji / ewidencji	Pomieszczenia przetwarzania
1.	Kadry i płace	Serwerownia	Super Kadry	pok. 12, 13, 15, 21
		pok. 12	Akta osobowe	pok. 12, 13

Zasadnym jest również **uzupełnienie** przedmiotowej ewidencji o informacje dotyczące przetwarzania danych osobowych w każdym z wymienionych zbiorów danych osobowych:

- cel przetwarzania i jego podstawa prawna;
- źródło pochodzenia danych osobowych w zbiorze;
- kategoria osób, których dane dotyczą;
- spełnienie lub zwolnienie z obowiązku rejestracji;
- udostępnienie danych innemu podmiotowi i jego podstawa.

[196] A. Kaczmarek (opr.): Wytyczne w zakresie opracowania …, s. 3-4.
[197] A. Kaczmarek (opr.): Wytyczne w zakresie opracowania …, s. 5.

Struktura informacyjna zbioru danych osobowych to wyszczególnienie wszystkich pól informacyjnych w strukturze zbioru, które powinny jednoznacznie wskazywać, jakie kategorie danych są w nich przechowywane, np. imię, nazwisko, data urodzenia, miejsce zamieszkania, itd.

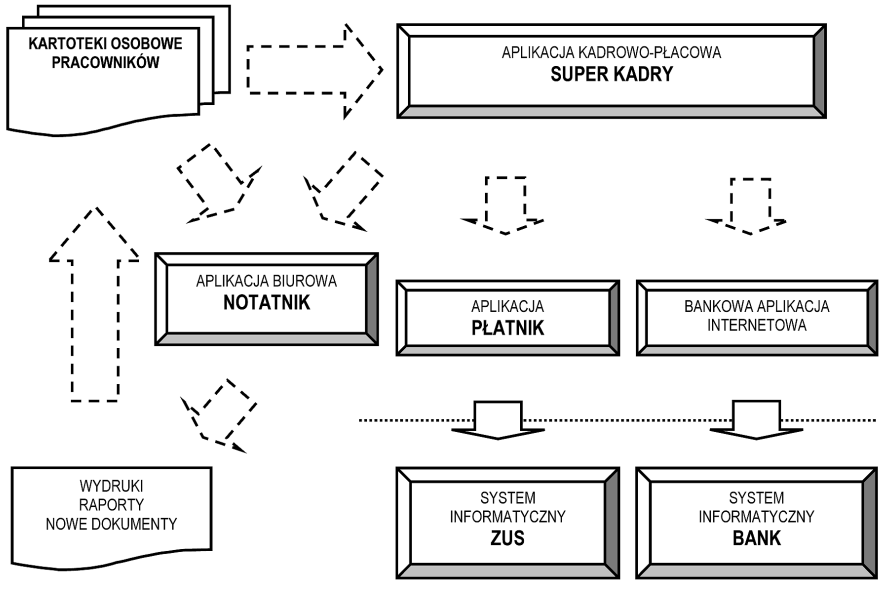
Przykładowy układ wykazu:

l.p.	Zbiór danych osobowych	Zawartość informacyjna
1.	Kadry i płace	nazwisko, imię, imię ojca, imię matki, data urodzenia, numer PESEL, dane adresowe, numer telefonu, seria i numer dokumentu tożsamości, obywatelstwo, wykształcenie, tytuł zawodowy, data ukończenia szkoły, …

Dodatkowo dla każdego zbioru danych osobowych istnieje wymóg opisania **powiązań** pomiędzy poszczególnymi polami informacyjnymi. Należy przez to rozumieć konieczność wskazania wszystkich tych danych, występujących w strukturze zbioru, które poprzez występujące relacje można skojarzyć z określoną osobą, np. identyfikator towaru pozwala na ustalenie identyfikatorów klientów, którzy dokonali jego zakupu, a to z kolei pozwala na dostęp do danych osobowych klientów[198]. W praktyce jednak jest to obowiązek zupełnie niezrozumiały, a w przypadku większości współczesnych zbiorów – niemożliwy do realizacji. **Przepływ danych pomiędzy elementami systemu informatycznego** ma na celu przedstawienie procesu przetwarzania danych osobowych, ze szczególnym uwzględnieniem biorących w nim udział aplikacji i sposobu przesyłania danych pomiędzy nimi. Szczególne znaczenie ma tu właściwe opisanie rodzaju danych i sposobu ich eksportu **poza system** Administratora danych osobowych.

Ciągle najpopularniejszym sposobem realizacji tego wymogu jest przedstawienie tych relacji w formie graficznej.

Przykładowa prezentacja:



Podsumowując tą cześć należy powtórzyć argument o **archaicznym wymogu** tworzenia przedmiotowych wykazów i opisów. Praktyka i piśmiennictwo pokazują ponadto, że często niezwykle trudne jest spełnienie tych wymagań, np. konieczności wskazania powiązań pomiędzy poszczególnymi polami informacyjnymi w przypadku relacyjnych baz danych, których podstawową cechą jest możliwość tworzenia dowolnych relacji i ich modyfikacja w krótkim czasie. W związku z tym jest postulowana konieczność **rezygnacji z obowiązkowych wykazów i spisów,** jako nadmiernych informacji w stosunku do potrzeb ochrony danych osobowych, którym ma służyć „Polityka bezpieczeństwa danych osobowych"[199].

[198] A. Kaczmarek (opr.): *Wytyczne w zakresie opracowania* …, s. 8-10.
[199] Fajgielski P.: Obowiązki związane z zabezpieczeniem …, s. 145.

5.1.4. WDROŻENIE PROCEDUR BEZPIECZEŃSTWA

Zgodnie z dyspozycją Rozporządzenia ws. dokumentacji Administrator danych osobowych jest zobowiązany nie tylko do opracowania „Polityki bezpieczeństwa danych osobowych", ale przede wszystkim do jej **wdrożenia** (§3 ust. 3). Nie należy jednak rozumieć przez to wyłącznie podpisania **wewnętrznego zarządzenia** wprowadzającego „Politykę bezpieczeństwa danych osobowych" jako dokumentu obowiązującego wszystkich pracowników. (Chociaż nawet ten element bywa bardzo często pomijany w różnego rodzaju firmach, gdzie przygotowana „Polityka" nigdy nie uzyskała faktycznego obowiązywania, z uwagi na brak jej formalnego włączenia do systemu prawnego organizacji).

Polityka powinna zostać **opublikowana**, tj. udostępniona dla wszystkich pracowników i współpracowników firmy. Z jej treścią należy bezwzględnie zapoznać wszystkie osoby, które mają lub będą miały dostęp do procesu przetwarzania danych osobowych, ale także pozostałe osoby, których zachowania mogą mieć wpływ na jego bezpieczeństwo.

Studium przypadku:
Personelowi sprzątającemu nie nadaje się „Upoważnień do przetwarzania danych osobowych", ale musi on mieć niezbędną wiedzę w zakresie podstawowych zasad zachowania się w sytuacji stwierdzenia niewłaściwie zabezpieczonych dokumentów zawierających dane osobowe.

Najskuteczniejszym sposobem wykonania tego obowiązku jest przeprowadzenie serii **szkoleń** prezentujących istotę ochrony danych osobowych oraz zasady bezpieczeństwa określone w nowo wdrażanej dokumentacji. Najlepiej żeby te szkolenia były podzielone pod względem poziomu niezbędnej wiedzy, tj. odrębne dla każdego pionu oraz inne dla ich kierowników, a inne dla osób, które będą bezpośrednio realizowały proces przetwarzania danych osobowych. Wymaga to jednak właściwego przygotowania wykładowego.

Studium przypadku:
Szkolenia polegające na odczytaniu wymagań ustawowych lub prowadzone językiem zrozumiałym wyłącznie dla informatyków odnoszą skutek odmienny od oczekiwanego.
W pierwszym przypadku pracownicy dowiedzą się, że wszystkie obowiązki spoczywają na szefie, a w drugim, że ich wykonawcą jest informatyk, nie rozumiejąc żadnego z nich.

Niemniej jednak najważniejszym elementem procesu wdrożenia nowego systemu ochrony danych osobowych jest **wprowadzenie do codziennej działalności** firmy wszystkich opisanych procedur bezpieczeństwa. W tym względzie jest zalecane założenie okresu przejściowego, w którym będą implementowane kolejne wymagane zmiany. Nie może to następować w sposób chaotyczny i przypadkowy, ale powinno stanowić efekt zaplanowanej strategii. Pracownicy muszą nie tylko realizować określone zadania, ale również rozumieć ich istotę i cel.

Studium przypadku:
Przedsiębiorca nie powinien wymuszać na pracownikach przestrzegania wszystkich procedur pracy z komputerami przed ukończeniem dostosowywania samego systemu informatycznego do wymogów zmienionych zasad bezpieczeństwa.

Ponadto w trakcie trwania takiego rozłożonego w czasie procesu wdrażania powinna istnieć możliwość **wprowadzania korekt**. Żaden, nawet najlepiej przygotowany dokument mający opisywać jednolite zasady bezpieczeństwa dla różnych obszarów działalności organizacji, nie będzie w swojej pierwszej wersji idealnie dopasowany.

Studium przypadku:
Jednym z częściej spotykanych przypadków niezgodności wdrażanego systemu jest występujący w starszych aplikacjach brak możliwości wymuszenia automatycznej zmiany i siły hasła.
Nie należy w takiej sytuacji pozostawiać zapisu procedury niezgodnej ze stanem faktycznym, a uzupełnić ją o możliwe wyjątki.

Ciągłe doskonalenie procedur jest istotą i warunkiem skuteczności działających systemów bezpieczeństwa – tzw. „Cykl Deminga".

W tym miejscu należy poruszyć bardzo ważny problem **dostępności dokumentacji** systemu zarządzania bezpieczeństwem danych osobowych. Zgodnie z dyspozycją Ustawy, zasady zabezpieczenia danych osobowych podlegają **bezwzględnej tajemnicy** (art. 39 ust. 2). Dlatego też „Polityka bezpieczeństwa danych osobowych" – bez względu na

swoją ogólności – nie może być w żaden sposób publikowana w Internecie[200], ani też udostępniana osobom, które nie zobowiązały się do zachowania jej w poufności.

5.2. REJESTRY ZBIORÓW DANYCH OSOBOWYCH

Zbiory danych osobowych są podstawowym przedmiotem regulacji ustawowej. Możliwość otwartej kontroli ich tworzenia, a następnie prowadzenia przez Administratora danych osobowych, stanowi istotę całego systemu sprawowania **nadzoru nad legalnością** przetwarzania danych osobowych, zarówno ze strony Generalnego Inspektora, jak również – a może nawet przede wszystkim – indywidualnej ze strony osób, których dane dotyczą.

Transparentność procesu przetwarzania danych osobowych jest warunkiem koniecznym dla zapewnienia gwarancji nienaruszalności istoty konstytucyjnego prawa do autonomii informacyjnej jednostki. W związku z tym niezbędnym warunkiem zapewniającym tą właściwość jest powszechna dostępność do możliwości ustalenia istnienia konkretnego zbioru, jego administratora, celu, rodzaju i zakresu przetwarzania w nim danych osobowych.

Reasumując wprowadzenie należy jednocześnie obalić ciągle żywą potoczną opinię, że rejestracja zbioru danych osobowych jest kluczowym obowiązkiem Administratora danych osobowych. Najważniejsze jest spełnienie warunków dopuszczających przetwarzanie danych osobowych, następnie ich skuteczne zabezpieczenie przed działaniami niepożądanymi, a rejestracja jest **ostatnim z obowiązków** – oświadczeniem o ich wypełnieniu.

5.2.1. OGÓLNOKRAJOWY REJESTR ZBIORÓW DANYCH OSOBOWYCH

Podstawową ustawową zasadą rejestracji zbioru danych osobowych jest obowiązek zgłoszenia do rejestru prowadzonego przez **Generalnego Inspektora Ochrony Danych Osobowych** (art. 40). Obowiązek rejestracyjny dotyczy **wszelkich zbiorów** danych osobowych, bez względu na:

- kategorię przetwarzanych danych osobowych, tj. zwykłe czy wrażliwe;
- rodzaj przetwarzanych danych osobowych, tj. zawartość informacyjna dla każdej z osób;
- wielkość zbioru, tj. liczby przetwarzanych w nim informacji[201].

Studium przypadku:
Zbiór danych osobowych wykorzystywany na potrzeby marketingu własnych towarów składający się z kilkudziesięciu rekordów informacyjnych zawierających wyłącznie: imię, nazwisko, adres e-mail; podlega obowiązkowej rejestracji.

Nie występuje jednak związanie obowiązkiem rejestracyjnym w sytuacji, gdy zbiór danych osobowych jeszcze nie powstał, bez względu na to, czy ostatecznie do tego dojdzie[202]. Adresatem obowiązku zgłoszenia zbioru danych osobowych do rejestru prowadzonego przez Generalnego Inspektora jest wyłącznie **Administrator danych osobowych** (art. 40). Nie jest to więc każdy przetwarzający dane osobowe, a ten komu przysługuje status uprawniający do decydowania o celach i środkach tego przetwarzania.

Studium przypadku:
Przedsiębiorca prowadzący kancelarię podatkową ma obowiązek zarejestrowania wyłącznie zbiorów danych osobowych, dla których jest Administratorem danych osobowych.
Nie może one rejestrować zbiorów danych podatkowych pracowników swoich klientów.

Nie istnieje jednak przeciwwskazanie, żeby formalnych czynności związanych z poszczególnymi etapami rejestracji zbioru danych osobowych dokonywał właściwie upoważniony pełnomocnik[203]. Zgłoszenie zbioru jest dokonywane na **sformalizowanym druku zgłoszenia** – jednolitym dla wszystkich Administratorów danych osobowych (art. 46a), którego wizualizację stanowi załącznik do Rozporządzenie ws. wzoru zgłoszenia zbioru.

Do „Wniosku o rejestrację zbioru" **nie należy załączać**:

- wydrukowanej lub zapisanej na komputerowym nośniku zawartości informacyjnej zbioru danych osobowych;
- dokumentacji systemu zabezpieczeń przetwarzanych danych osobowych.

---

[200] Problem ten dotyczy głównie instytucji publicznych, które z nieznanych powodów publikują swoje procedury bezpieczeństwa na stronach Biuletynu Informacji Publicznej, np.: Urząd Województwa Świętokrzyskiego, Urząd Marszałkowski Województwa Wielkopolskiego, Urząd Miasta w Krynicy Zdroju, i in..

[201] A. Drozd: *Ustawa o ochronie* …, s. 277.

[202] P. Barta, P. Litwiński: *Ustawa o ochronie* …, s. 429-430.

[203] P. Barta, P. Fajgielski, R. Markiwicz: *Ochrona danych osobowych* …, s. 641.

Studium przypadku:
Przedsiębiorca, który nadał pocztą„Wniosek o rejestrację zbioru", dołączając do niego płytę DVD zawierającą zawartość informacyjną tego zbioru, może ponieść odpowiedzialność karną za udostępnienie danych osobowych nieuprawnionemu podmiotowi, lub przynajmniej niewłaściwe zabezpieczenie nośników danych osobowych wyniesionych poza„strefę przetwarzania".

Aktualnie istnieją realnie dwa **sposoby złożenia wniosku** o rejestrację zbioru danych osobowych:

1) Półautomatyczny, który polega na takich kolejnych działaniach, jak:
   a) wypełnienie elektronicznego formularza wniosku znajdującego się na platformie internetowej Generalnego Inspektora[204] i wstępnego zatwierdzenia jego treści – nie wymaga to posiadania podpisu elektronicznego i nie jest formalnym potwierdzeniem złożenia wniosku;
   b) wydrukowanie wniosku i podpisanie go przez Administratora danych osobowych lub osobę przez niego właściwie upoważnioną;
   c) przesłanie wniosku pocztą na adres Biura Generalnego Inspektora[205].
2) Automatyczny, który polega na wykonaniu takich działań, jak:
   a) wypełnieniu elektronicznego formularza wniosku znajdującego się na platformie internetowej Generalnego Inspektora;
   b) zatwierdzenie jego treści poprzez uwierzytelnienie przez Administratora danych osobowych lub osobę przez niego właściwie upoważnioną przy użyciu mechanizmów podpisu elektronicznego[206] – formalne złożenie wniosku.

Uznaje się, że obowiązek rejestracji zbiorów danych osobowych jest szczególnym elementem systemu nadzoru ze strony Generalnego Inspektora. Na podstawie złożonych wniosków ma on możliwość, co najmniej **wstępnej kontroli zgodności przetwarzania** danych osobowych z wymogami prawa[207].

Jakiekolwiek stwierdzone naruszenie podstawowych zasad dopuszczalności przetwarzania danych osobowych lub ich niewłaściwe zabezpieczenie, skutkuje wydaniem decyzji administracyjnej **odmawiającej rejestracji** zbioru danych osobowych (art. 44 ust. 1), a przede wszystkim **nakazującej**:

- zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe;
- nieudostępnianie danych osobowych innym podmiotom;
- wstrzymanie przekazywania danych osobowych do państwa spoza Europejskiego Obszaru Gospodarczego;
- ograniczenie przetwarzania wszystkich albo niektórych kategorii danych wyłącznie do ich przechowywania;
- przekazanie danych innemu podmiotowi, który gwarantuje ich zgodne z prawem zabezpieczenie;
- usunięcie danych osobowych.

Ten przepis ustawowy potwierdza wskazaną na wstępie zasadę, ze rejestracja zbioru danych osobowych jest zwieńczeniem działań Administratora danych osobowych, związanych z właściwym zebraniem, a następnie zabezpieczeniem przetwarzanych danych osobowych.

Studium przypadku:
Przedsiębiorca, który złożył „Wniosek o rejestrację zbioru" wskazując niewypełnienie któregokolwiek z obowiązkowych zabezpieczeń organizacyjnych lub technicznych, np. brak systemu upoważnień do przetwarzania danych osobowych, musi liczyć się z odmową rejestracji zbioru.
Natomiast w sytuacji gdy „Wniosek" będzie potwierdzał nieprawdziwe fakty, np. w rzeczywistości nie będą wydawane „Upoważnienia do przetwarzania danych osobowych", wtedy Administratorowi danych osobowych poza odpowiedzialnością wynikającą z przepisów Ustawy, grozić będzie również odpowiedzialność karna z art. 271 Kodeksu karnego.

Jednym z najważniejszych skutków faktycznych rejestracji zbiorów jest wyznaczenie chwili, w której następuje ustawowa **zgoda na przetwarzanie danych osobowych w zbiorze**:

- „zwykłe" dane osobowe można przetwarzać z chwilą złożenia „Wniosku o rejestrację zbioru" (art. 46 ust. 1);
- „wrażliwe" dane osobowe można przetwarzać dopiero po uzyskaniu decyzji o zarejestrowaniu zbioru (art. 46 ust. 2 w zw. z art. 42 ust. 4)[208].

---

[204] Moduł internetowej rejestracji „zbiorów danych osobowych" znajduje się pod adresem: https://egiodo.giodo.gov.pl/index.dhtml.

[205] Adres: Biuro Generalnego Inspektora Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

[206] Ustawa z dnia 17 lutego 2005 roku *o informatyzacji działalności podmiotów realizujących zadania publiczne*, (Dz.U. nr 64, poz. 565, z późn. zm.) – art. 20a.

[207] A. Drozd: *Ustawa o ochronie* …, s. 275.

[208] W piśmiennictwie występuje szeroka dyskusja, czy rejestracja zbioru danych osobowych jest warunkiem legalizującym proces przetwarzania. Patrz: J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 641, 646, 672; P. Barta, P. Litwiński: *Ustawa o ochronie* …, s. 471-472; A. Drozd: *Ustawa o ochronie* …, s. 284-285.

Studium przypadku:
Przedsiębiorca, który zebrał „wrażliwe" dane osobowe i utworzył z nich zbiór, może podjąć dalsze ich przetwarzanie dopiero po uzyskaniu od Generalnego inspektora decyzji o rejestracji tego zbioru danych osobowych.

5.2.2. LOKALNY REJESTR ZBIORÓW DANYCH OSOBOWYCH

Szczególny rodzaj rejestru zbiorów danych osobowych wprowadziła ostatnia nowelizacja Ustawy[209]. Zgodnie z jej dyspozycją Administrator bezpieczeństwa informacji prowadzi „Rejestr zbiorów danych Administratora danych osobowych", który obejmuje wyłącznie zbiory, w których są przetwarzane „**zwykłe**" **dane osobowe**. W tym zakresie Administrator danych osobowych nie ma obowiązku ich zgłaszania do rejestracji przez Generalnego Inspektora (art. 43 ust. 1a). **Warunkiem koniecznym** dla dopuszczalności takiej sytuacji jest to, żeby Administrator bezpieczeństwa informacji był właściwie powołany przez Administratora danych osobowych (art. 36a ust. 1), i skutecznie zarejestrowany w rejestrze prowadzonym przez Generalnego Inspektora (art. 46b).

Studium przypadku:
Przedsiębiorca do czasu poprawnego wyznaczenia Administratora bezpieczeństwa informacji, musi dokonać obowiązkowej rejestracji zbiorów danych osobowych, nawet w sytuacji rozpoczętej procedury rekrutacji osoby na to stanowisko.

Zasady prowadzenia tego rodzaju rejestru zbiorów danych osobowych określa Rozporządzenie ws. lokalnego rejestru zbiorów. **Zakres informacji**, które powinny zostać umieszczone w „Lokalnym rejestrze zbiorów danych osobowych", pokrywa się z tym, który jest wymagany w zgłoszenia zbioru do rejestracji przez Generalnego Inspektora (§3 ust. 1), z takim samym wyłączeniem opisu o zastosowanych zabezpieczeń organizacyjno-technicznych procesu przetwarzania danych osobowych.

Ponadto Administrator bezpieczeństwa informacji musi odnotowywać historię zmian w rejestrze zawierającą:
- informację o rodzaju zmiany, tj. nowy wpis, aktualizacja, wykreślenie;
- datę dokonania zmiany;
- informację o zakresie zmiany (§6).

Nie istnieje niestety żaden obowiązujący szablon takiego „Rejestru"[210]. Także w przypadku „Lokalnego rejestru zbiorów danych osobowych" ustawodawca nakazał obowiązek jego **jawności** (art. 36a ust. 3).

Administrator bezpieczeństwa informacji ma obowiązek udostępnić „Rejestr", w jednej z poniższych form:
- **na stronie internetowej** Administratora danych osobowych;
- **na ogólnodostępnym komputerze** w siedzibie Administratora danych osobowych;
- **w postaci papierowej** w siedzibie Administratora danych osobowych (§5).

Możliwości prowadzenia „Lokalnego rejestru zbiorów danych osobowych" nie należy utożsamiać lub stosować zastępczo z obowiązkiem umieszczenia w „Polityce bezpieczeństwa danych osobowych" załącznika zawierającego wykaz zbiorów danych osobowych oraz ich szczegóły.

5.2.3. ZBIORY DANYCH OSOBOWYCH ZWOLNIONE Z OBOWIĄZKU REJESTRACJI

Ustawodawca przyjmując za podstawę interes publiczny, lub ograniczone ryzyko naruszenia praw i wolności jednostki, wprowadził **wyjątki od obowiązku** rejestracji zbiorów danych osobowych[211]. Wyłączenia generalnie zostały podzielone z uwagi na:
- cel prowadzenia zbioru danych osobowych;
- zawartość informacyjną zbioru danych osobowych;
- specyfikę działalności Administratora danych osobowych.

Poniżej poruszone zostaną tylko te zwolnienia z obowiązku rejestracji zbiorów danych osobowych, które mogą dotyczyć przedsiębiorców[212]. Wszyscy Administratorzy danych osobowych są zwolnieni z obowiązku rejestracyjnego

[209] Weszła w życie z dniem 1 stycznia 2015 roku.
[210] Można w tym względzie skorzystać z dostępnych w Internecie projektów przygotowanych przez różnego rodzaju firmy doradcze. Należy jednak pamiętać o sprawdzeniu, czy zawierają wszystkie obowiązkowe elementy.
[211] P. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 659.
[212] Generalnie zwolnienie z obowiązku rejestracji obejmuje znacznie szerszy zakres zbiorów danych osobowych. Dotyczy on jednak wyłącznie wyspecjalizowanych zbiorów danych osobowych prowadzonych przez instytucje publiczne, np. Krajowy Rejestr Karny; lub danych gromadzonych przez partie polityczne, związki zawodowe czy kościoły.

w odniesieniu do **zbiorów kadrowo-płacowych** (art. 43 ust. 1 pkt 4). W tym przypadku zwolnienie obejmuje cały zbiór danych osobowych, którego celem prowadzenia jest realizacja jakichkolwiek obowiązków pracodawcy związanych z wykonywaniem dla niego lub na jego rzecz pracy przez osobę fizyczną, **bez względu na rodzaj łączącego strony stosunku prawnego**.

Studium przypadku:
W skład zbioru kadrowo-płacowego wchodzą wszystkie kartoteki i ewidencje, które służą wykonaniu obowiązków nałożonych na Administratora danych osobowych w stosunku do pracowników, przez jakikolwiek akt prawny lub regulację wewnętrznego regulaminu pracy, np. dokumentacja zakładowego funduszu świadczeń socjalnych.

Ze tego zwolnienia nie mogą skorzystać przedsiębiorcy, których przedmiotem działalności jest **pośrednictwo pracy**. Podmioty te bowiem nie przetwarzają danych osobowych w celu zatrudnienia u siebie, ale jako pewnego rodzaju usługę dla innych instytucji i firm[213].

Drugim dosyć powszechnym wyłączeniem jest przetwarzanie danych osobowych wyłączenie **w celu wystawienia dokumentu sprzedaży** lub prowadzenia sprawozdawczości finansowej (43 ust. 1 pkt 8). Należy jednak pamiętać, że zwolnienie to **nie dotyczy** sytuacji, w których dane te będą wykorzystywane także dla innych celów, np. dochodzenie roszczeń reklamacyjnych[214]czy marketingu własnych produktów[215].

Studium przypadku:
Przedsiębiorca przetwarzający dane osobowe swoich klientów, którym wystawia dowody zakupu sprzedawanych urządzeń AGD, nie jest zwolniony z obowiązku rejestracji tak powstałego zbioru, gdyż poza samą ewidencją sprzedaży dane te mogą stać się elementem procedury reklamacyjnej.

Z obowiązku rejestracji są zwolnione zbiory danych osobowych prowadzone w związku ze świadczeniem szczególnego rodzaju usług objętych **tajemnicą zawodową**:
- medycznych: lekarza, pielęgniarki, położnej, ratownika medycznego, technika medycznego, rehabilitanta;
- prawnych: notarialnych, adwokackich, radcy prawnego, rzecznika patentowego;
- księgowych: doradcy podatkowego, biegłego rewidenta (art. 43 ust. 1 pkt 5).

Wyjątek ten **nie dotyczy wszystkich zbiorów** danych prowadzonych przez podmioty medyczne, prawne czy księgowe, a jedynie tych, które są przetwarzane do realizacji czynności objętych wskazanymi czynnościami.

Studium przypadku:
Przedsiębiorca prowadzący sklep zaopatrzenia medycznego zwolniony jest z obowiązku rejestracji zbioru danych osobowych pacjentów, dla których świadczy usługę sprzedaży oraz rozliczania dofinansowania wyrobów medycznych.

Ponadto obowiązek rejestracji nie obejmuje danych osobowych przetwarzanych w zakresie „**drobnych bieżących spraw życia codziennego**" (art. 43 ust. 1 pkt 11). Termin ten pozostaje jednak nieokreślony, nawet na gruncie prawa cywilnego, z którego się wywodzi. Ponadto przyjmuje się, że dotyczy on spraw niewielkiej wagi, których dokładne sprecyzowanie nie jest możliwe. Powszechnie przyjmuje się, że będą to takie zbiory, jak:
- książki wejść i wyjść;
- rejestry przepustek;
- wewnętrzne listy służbowych telefonów[216].

Ostatnim z omówionych wyjątków będzie zwolnienie z obowiązkowej rejestracji zbiorów „zwykłych" danych osobowych przetwarzanych **bez udziału systemu informatycznego** (art. 43 ust. 1 pkt 12).

[213] A. Drozd: *Ustawa o ochronie* …, s. 290.
[214] A. Drozd: *Ustawa o ochronie* …, s. 292.
[215] P. Barta, P. Fajgielski, R. Markiwicz: *Ochrona danych osobowych* …, s. 662.
[216] A. Drozd: *Ustawa o ochronie* …, s. 293.

Studium przypadku:
Przedsiębiorca prowadzący wyłącznie papierową ewidencję zawierającą „zwykłe" dane osobowe, wykonuje czynności sporządzania niektórych z tworzących ją dokumentów przy wykorzystaniu zainstalowanego na stanowisku komputerowym edytora tekstu.
Jeżeli tylko na tym stanowisku komputerowym nie są zapisywane kopie wydrukowanych dokumentów, tzw. maszyna do pisania, to w takim przypadku nie ma obowiązku rejestracji zbioru danych osobowych.

Reasumując należy jednoznacznie zauważyć, że zwolnienie z obowiązku rejestracji zbioru danych osobowych, **nie zwalnia** Administratora danych osobowych z jakichkolwiek innych wymogów ustawowych, np. zabezpieczenia tych zbiorów.

5.3. UPOWAŻNIENIA I ICH EWIDENCJA

Sprawowanie przez Administratora danych osobowych bezpośredniej kontroli nad tym, kto i w jakim zakresie przetwarza pozostające w jego dyspozycji zbiory danych osobowych, stanowi jeden z kluczowych elementów całego systemu bezpieczeństwa. Ustawodawca nie pozostawia w tym względzie żadnej możliwości odstępstw.

Skuteczność tej kontroli jest możliwa wyłącznie poprzez **sformalizowany proces** nadawania upoważnień do przetwarzania danych osobowych. Jego właściwe udokumentowanie potwierdza dochowanie przez Administratora danych osobowych „szczególnej staranności" przy realizacji dyspozycji ustawowej.

5.3.1. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Ustawodawca nie określił ani formy, ani treści „Upoważnienia do przetwarzania danych osobowych". Uczyniła to skutecznie doktryna, piśmiennictwo i praktyka. Upoważnienie powinno mieć **formę dokumentu tradycyjnego** wydawanego indywidualnie dla każdej osoby upoważnianej przez Administratora danych osobowych[217]. Przyjęcie innej formy niż pisemna nie skutkuje nieważnością takiej decyzji[218]. Może oznaczać jednak, że tak nadane upoważnieniem, np. przy przyjęciu formy ustanej, będzie niezgodne z wymogami Ustawy, gdyż mogą wystąpić nieusuwalne trudności w ustaleniu jego niezbędnych elementów, m.in. daty wydania i zakresu[219].

Choć przedmiotowe upoważnienie nie ma waloru **decyzji administracyjnej** – takie uprawnienie nie przysługuje Administratorowi danych osobowych – jest zasadnym, żeby jego treść odpowiadała rygorom wydawanych w tym trybie dokumentów[220]. Powinno ono określać co najmniej informacje pozwalające na identyfikację:

1) **podstawy prawnej decyzji** – właściwy przepis ustawowy,
2) **wystawcy decyzji** – Administratora danych osobowych,
3) **adresata decyzji** – osobę upoważnianą,
4) **zakres przedmiotowy decyzji**:
   a) zbiór danych osobowych lub jego część;
   b) sposób przetwarzania: tradycyjny i/lub w systemie informatycznym;
   c) rodzaj dopuszczalnych czynności na danych osobowych, np. zbieranie, przeglądanie, aktualizowanie, kopiowanie, udostępnianie, usuwanie, itp.,
5) **okres ważności decyzji** – wydarzenie lub termin, który decyduje o ustaniu ważności upoważnienia, np. na czas trwania stosunku pracy lub realizacji umowy.

Nic nie stoi na przeszkodzie, żeby „Upoważnienie" zawierało jeszcze inne informacje niezbędne dla prawidłowego zarządzania dostępem do danych osobowych. Za przygotowanie wniosku o wydanie „Upoważnienia", zakreślającego obszar przedmiotowy niezbędnego dostępu do danych osobowych, powinien odpowiadać **bezpośredni przełożony** osoby, której ma ono zostać nadane.

---

217 A. Krasuski, D. Skolimowska: *Dane osobowe* …, s. 200; A. Drozd: *Ustawa o ochronie* …, s. 266.
218 P. Barta, P. Litwiński: *Ustawa o ochronie* …, s. 419.
219 A. Drozd: *Ustawa o ochronie* …, s. 266.
220 Patrz: Ustawa z dnia 14 czerwca 1960 roku – *Kodek postępowania administracyjnego*, (Dz.U. nr 30, poz. 168) – art. 268a.

Przykładowa treść:
Na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. nr 133, poz. 883, z późn. zm.) upoważniam:
Jana Kowalskiego
do przetwarzania danych osobowych:
w zbiorze: *Kadry i płace*
dokumentacja tradycyjna: *rejestr szkoleń specjalistycznych*
w zakresie: *wprowadzania i aktualizacji danych*
aplikacja informatyczna: *Super Kadry – szkolenia*
w zakresie: *wprowadzania danych, modyfikacji danych, drukowania skierowań*.

Upoważnienia udzielam:
na czas trwania stosunku pracy / ~~umowy nr ……../ do dnia .....~~ *

Upoważnienie musi być **podpisane** przez:
- wydającego decyzję, tj. Administratora danych osobowych lub osobę przez niego właściwie uprawomocnioną do tej czynności;
- adresata decyzji, tj. osobę upoważnianą, która potwierdza w ten sposób przyjęcie określonych uprawnień i obowiązków.

W przypadku podpisywania „Upoważnienia" przez inną osobę niż Administrator danych osobowych, należy pamiętać, że to on jest nadal wydającym, a zatem podpisanie następuje wyłącznie w jego imieniu[221]. Niedopuszczalne wydaje się być jednak, żeby osoba, która ma otrzymać „Upoważnienie do przetwarzania danych osobowych", wyznaczyła inną osobę do jego odebrania w swoim imieniu.

5.3.2. EWIDENCJA UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

Ustawodawca szczególne znacznie przykłada nie tylko do samego udokumentowania decyzji Administratora danych osobowych w postaci „Upoważnień do przetwarzania danych osobowych", ale także do ich **właściwej ewidencji**.

Ewidencja osób upoważnionych do przetwarzania danych osobowych powinna zawierać, co najmniej takie **informacje o tych osobach**, jak:
1) imię i nazwisko;
2) identyfikator użytkownika w systemie informatycznym;
3) datę nadania i ustania upoważnienia;
4) zakres upoważnienia (art. 39 ust. 1).

Dodatkowo nic nie stoi na przeszkodzie by w tym rejestrze mogły być umieszczane inne dane, które są niezbędne do zapewnienia właściwej kontroli nad procesem przetwarzania danych osobowych, np. dział, w którym pracują poszczególne upoważnione osoby[222].

Przykładowy wpis w ewidencji:

l.p.	Osoba upoważniona			Dane upoważnienia		
	Nazwisko	Imię	Identyfikator	Zakres	Data nadania	Data ustania
1.	Kowalska	Anna	akowalska	Rejestr Gości: wprowadzanie danych	12.11.2015	
2.	Nowak	Jan	jnowak	Kadry i płace: administrowanie aplikacją informatyczną „Super Kadry"	15.11.2015	

[221] A. Krasuski, D. Skolimowska: *Dane osobowe* …, s. 201.
[222] A. Drozd: *Ustawa o ochronie* …, s. 271.

Ewidencję wydanych przez Administratora danych osobowych „Upoważnień do przetwarzania danych osobowych" powinien prowadzić **Administrator bezpieczeństwa informacji** lub osoba wyznaczona do nadzoru nad procesem przetwarzania danych osobowych. Ewidencja może być prowadzona w formie papierowej lub **elektronicznej**. Ta druga wydaje się być znacznie bardziej funkcjonalna i nie naruszać żadnych obowiązków[223].

Niedopuszczalne jest zastąpienie „Ewidencji osób upoważnionych" przez zbiór kopii wszystkich wydanych „Upoważnień do przetwarzania danych osobowych", np. w formie chronologicznie prowadzonego segregatora.g

5.3.3. ZOBOWIĄZANIE DO ZACHOWANIA POUFNOŚCI

Zapewnienie przestrzegania przez osoby upoważnione do przetwarzania danych osobowych **obowiązku poufności** to gwarancja ich właściwej ochrony przed działaniami niepożądanymi. Ze względów dowodowych, potwierdzających przyjęcie na siebie przez osobę zobowiązania do zachowania w tajemnicy danych osobowych, do których ma dostęp w związku z wykonywanymi obowiązkami służbowymi, niezbędne jest, żeby takie „oświadczenie woli" zostało bezwzględnie **sporządzone na piśmie**[224].

Dokument „Zobowiązania do zachowania poufności" powinien być **imienny**, tj. sporządzony odrębnie dla każdej osoby, której nadawane jest „Upoważnienie do przetwarzania danych osobowych".

Zawartość merytoryczna „Zobowiązania do zachowania poufności" powinna obejmować takie elementy, jak:

- potwierdzenie znajomości Ustawy, rozporządzeń wykonawczych oraz procedur wewnętrznych organizacji;
- wskazanie zakresu tajemnicy, tj. dane osobowe i zasady ich zabezpieczenia;
- przyjęcie odpowiedzialności za podejmowane działania[225].

Należy także pamiętać o **warunkach ważności** takiego oświadczenia woli:

- dobrowolność jego złożenia;
- pełna zdolność do właściwego pojmowania przedsiębranego zobowiązania.

Przykładowa treść:
Ja, niżej podpisana(y) oświadczam, że zostałam(em) zapoznana(y) z zasadami przetwarzania i ochrony danych osobowych określonymi w przepisach prawa oraz dokumencie „Polityka Bezpieczeństwa Danych Osobowych".
Zobowiązuje się do zachowania w tajemnicy wszelkich danych osobowych, do których mam lub będę miał(a) dostęp w związku z wykonywaniem obowiązków pracowniczych oraz do przestrzegania zasad i procedur bezpieczeństwa określonych w w/w dokumencie, którego zapisy także podlegają ochronie.
Informacje te zobowiązuję się zachować w tajemnicy przez cały okres zatrudnienia, a także po jego ustaniu.
Oświadczam, że jestem świadoma(y) odpowiedzialności dyscyplinarnej, finansowej i karnej, wynikającej z niewłaściwego postępowania przy przetwarzaniu danych osobowych.

[223] Odmiennie: A. Krasuski, D. Skolimowska: *Dane osobowe* …, s. 203; A. Drozd: *Ustawa o ochronie* …, s. 271; P. Barta, P. Litwiński: *Ustawa o ochronie* …, s. 425.
[224] P. Barta, P. Fajgielski, R. Markiwicz: *Ochrona danych osobowych* …, s. 636.
[225] A. Krasuski, D. Skolimowska: *Dane osobowe* …, s. 203.

6. DANE OSOBOWE W WYBRANYCH OBSZARACH DZIAŁALNOŚCI GOSPODARCZEJ

dr Łukasz Kister

Wolny rynek powoduje, że przedsiębiorcy podejmują swoją działalność w przeróżnych dziedzinach – od drobnego handlu, po tworzenie nowoczesnych technologii informatycznych. Niemniej jednak bez względu na zakres realizowanych przedsięwzięć biznesowych wszyscy posiadają wspólne obszary aktywności.

W tym rozdziale przedstawione zostaną trzy z nich, bez których trudno wyobrazić sobie dzisiaj jakiekolwiek przedsiębiorstwo – od małego, po wielkie korporacje. Nie ma on jednak ambicji wyjaśnić wszelkich możliwych przypadków, czy odpowiedzieć na wszystkie problemy związane z ich specyfiką, ale wskazać na generalne zasady przetwarzania danych osobowych, których mogą dotyczyć.

6.1. ZARZĄDZANIE ZASOBAMI LUDZKIMI

Pracownicy to ciągle najistotniejszy zasób każdego przedsiębiorstwa, decydujący o jego rozwoju i pozycji rynkowej. Stąd umiejętne zarządzanie zasobami ludzkimi to warunek sukcesu. Jednym z kluczowych obowiązków przedsiębiorcy w zakresie polityki kadrowej jest właściwe i zgodne z prawem wypełnianie obowiązków pracodawcy. Ich realizacja nieodłącznie wiąże się z procesem przetwarzania danych osobowych. Właściwe postępowanie z informacjami o swoich pracownikach nie tylko gwarantuje wypełnianie obowiązków ustawowych, ale pozwala na stworzenie sprawnego systemu zarządzania nimi i wykorzystywania ich do podnoszenia funkcjonalności wszystkich obszarów biznesowych w przedsiębiorstwie.

6.1.1. ZAKRES INFORMACYJNY ZBIORU KADROWO-PŁACOWEGO

Jednym z podstawowych obszarów, jakie łączą proces zarządzania zasobami ludzkimi z przetwarzaniem danych osobowych, jest obowiązek realizacji przez przedsiębiorcę różnych zadań wynikających z powszechnie obowiązującego prawa pracy oraz łączącej strony umowy. Niezbędnym jest więc ustalenie, jaki zakres informacji o pracowniku może być przetwarzany przez pracodawcę, by nie wykraczał poza **cel** jakiemu mają służyć, a tym samym nie naruszał prawa do prywatności.

Zgodnie z decyzją ustawodawcy przetwarzanie danych osobowych, nawet tych o charakterze „wrażliwym", jest dopuszczalne gdy:

- **jest to niezbędne do zatrudnienia pracowników i innych osób**;
- **zakres danych osobowych jest określony w ustawie** (art. 27 ust. 2 pkt 6).

Generalnym aktem prawnym regulującym obszar zatrudnienia, określającym wzajemne prawa pracodawcy i pracownika jest Ustawa z dnia 26 czerwca 1974 roku – ***Kodeks pracy***[226]. Uzupełniają go akty wykonawcze wydane zgodnie z jego dyspozycją oraz szereg innych aktów ustawowych, które odnoszą się do szeroko rozumianego stosunku pracy. Choć przepisy Kodeksu pracy odnoszą się wyłącznie do praw i obowiązków związanych z zawarciem **umowy o pracę**, powołaniem, wyborem, mianowaniem lub spółdzielczą umową o pracę, to jednak w odniesieniu do przedmiotu niniejszych rozważań należy stosować go także w przypadku **innych stosunków pracy**, np. wynikających z umów cywilno-prawnych[227].

Zgodnie z dyspozycją Kodeksu pracy, **podstawowy zakres treściowy zbioru** danych osobowych pracowników, jest tworzony dwuetapowo. Pracodawca ma prawo żądać od **kandydata do pracy** podania informacji obejmujących:

- imię (imiona) i nazwisko;
- imiona rodziców;
- datę urodzenia;
- miejsce zamieszkania (adres do korespondencji);
- wykształcenie;
- przebieg dotychczasowego zatrudnienia (art. 22^1 §1).

Ponadto już **od pracownika**, także:

- numer PESEL;

[226] (Dz.U. nr 24, poz. 141, z późn. zm.).

[227] Patrz: T. Kuczyński: *Ochrona danych osobowych w stosunku zatrudnienia*, „Przegląd sądowy", nr 11-12, 1998, s. 122-123; A. Drozd: *Ustawa o ochronie* …, s. 179; P. Barta, P. Litwiński: *Ustawa o ochronie* …, s. 315-316.

- informacje niezbędne do realizacji szczególnych uprawnień pracownika wynikających z prawa pracy, np. imiona, nazwiska i daty urodzenia dzieci (art. 22^1 §2).

Rozszerzenie zbioru danych pracowniczych może wynikać również z treści innych szczegółowych przepisów Kodeksu pracy, które wymuszają na pracodawcy przetwarzania także takich informacji, jak m.in.:
- dane o stanie zdrowia (art. 229);
- informacje o nagrodach i wyróżnieniach (art. 105);
- informacje o karach porządkowych (art. 110);
- nazwa banku i numer konta bankowego (art. 86).

Dalsze rozbudowanie zawartości informacyjnej zbioru danych pracowniczych może wynikać z **praw bądź obowiązków** wyznaczonych przez inne przepisy rangi ustawowej, które odnoszą się do spraw związanych z zatrudnieniem (art. 24^1 §4). Wśród nich szczególne zainteresowanie budzą możliwości przetwarzania:
- informacji o szczególnych uprawnieniach;
- danych o karalności.

W pierwszym przypadku nie występują praktycznie żadne wątpliwości interpretacyjne, gdyż obowiązek pozyskania i przetwarzania takich informacji wynika nie tyle z konkretnych przepisów prawa, co przede wszystkim ich posiadanie gwarantuje **możliwość wykonywania określonej pracy**, np.:
- kierowcy[228];
- zawodowego kierowcy[229];
- kwalifikowanego pracownika ochrony osób i mienia[230].

Brak jest w takiej sytuacji jakichkolwiek zastrzeżeń co do dopuszczalności przetwarzania tego rodzaju informacji osobowych przez pracodawcę[231].

Studium przypadku:
Przedsiębiorca prowadzący transport międzynarodowy ma prawo do okresowej weryfikacji i przetwarzania danych o uprawnieniach swoich pracowników niezbędnych do kierowania pojazdami i wykonywania transportu międzynarodowego osób i towarów.

Całkowicie odmienną sytuacją, a jednocześnie wywołującą liczne kontrowersje jest możliwość przetwarzania **danych o karalności**.

Po pierwsze, możliwość uzyskania zaświadczenia z Krajowego Rejestru Karnego przysługuje wyłącznie pracodawcom, w zakresie niezbędnym dla zatrudnienia pracownika, co do którego **z przepisów ustawy wynika wymóg niekaralności**, korzystania z pełni praw publicznych, a także ustalenia uprawnienia do zajmowania określonego stanowiska, wykonywania określonego zawodu lub prowadzenia określonej działalności gospodarczej[232], np.:
- agent celny[233];
- detektyw[234];
- pracownik kantoru wymiany walut[235].

Po drugie, szczególnie przedsiębiorcy zatrudniający na stanowiska związane z odpowiedzialnością materialną (np. kasjer czy magazynier) chcą mieć możliwość ustalenia czy kandydat lub pracownik nie był karany. Nie mając jednak podstaw do skorzystania z ustawowego uzasadnienia dostępu do takich informacji, żądają od kandydatów lub pracowników dostarczenia osobiście uzyskanego zaświadczenia o niekaralności, a jednocześnie wyrażenia pisemnej zgody na ich przetwarzanie jako warunku legalizacyjnego (art. 27 ust. 2 pkt 1). Tego rodzaju postępowanie jest **bezprawne**, a wyrażona przez osobę zgoda nie ma mocy sprawczej legalizującej przetwarzanie, gdyż została wyrażona w sposób wyłączający jej dobrowolny charakter (brak równowagi w stosunkach pracodawca – pracownik[236]). **Niedopuszczalne** jest również skorzystanie przez

[228] Patrz: Ustawa z dnia 5 stycznia 2011 roku *o kierujących pojazdami*, (Dz.U. nr 30, poz. 151, z późn. zm.).
[229] Patrz: Ustawa z dnia 6 września 2001 roku *o transporcie drogowym*, (Dz.U. nr 125, poz. 1371, z późn. zm.).
[230] Patrz: Ustawa z dnia 22 sierpnia 1997 roku *o ochronie osób i mienia*, (Dz.U. nr 114, poz. 740, z późn. zm.).
[231] A. Wołyniec: Granice uprawnienia pracodawcy do zbierania danych osobowych,„Radca Prawny", nr 3, 2015, s. 139.
[232] Ustawa z dnia 24 maja 2000 roku *o Krajowym Rejestrze Karnym*, (Dz.U. 50, poz. 580, z późn. zm.) – art. 6 ust. 1 pkt 10.
[233] Patrz: Ustawa z dnia 19 marca 2004 roku – *Prawo celne*, (Dz.U. nr 68, poz. 622, z późn. zm.).
[234] Patrz: Ustawa z dnia 6 lipca 2001 roku *o usługach detektywistycznych*, (Dz.U. nr 12, poz. 110, z późn. zm.).
[235] Patrz: Ustawa z dnia 27 lipca 2002 roku – *Prawo dewizowe*, (Dz.U. nr 141, poz. 1178, z późn. zm.).
[236] Patrz: A. Drozd: *Ustawa o ochronie* …, s. 181; J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 563.

pracodawcę z przesłanki „prawnie usprawiedliwionego celu" (art. 23 ust. 1 pkt 5), gdyż dotyczy ona wyłącznie „zwykłych" danych osobowych, a charakter informacji o karalności jest bezwzględnie „wrażliwy"[237]. **Dyskusyjne** jest także uprawnienie pracodawcy do przetwarzania zaświadczenia o niekaralności dostarczonego samodzielnie i dobrowolnie, bez jakiegokolwiek żądania. Szczególnie gdyby miało być elementem decydującym o wyborze w procesie rekrutacji[238].

Studium przypadku:
Przedsiębiorca nakazujący kandydatowi do pracy lub pracownikowi wyłącznie okazanie sobie „zaświadczenia o niekaralności", bez jego kopiowania i umieszczania w aktach osobowych, także popełnia czyn bezprawnego przetwarzania danych osobowych.

6.1.2. OUTSOURCING OBSŁUGI KADROWO-PŁACOWEJ

Administrator danych osobowych decydując o celach i środkach przetwarzania danych osobowych, może wykonywać czynności na tych danych samodzielnie bądź zlecić je innemu podmiotowi[239]. Bardzo częstą praktyką przedsiębiorców staje się powierzenie całości lub części czynności związanych z prowadzeniem polityki kadrowo-płacowej wyspecjalizowanym podmiotom zewnętrznym (ang. outsourcing). Działania tego rodzaju, choć jak najbardziej **dopuszczalne prawnie** i gwarantujące profesjonalną obsługę, najczęściej realizowane są w sposób naruszający obowiązki ustawowe. Zgodnie z dyspozycją Ustawy, przedsiębiorca może **powierzyć innemu podmiotowi przetwarzanie danych osobowych** swoich pracowników, w celu wykonywania na jego rzecz lub w jego imieniu obowiązkowych czynności określonych w szeroko rozumianym prawie pracy. Zlecenie tego rodzaju usługi musi być wynikiem **umowy zawartej na piśmie** pomiędzy Administratorem danych osobowych, a Usługobiorcą – Przetwarzającym dane osobowe (art. 31 ust. 1)[240].

Umowa powierzenia danych osobowych do przetwarzania, to szczególny rodzaj **umowy o świadczeniu usług**[241], będących kombinacją czynności prawnych i faktycznych, dlatego też winna ona zawierać takie elementy niezbędne dla jej prawidłowej realizacji, jak:

1) strony umowy,
2) przedmiot umowy,
3) zabezpieczenia przedmiotu umowy,
4) podwykonawcy,
5) rozwiązanie umowy,
6) zasady odpowiedzialności stron umowy.

Poza dokładnym oznaczeniem stron umowy powierzenia, pozwalającym na ich jednoznaczną identyfikację, w pierwszej części umowy można zawrzeć także **elementy decydujące o legalności** takiego zlecenia, tj.:

- podstawę prawną dopuszczającą powierzenie danych do przetwarzania – art. 31 ust. 1;
- identyfikację Administratora danych osobowych w stosunku do informacji stanowiących przedmiot umowy;
- oświadczenie o posiadaniu przez Przetwarzającego wszystkich niezbędnych uprawnień do wykonywania działalności objętej umową, np. związanych z prowadzeniem ksiąg rachunkowych[242].

Przykładowy zapis umowy:
§1.
1. Administratorem danych osobowych w stosunku do wszelkich danych osobowych przetwarzanych w wyniku przedmiotowej umowy jest Zleceniodawca.
2. Zleceniobiorca oświadcza, że posiada kwalifikacje zawodowe i uprawnienia niezbędne do wykonania przedmiotu umowy.

Przedmiot umowy powinien zawierać przede wszystkim ustawowy wymóg określenia **zakresu i celu powierzenia** danych osobowych (art. 31 ust. 2), na który powinny się składać:

---

[237] Odmienne stanowisko w obu tych sprawach prezentuje: K. Walczak: Ochrona danych osobowych kandydata do pracy w trakcie rekrutacji, (w:) T. Wyka, A. Nerka (red.): Ochrona danych osobowych podmiotów objętych prawem pracy i prawem ubezpieczeń społecznych. Stan obecny i perspektywy zmian, Warszawa: Wolters Kluwer Polska, 2012, s. 87i nast..

[238] A. Wołyniec: Granice uprawnienia pracodawcy …, s. 141-142.

[239] J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 571.

[240] W literaturze można znaleźć również opinie, że ustawowy obowiązek formy pisemnej nie jest bezwzględny. Patrz: A. Drozd: *Ustawa o ochronie* …, s. 207-208.

[241] Patrz: Ustawa z dnia 23 kwietnia 1964 roku – *Kodeks cywilny*, (Dz.U. nr 16, poz. 93, z późn. zm.).

[242] Ustawa z dnia 29 września 1994 roku *o rachunkowości*, (Dz.U. nr 121, poz. 591, z późn. zm.).

1) rodzaj powierzanych danych osobowych;
2) cel przetwarzania danych osobowych;
3) zakres dopuszczalnego przetwarzania danych osobowych;
4) forma przetwarzania danych osobowych;
5) czas trwania umowy.

Przykładowy zapis umowy:
§2.
1. Zleceniodawca powierza Zleceniobiorcy dostęp do danych osobowych w zbiorze: „Kadry i Płace".
2. Przetwarzający może przetwarzać powierzone mu dane osobowe wyłącznie w celu realizacji dla Zleceniodawcy i w Jego imieniu obowiązkowych zadań wynikających z prawa pracy.
3. Szczegółowy opis czynności określonych w pkt 2 i zakres danych osobowych niezbędnych do ich realizacji stanowi Załącznik nr 1 do niniejszej Umowy.
4. Zakres przetwarzanych danych osobowych i sposób ich przetwarzania nie może wykraczać poza niezbędny do realizacji czynności określonych w Załączniku nr 1 do niniejszej Umowy.
5. Zleceniobiorca może przetwarzać powierzone dane osobowe zarówno w formie tradycyjnej, jak również w systemie informatycznym.
6. Umowa obowiązuje do czasu jej pisemnego wypowiedzenia przez Zleceniodawcę.

W przypadku powierzenia danych osobowych w celu realizacji obowiązków kadrowo-płacowych ciążących na przedsiębiorcy, nie ma bezwzględnego obowiązku enumeratywnego wymieniania wszystkich danych oraz zakresu dopuszczalnych czynności, gdyż zarówno zawartość tego zbioru, jak również **procesy kadrowe są jednoznacznie określone** przez prawo powszechnie obowiązujące[243]. Najczęściej pomijanym elementem umów powierzenia są zasady zapewnienia **właściwego zabezpieczenia** powierzonym danym osobowym, do których wdrożenia jest zobowiązany Przetwarzający jeszcze przed rozpoczęciem realizacji zlecenia (art. 31 ust. 3).

Zacząć należy od określenia zasad realizacji obowiązku udzielania **upoważnień do przetwarzania** danych osobowych dla poszczególnych pracowników Przetwarzającego, którzy będą mieć dostęp do powierzonych danych osobowych[244]. Wymóg ten może zostać zrealizowany dwojako:
- „Upoważnienia" dla pracowników Przetwarzającego są wydawane osobiście przez Administratora danych osobowych;
- „Upoważnienia dla pracowników wydaje sam Przetwarzający, na podstawie właściwego pełnomocnictwa uzyskanego od Administratora danych osobowych.

Przykładowy zapis umowy:
§3.
1. Zleceniodawca udziela Zleceniobiorcy pełnomocnictwa do wydawania w swoim imieniu Upoważnień do przetwarzania powierzonych danych osobowych.
2. Zleceniobiorca poinformuje pisemnie Zleceniodawcę o wydanych Upoważnieniach. Informacja powinna zawierać: imiona i nazwiska pracowników, stanowisko pracy, identyfikator w systemie informatycznym, zakres dostępu do danych osobowych.
3. Pracownicy upoważnieni do przetwarzania danych osobowych, przed udzieleniem im fizycznego dostępu do danych osobowych, są zobowiązani do złożenia oświadczenia – zobowiązania do zachowania poufności, według wzoru przygotowanego przez Zleceniodawcę.
4. Zabrania się udzielenia fizycznego dostępu do danych osobowych przed formalnym uzyskaniem przez pracowników Upoważnień określonych w pkt 1 i złożenia oświadczeń określonych w pkt 3.

Przyjmuje się jednak, że nawet w przypadku udzielenia Przetwarzającemu pełnomocnictwa do nadawania „Upoważnień", Administrator danych osobowych jest zobowiązany przynajmniej do ich **ewidencjonowania**[245]. Następnie Administrator danych osobowych, który wraz z umową powierzenia nie wyzbywa się odpowiedzialności za bezpieczeństwo danych osobowych i ich zgodne z prawem przetwarzanie (art. 31 ust. 4), musi zapewnić sobie możliwość ustalenie czy Przetwarzający wdrożył niezbędne **zabezpieczenia organizacyjno-techniczne** oraz obowiązkową dokumentację bez-

[243] Patrz: A. Krasuski, D. Skolimowska: *Dane osobowe* …, s. 139 i nast..
[244] J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 573.
[245] A. Drozd: *Zabezpieczenie danych* …, s. 156-157.

pieczeństwa[246]. Wiedzę w tym zakresie powinien posiąść jeszcze przed przekazaniem danych osobowych do przetwarzania. Może ją sobie zapewnić poprzez:

- odpowiednie oświadczenie złożone w umowie przez Przetwarzającego;
- przeprowadzenie audytu u Przetwarzającego.

Przykładowy zapis umowy:

§4.

1. Warunkiem powierzenia danych osobowych do przetwarzania Zleceniobiorcy jest pozytywny wynik audytu przeprowadzonego przez Zleceniodawcę.
2. Celem audytu wskazanego w pkt 1 jest ustalenie, czy Zleceniobiorca wdrożył określone w Ustawie obowiązkowe zabezpieczenia organizacyjno-techniczne procesu przetwarzania danych osobowych.
3. Audyt przeprowadzi Administrator bezpieczeństwa informacji Zleceniodawcy wraz z osobą wyznaczoną przez Zleceniobiorcę.
4. Negatywny wynik audytu, a w szczególności stwierdzenie niespełniania przez Zleceniobiorcę wymagań ustawowych, pozwala na natychmiastowe odstąpienie od niniejszej umowy.

Jednocześnie przyjmuje się, że Administrator danych osobowych powinien zabezpieczyć sobie w umowie możliwość **regularnych kontroli** procesu przetwarzania powierzonych danych osobowych[247]. Ważnym elementem możliwości nadzoru Administratora danych osobowych nad danymi osobowymi powierzonymi innemu podmiotowi jest kwestia ewentualnego **dalszego powierzenia** podwykonawcom. Regulację w tym względzie uzależniającą możliwość podzlecenia przez Przetwarzającego należy umieścić w umowie[248].

Przykładowy zapis umowy:

§5.

1. Zleceniobiorca nie może zlecić wykonania jakiejkolwiek części niniejszej Umowy innemu podmiotowi bez uzyskania pisemnej zgody Zleceniodawcy.
2. W przypadku udzielenia zgody na dalsze podwykonawstwo, Zleceniobiorca przejmuje całkowitą odpowiedzialność za te działania.

Decydując się na powierzenie danych osobowych do przetwarzania należy określić również kwestie związane z działaniami mającymi nastąpić w chwili **rozwiązania umowy**, tj.:

1) zwrot danych osobowych;
2) usunięcie danych osobowych;
3) anonimizacja danych osobowych[249].

Przykładowy zapis umowy:

§6.

1. Z chwilą rozwiązania niniejszej umowy, Zleceniobiorca zobowiązany jest do:
   a) uniemożliwienia dostępu pracowników do powierzonych danych osobowych;
   b) zwrotu Zleceniodawcy wszelkich dokumentów tradycyjnych i komputerowych nośników zawierających powierzone dane osobowe;
   c) usunięcia powierzonych danych osobowych z systemu informatycznego;
2. Wykonanie czynności określonych w pkt 1a) musi nastąpić niezwłocznie.
3. Wykonanie czynności określonych w pkt 1b) i c) musi nastąpić najpóźniej w terminie 14 dni od rozwiązania umowy.
4. Przetwarzający sporządzi pisemne oświadczenie o zrealizowaniu czynności określonych w pkt 1.

Ostatnim z obowiązkowych elementów jaki powinien być umieszczony w umowie powierzenia, to kwestia **odpowiedzialności** Przetwarzającego za niezgodne z prawem oraz zapisami umownymi przetwarzanie danych osobowych[250].

---

246 P. Barta, P. Litwiński: *Ustawa o ochronie* …, s. 332-333.
247 A. Krasuski, D. Skolimowska: *Dane osobowe* …, s. 149-150.
248 P. Barta, P. Litwiński: *Ustawa o ochronie* …, s. 326-327.
249 A. Krasuski, D. Skolimowska: *Dane osobowe* …, s. 142-143.
250 Szerzej: J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 576-580.

Przykładowy zapis umowy:
§6.
1. Zleceniobiorca ponosi pełną odpowiedzialność za nieprzestrzeganie zasad określonych w Ustawie, w szczególności za działania lub zaniechania sprzeczne z zapisami niniejszej umowy.
2. Zleceniobiorca ponosi odpowiedzialność za wszelkie działania lub zaniechania swoich pracowników, które doprowadziły lub mogły doprowadzić do naruszenia zasad bezpieczeństwa danych osobowych.

Przedsiębiorca podejmując decyzję o powierzeniu danych osobowych swoich pracowników do przetwarzania innemu podmiotowi w celu realizacji swoich zadań kadrowo-płacowych, **nie musi**:
- uzyskiwać jakiejkolwiek ich zgody;
- informować ich o tym fakcie[251].

6.2. MARKETING WŁASNYCH PRODUKTÓW I USŁUG

Marketing to sztuka wzbudzania zainteresowania odbiorców oferowanymi produktami lub usługami.

Najskuteczniejszym sposobem reklamy jest marketing bezpośredni, polegający na kierowaniu komunikatów do starannie wybranych, pojedynczych klientów. Pozwala on na niemal indywidualny kontakt z odbiorcą, a w jego następstwie uzyskanie najczęściej natychmiastowej reakcji konsumenta.

Do powodzenia marketingu bezpośredniego konieczne są bazy zawierające informacje o potencjalnych klientach, obejmujące różnego rodzaju dane osobowe, nie zawsze wyłącznie teleadresowe. W związku z tym od zawsze budzi on wiele kontrowersji w przedmiocie zakresu zbieranych na jego potrzeby danych osobowych, a także dopuszczalnych zasadach ich przetwarzania.

6.2.1. ZAWARTOŚĆ INFORMACYJNA ZBIORU MARKETNGOWEGO

Szczególnym rodzajem zrozumienia przez ustawodawcę zasad panujących na współczesnym rynku jest uznanie , że przesłanką dopuszczającą przetwarzanie danych osobowych jest argument **prawnie usprawiedliwionego celu** realizowanego przez Administratora danych osobowych (art. 23 ust. 1 pkt 5)[252]. Jednocześnie jednym z dwóch jednoznacznie wymienionych przez przepis, tego rodzaju celem działalności jest w szczególności – **marketing własnych produktów lub usług** (art. 23 ust. 4 pkt 1). W związku z powyższym Administrator danych osobowych nie musi pozyskiwać żadnej zgody od osób, których dane osobowe zamierza przetwarzać w takim celu. Skorzystanie przez przedsiębiorcę z takiego szczególnego uprawnienia do przetwarzania danych osobowych dla celów marketingowych nie jest jednak pozbawione żadnych ograniczeń czy szczegółowych wymagań faktycznych.

Użycie przez ustawodawcę terminu„**własnych produktów i usług**" wyłącza możliwość zastosowania tej przesłanki legalizującej przetwarzanie danych osobowych w odniesieniu do:
- marketingu produktów i usług innych przedsiębiorców, bez względu na wzajemne powiązania kapitałowe;
- działalności agencji marketingowych i reklamowych[253].

Studium przypadku:
Przedsiębiorca nie może prowadzić marketingu cudzych produktów lub usług do osób z własnej bazy, bez uprzedniego pozyskania ich zgody, bez względu na umowę łączącą go z innym podmiotem.

Ponadto liberalny charakter tego uprawnienia nie zwalania z obowiązku dostosowania **zawartości informacyjnej zbioru** danych osobowych w odniesieniu do kryterium adekwatności do celu (art. 26 ust. 1 pkt 3). Z całą pewnością w bazie marketingowej mogą znaleźć się tylko i wyłącznie takie dane osobowe, które są **konieczne do osiągnięcia celu**, tj. powiadomienia o własnych produktach lub usługach[254].

---

[251] A. Drozd: *Ustawa o ochronie* …, s. 207.

[252] Szerzej na temat prawnego usprawiedliwienia celu przetwarzania, w: P. Barta: *Klauzula prawnie usprawiedliwionego celu w ustawie o ochronie danych osobowych*, (w:) Konarski X., Sibiga G. (red.): *Ochrona danych osobowych* …, s. 61-85.

[253] P. Barta, P. Litwiński: *Ustawa o ochronie* …, s. 260-261; P. Barta: *Klauzula prawnie usprawiedliwionego* …, s. 81-82. Odmiennie: A. Drozd: *Ustawa o ochronie* …, s. 135-136.

[254] P. Barta, P. Litwiński: *Ustawa o ochronie* …, s. 251.

Studium przypadku:
Przedsiębiorca narusz obowiązek związania celem przetwarzając w bazie marketingowej dane osobowe zawierające imiona i nazwiska rodziców, miejsce urodzenia czy numer identyfikacji podatkowej NIP.

Określenie zawartości informacyjnej zbioru danych osobowych przetwarzanego do celu marketingu własnych produktów lub usług powinno następować **najpóźniej w momencie zbierania danych** i tworzenia tego zbioru[255]. Determinantem dla procesu określenia rodzaju danych osobowych, które mogą się znaleźć w bazie marketingowej, jest **kanał dystrybucji** reklam, m.in.:

- tradycyjne imienne ulotki reklamowe wysyłane pocztą;
- telemarketing;
- wiadomości tekstowe SMS;
- wiadomości poczty elektronicznej e-mail.

Niemożliwe jest więc zbudowanie zamkniętej listy informacji o osobie, które mogą być pozyskiwane i przetwarzane przez Administratora danych osobowych do celów prowadzenia działań reklamowych. Za każdym razem podlegać to będzie odrębnej analizie i ocenie celowościowej.

Studium przypadku:
Przedsiębiorca prowadzący stację kontroli pojazdów chcący prowadzić reklamę swoich usług za pomocą rozsyłanych wiadomości SMS do właścicieli samochodów, nie potrzebuje do tego przetwarzać nawet danych osobowych w postaci: imienia i nazwiska.

Zabronione jest zbieranie danych osobowych wykraczających poza wyznaczony cel działań marketingowych, czyli „na zapas".

Ważnym obowiązkiem, jaki ciąży na Administratorze danych osobowych, jest **wymóg poinformowania osoby** o szczegółach dotyczących przetwarzania jej danych osobowych. Zakres tego wymogu wyznacza sposób pozyskania danych osobowych. W przypadku gdy przedsiębiorca pozyskuje dane osobowe **bezpośrednio od osoby**, której one dotyczą, ma on obowiązek poinformować ją o:

1) swoich danych identyfikujących – nazwa i adres,
2) celu zbierania danych,
3) przewidywanych odbiorcach danych,
4) prawie dostępu do swoich danych i ich poprawiania,
5) dobrowolności podania danych osobowych (art. 24 ust. 1).

Sytuacja zbierania danych osobowych bezpośrednio od osoby, której one dotyczą, **nie oznacza**, że dane muszą być uzyskiwane:

- w jej obecności, tj. może to odbywać się za pośrednictwem telefonu, poczty elektronicznej, faksu czy tradycyjnego listu;
- przez samego Administratora danych osobowych lub jego pracowników, tj. zbieranie danych osobowych może być wykonywane poprzez zleceniobiorców[256].

Przykładowa treść powiadomienia:

1. Administratorem Pani/Pana danych osobowych będzie SuperButy sp. z o.o. z/s w Warszawie przy ul. Zakamarek 22.
2. Dane zbierane są w celu prowadzenia marketingu bezpośredniego własnych produktów i usług przy wykorzystaniu poczty elektronicznej e-mail.
3. Nie przewidujemy udostępniania zebranych danych osobowych innym podmiotom.
4. Ma Pani/Pan prawo dostępu do przetwarzanych danych osobowych oraz ich aktualizację.

W przypadku gdy przedsiębiorca pozyskuje bazę danych marketingowych **od innego podmiotu**, ma obowiązek powiadomienia wszystkich osób, których dane osobowe będzie przetwarzał, również o:

1) źródle danych osobowych, tj. informacji o podmiocie, od którego je uzyskano;
2) uprawnieniach do żądania wstrzymania przetwarzania danych osobowych (art. 25. ust. 1).

[255] J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 537.
[256] A. Drozd: *Ustawa o ochronie* …, s. 141.

W obu przypadkach **nie ma obowiązku,** aby informacja o przetwarzaniu:

- była przekazywana w formie pisemnej, ale musi być pełna i wyodrębniona z innych przekazywanych osobie komunikatów, a ponadto wyrażona w sposób zrozumiały dla osoby, której dane dotyczą;
- zawierała informacje o rodzaju pozyskanych od innego podmiotu danych osobowych[257].

Obowiązek informacyjny następuje **niezwłocznie** po uzyskaniu danych osobowych (art. 25 ust. 1). Brak jest jakichkolwiek wyjątków pozwalających na ominięcie tego obowiązku przez przedsiębiorcę w odniesieniu do celu przetwarzania jakim jest marketing własnych produktów lub usług.

Ustawodawca, świadomy możliwości nadinterpretacji tej niedookreślonej prawnie i praktycznie przesłanki, wskazał na istotne zastrzeżenie, aby przetwarzanie danych osobowych dla celu marketingowego – choć prawnie usprawiedliwionego – to jednak **nie naruszało praw i wolności osób**, których dane dotyczą (art. 23 ust. 1 pkt 5). Nie oznacza to, że decyzja w tym względzie jest pozostawiona do indywidualnej decyzji osoby, tj. jej subiektywnego osądu, że przetwarzanie dla celów marketingowych narusza jej prawa i wolności. Ale winno to być przedmiotem tzw. „ważenia dóbr", dokonywanego przez Administratora danych osobowych, który ma obowiązek ocenić ewentualnie **kolidujące ze sobą interesy**, w wyniku czego byłoby możliwe naruszenie dóbr osoby, której dane dotyczą[258]. Jednocześnie zupełnie pozbawionym podstaw jest twierdzenie, że wskazanie marketingu własnych produktów lub usług jako prawnie usprawiedliwionego celu oznacza, że Ustawa wyklucza w tym przypadku sytuację możliwości naruszenia praw i wolności osób, których dane dotyczą. Ocena taka musi wynikać z analizy zarówno rodzaju przetwarzanych danych osobowych, jak również **sposobu ich wykorzystania** do działań marketingowych[259].

Studium przypadku:
Przedsiębiorca prowadzący sprzedaż produktów erotycznych, powinien rozważyć możliwość ich reklamowania wśród nastolatków.

Bezpośrednim wypełnieniem konstytucyjnego prawa do autonomii informacyjnej jest określone przez ustawodawcę prawo osoby do wniesienia:

1) **sprzeciwu wobec przetwarzania** jej danych osobowych dla celów marketingowych (art. 32 ust. 1 pkt 8);
2) żądania zaprzestania przetwarzania danych osobowych dla celów marketingowych, umotywowanego względami osobistymi (art. 32 ust. 1 pkt 7).

Pierwsze uprawnienie może być realizowane już w czasie **zbierania danych** osobowych:

- wykluczając możliwość ich włączenia do zbioru;
- skutkując obowiązkiem zniszczenia zapisanych już danych osobowych.

Studium przypadku:
Przedsiębiorca zawierając umowę na wykonanie usługi remontowej, nie może skorzystać z zawartych w niej danych Klienta do celów marketingu własnych produktów lub usług, jeżeli ten złoży sprzeciw w tym zakresie.

Ponadto na każdym etapie przetwarzania, wniesienie przez osobę, której dane dotyczą, sprzeciwu skutkuje natychmiastowym obowiązkiem:

- **zaprzestania przetwarzania** jej danych osobowych dla celów marketingowych;
- **usunięcia jej danych** osobowych ze zbioru marketingowego;

W celu uniknięcia ponownego wykorzystania danych tej osoby w zakresie objętym sprzeciwem, Administrator danych osobowych może pozostawić w zbiorze marketingowym: imię, nazwisko oraz numer PESEL lub adres (art. 32 ust. 3). Obowiązek ten nie dotyczy danych osobowych tej samej osoby, które są przetwarzane dla innych zgodnych z prawem celów, np. świadczenie usługi[260].

[257] J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 520-521.
[258] A. Drozd: *Ustawa o ochronie* …, s. 135-136.
[259] P. Barta: Klauzula prawnie usprawiedliwionego …, s. 82.
[260] J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 605-606.

Studium przypadku:
Przedsiębiorca świadczący sprzedaż sprzętu AGD może przetwarzać dane osobowe Klienta dla celów ewentualnego postępowania gwarancyjnego lub reklamacyjnego, nawet w sytuacji złożenia przez niego sprzeciwu wobec przetwarzania jego danych osobowych dla celów marketingowych.

Ten sam rodzaj sprzeciwu może dotyczyć możliwości **przekazywania danych** osobowych innym przedsiębiorcom, w tym przede wszystkim dla celów marketingowych[261].

Kluczowym dla praktycznej realizacji uprawnień osoby w zakresie sprzeciwu wobec przetwarzania danych osobowych dla celów marketingowych jest fakt, że może on zostać złożony **w każdej formie** – pismo, faks, mail, telefon, ustnie, i jednocześnie **nie wymaga uzasadnienia**[262].

Drugie uprawnienie, tj. żądanie zaprzestania przetwarzania żądania zaprzestania przetwarzania danych osobowych dla celów marketingowych, z uwagi na swoje skomplikowanie wydaje się być zupełnie pomijalne w obliczu możliwość wniesienia sprzeciwu. Jest ono znacznie bardziej pracochłonne, tj. obowiązek pisemnej formy zawierającej uzasadnienie, a jednocześnie **nie gwarantuje** takich samych skutków faktycznych, np. nieuwzględnienie żądania[263]. Przedsiębiorca **nie jest zobowiązany** złożonym przez osobę sprzeciwem lub żądaniem, jeżeli przesłanką przetwarzania jej danych osobowych dla celów marketingowych jest złożona uprzednio osobista zgoda w tym zakresie[264]. Należy jednak pamiętać, że zgoda ta nie może być dorozumiana z innego oświadczenia woli lub złożona z naruszeniem prawa[265].

6.2.2. MARKETING I REKLAMA W INTERNECIE

Jednym z najpopularniejszych rodzajów działań marketingowych wśród małych i średnich przedsiębiorstw jest przesyłanie informacji o produktach lub usługach na skrzynki poczty elektronicznej potencjalnych klientów, tzw. „**e-mail marketing**".

Zasady związane z tworzeniem **bazy adresów mail'owych** zostały opisane w poprzednim podrozdziale. Nie ma znaczenia czy zbieramy dane osobowy dla tradycyjnych form marketingu bezpośredniego, czy wykorzystujących nowe formy komunikacji. Takie same warunki przetwarzania dotyczą adresu pocztowego, elektronicznego czy numeru telefonu. Bazy danych marketingowych zawierające wyłącznie adresy e-mail nie będą w zasadzie zbiorami danych osobowych dla przedsiębiorcy, jeżeli nie będzie on miał możliwości powiązania ich z innymi informacjami, które umożliwią choćby pośrednią identyfikację osoby[266].

Studium przypadku:
Samodzielny adres e-mail: jan.kowalski@mail.pl, nie może być traktowany jako dana osobowa, w szczególności dla przedsiębiorcy, który nie jest dostawcą usług internetowych.
Ale już adres: jan@kowalski.pl, będzie z całą pewnością stanowił daną osobową, gdyż bez zaangażowania nadmiernych środków możliwe byłoby ustalenie właściciela domeny pocztowej.

Niemniej jednak jednoznaczne uznanie, że posiadana baza adresów poczty elektronicznej nie zawiera danych osobowych nie jest jednak bezwzględnie możliwe, a czas poświęcony na tworzenie uzasadnienia takiej opinii nie jest wart pozornego wyłączenia działalności marketingowej z rygorów Ustawy.

W e-mail marketingu rola ustawowej ochrony danych osobowych kończy się na poziomie legalności utworzenia zbioru danych i zapewnienia mu zasad bezpiecznego przetwarzania. Natomiast pozostałe elementy, najistotniejsze z punktu widzenia samych działań marketingowych przedsiębiorcy wynikają z wymagań **Ustawy** z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną[267].

Zgodnie z jej dyspozycją **zakazane jest przesyłanie niezamówionej informacji handlowej** (tzw. spamu), skierowanej do oznaczonego odbiorcy będącego osobą fizyczną za pomocą środków komunikacji elektronicznej, a w szczególności poczty elektronicznej (art. 10 ust.1)[268].

---

261 Patrz: P. Barta: Klauzula prawnie usprawiedliwionego …, s. 79-81.
262 P. Barta, P. Litwiński: *Ustawa o ochronie* …, s. 362.
263 Szerzej: A. Drozd: *Ustawa o ochronie* …, s. 235-236.
264 P. Barta: Klauzula prawnie usprawiedliwionego …, s. 81.
265 J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 453.
266 A. Drozd: *Ustawa o ochronie* …, s. 53.
267 (Dz.U. 144, poz. 1204, z późn. zm.).
268 Rozsyłanie spamu stanowi czyn zabroniony podlegający karze grzywny (art. 24).

Jednocześnie „informacja handlowa" rozumiana jest bardzo szeroko, i obejmuje każdą informację przeznaczoną bezpośrednio lub pośrednio do promowania:

- **towarów**;
- **usług**;
- **wizerunku przedsiębiorcy** (art. 2 pkt 2).

Tak więc warunkiem niezbędnym dla możliwości prowadzenia marketingu bezpośredniego przy użyciu poczty elektronicznej jest posiadanie **zgody odbiorcy** – użytkownika danego adresu e-mail (art. 10 ust 2). Zgoda ta nie może być domniemana czy dorozumiana z innego oświadczenia (art. 4 ust. 1 pkt 1). Musi obejmować wyraźne uprawnienie dla przedsiębiorcy do przesyłania informacji handlowej. Przede wszystkim nie może być wywiedziona z samego udostępnienia adresu poczty elektronicznej do realizacji innych transakcji. **Nie jest dopuszczalne**, by przedsiębiorca wykorzystał posiadany adres e-mail dla celów rozsyłania informacji handlowej bez uzyskania na to uprzedniej zgody[269].

Studium przypadku:
Posiadane przez przedsiębiorcę adresy e-mail wykorzystywane w kontaktach zawodowych nie mogę być wykorzystywane do rozsyłania reklam, bez uzyskania zgody ich użytkowników.

Co najważniejsze zgoda na przesyłanie informacji handlowych **nie może być domniemana** z faktu legalnego przetwarzania danych osobowych w zbiorze marketingowym. Dotyczy to zarówno sytuacji korzystania z przesłanki wyłączającej obowiązek pozyskania zgody osoby, której dane dotyczą, jak również w przypadku posiadania takiej zgody.

Sposób wyrażenia zgody na przesyłanie informacji handlowych nie został przez ustawodawcę określony.

Po pierwsze, osoba może samodzielnie zapisać się do, tzw. bazy mailingowej, **poprzez stronę internetową** przedsiębiorcy.

Po drugie, metodą uzyskiwania takie zgody – najczęściej od osób z pozyskanej od innego podmiotu bazy adresowej, jest uprzednie przesłanie wiadomości **e-mail z prośbą** w wyrażenie zgody na dalszą korespondencję handlową.

W obu przypadkach należy zapewnić **uwierzytelnienie zgody**, np. „kliknięcie" w odpowiedni link przesłany w mailu potwierdzającym rejestrację na stronie internetowej lub mailu z prośbą. Pozwoli to na utrwalenie na serwerze faktu udzielenia zgody, wraz z zapisem daty, godziny oraz numer IP komputera, z którego wykonano tą operację[270].

Niemniej w odniesieniu do tak popularnej metody jaką jest „mail z prośbą" istnieją jednak pewne poważne **zastrzeżenia**, co do jej poprawności. W większości tego rodzaju zapytań znajdują się dane stanowiące informację handlową, tj. opis rodzaju oferowanego towaru lub usługi, a przede wszystkim dane promujące wizerunek przedsiębiorcy[271].

Studium przypadku:
Wiadomości e-mail z zapytaniem o wyrażenie zgody na przesłanie informacji handlowej już w swoim tytule zawierają treść reklamy: „Najlepsze biuro tłumaczeń", „Najtańsze kalendarze", „Profesjonalny księgowy".

Ważnymi dla praktyki „e-mail marketingu" są jeszcze dwa determinanty identyfikujące przedmiot ustawowych ograniczeń. Przede wszystkim, termin „**oznaczony odbiorca**" nie powinien być interpretowany w sposób zawężający. Intencją ustawodawcy nie jest by wymóg ten dotyczył adresu elektronicznego bezpośrednio identyfikującego odbiorcę, tj. imię i nazwisko, lecz by adres ten umożliwiał z nim kontakt[272]. Ponadto tym „oznaczonym odbiorcą", ze względu na brak jednoznacznych ustawowych ograniczeń w tym zakresie mogą być także osoby prawne, czy instytucje[273]. W szczególności dotyczy to sytuacji tzw. **służbowych adresów e-mail**.

Studium przypadku:
Przedsiębiorca nie może bez otrzymania uprzedniej zgody wysyłać niezamówionych informacji handlowych na skrzynki e-mail, których adresy znalazł w ogólnodostępnych bazach firmowych, np. kowalski@firma.bi czy sekretariat@firma.bi.

Przedsiębiorca, który uzyskał właściwą zgodę odbiorcy na przesyłanie informacji handlowych na jego skrzynkę e-mail, powinien w każdej takiej wiadomości umieszczać:

1) informacje identyfikujące nadawcę, oraz jego adresy elektroniczne;
2) wyraźny opis form działalności promocyjnej, w szczególności obniżek cen, nieodpłatnych świadczeń pieniężnych lub

[269] X. Konarski: Komentarz do ustawy o świadczeniu usług drogą elektroniczną, Warszawa: Difin, 2004, s. 116-117.
[270] M. Ossowski (red.): *Prawo w email marketingu*, Warszawa: GetResponse, 2013, s. 13.
[271] E. Nowińska, M. du Vall: *Ustawa o zwalczaniu nieuczciwej* …, s. 420-421; M. Ossowski (red.): *Prawo w email marketingu* … , s. 9.
[272] E. Nowińska, M. du Vall: *Ustawa o zwalczaniu nieuczciwej* …, s. 421.
[273] X. Konarski: *Komentarz do ustawy* …, s. 116-117.

rzeczowych i innych korzyści związanych z promowanym towarem, usługą lub wizerunkiem, a także jednoznaczne określenie warunków niezbędnych do skorzystania z tych korzyści, o ile są one składnikiem oferty;
3) wszelkie informacje, które mogą mieć wpływ na określenie zakresu odpowiedzialności stron, w szczególności ostrzeżenia i zastrzeżenia (art. 9 ust. 2).

Ponadto wraz z każdą przesyłaną informacją handlową musi być zapewniona możliwość **odwołania zgody** (art. 4 ust. 1 pkt 2), np. link umożliwiający rezygnację z subskrypcji[274].

6.3. USŁUGI TELEINFORMATYCZNE

Rozwój rynku profesjonalnych usług wsparcia biznesu spowodował, że przedsiębiorcy coraz częściej rezygnują z własnych informatyków na rzecz współpracy z zewnętrznymi firmami, które przejmują na siebie wszystkie procesy związane z **przetwarzaniem zasobów informacyjnych firmy** – od dostawy i serwisu sprzętu komputerowego, po tworzenie i administrowanie wielkimi bazami danych.

Systemy informatyczne są rdzeniem kręgowym procesu przetwarzania danych osobowych w każdej współczesnej organizacji. Dlatego też powierzenie zarządzania nimi innemu podmiotowi wymaga właściwej oceny ryzyka i przygotowania niezbędnej ochrony prawnej.

Ponadto coraz popularniejsze jest wykorzystywanie „**chmur obliczeniowych**" (ang.: „*cloud computing*"); staje się to tak powszechne, jak każda inna usługa informatyczna. Czy jednak ten sposób na ograniczenie kosztów działalności firmy, nie stanowi kluczowego zagrożenia dla jej bezpieczeństwa informacyjnego.

6.3.1. OUTSOURCING OBSŁUGI INFORMATYCZNEJ

Powierzenie wyspecjalizowanemu podmiotowi z branży informatycznej obsługi i zarządzania systemem teleinformatycznym w firmie jest szczególną formą powierzenia danych osobowych do przetwarzania.

W takiej sytuacji nie ma przecież dążenia Administratora danych osobowych do zlecenia czynności związanych z bezpośrednim wykonywaniem czynności na danych osobowych. Nawet w sytuacji gdy zewnętrzna usługa informatyczna miałaby wiązać się z koniecznością choćby **pośredniego dostępu do przetwarzanych danych** osobowych, to niezbędne jest zawarcie umowy powierzenia[275].

Studium przypadku:
Przedsiębiorca korzystający z zewnętrznego serwisu, którego rolą jest wyłącznie konserwacja systemu informatycznego dopuszcza się faktycznej czynności powierzenia danych osobowych do przetwarzania.

Nawet posłużenie się innym podmiotem do **usunięcia nośników danych** osobowych jest powierzeniem danych osobowych do przetwarzania[276].

Generalne reguły, którymi powinien kierować się przedsiębiorca przy zawieraniu umowy na obsługę informatyczną z podmiotem zewnętrznym są takie same jak w opisanym już uprzednio outsourcingu kadrowo-płacowym. Niemniej jednak jego charakter wymaga uwzględnienia kilku ważnych elementów odnoszących się do **specyfiki administrowania systemem informatycznym** służącym do przetwarzania danych osobowych.

Umowa outsourcingu usług informatycznych – w zakresie powierzenia danych osobowych do przetwarzania – powinna zawierać takie elementy niezbędne dla jej prawidłowej realizacji, jak:
1) strony umowy,
2) przedmiot usługi,
3) miejsce wykonywania usługi,
4) sposób wykonywania usługi,
5) podwykonawcy,
6) rozwiązanie umowy,
7) zasady odpowiedzialności stron umowy[277].

Określenie **przedmiotu usługi** nie powinno być ograniczone wyłącznie do stwierdzenia, że jest nim „obsługa informatyczna", ale jasno wskazywać na zakres czynności w odniesieniu do systemu informatycznego do jakich ma prawo usługobiorca. Natomiast wymagane przez Ustawę określenie **celu powierzenia** powinno jasno precyzować, że jest to usługa wspierająca.

[274] M. Ossowski (red.): *Prawo w email marketingu* … , s. 10.
[275] A. Drozd: *Ustawa o ochronie* …, s. 209.
[276] Patrz: Postanowienie Sadu Najwyższego z dnia 11 grudnia 2000 roku (II KKN 438/00).
[277] Poniżej omówione zostaną jedynie te obszary powierzenia danych, które są odmienne od tych już opisanych uprzednio.

Przykładowy zapis umowy:

§1.
1. Zleceniodawca powierza Zleceniobiorcy wykonywanie obowiązków „Administratora systemu informatycznego".
2. Szczegółowy zakres obowiązków określonych w pkt 1 stanowi Załącznik nr 1 do niniejszej Umowy.
3. Zleceniobiorca w wyniku realizacji czynności określonych w Załączniku nr 1 do niniejszej Umowy będzie miał dostęp do przetwarzanych przez Zleceniodawcę danych osobowych.
4. Zleceniodawca może przetwarzać dane osobowe w zakresie nie wykraczającym poza niezbędny do realizacji czynności określonych w Załączniku nr 1 do niniejszej Umowy.

W tym przypadku nie ma obowiązku wymieniania wszystkich zbiorów danych osobowych oraz zakresu dopuszczalnych czynności przetwarzania, gdyż nie jest to w praktyce możliwe, a przede wszystkim nie determinuje ich bezpieczeństwa[278].

Ponadto umowa powinna jednoznacznie wskazywać na siedzibę Administratora danych osobowych jako podstawowe **miejsce świadczenia usługi**, a tym samym możliwości dostępu do danych osobowych.

Przykładowy zapis umowy:

§2.
1. Zleceniobiorca będzie wykonywał swoje usługi związane z dostępem do systemu informatycznego Zleceniodawcy wyłącznie jego w siedzibie.
2. Zabrania się Zleceniobiorcy zdalnego dostępu do systemu informatycznego Zleceniodawcy.
3. Ewentualne umożliwienie dostępu zdalnego do systemu informatycznego Zleceniobiorcy musi zostać udzielone na piśmie, ze szczegółowym określeniem zakresu dostępu i jego dopuszczalnego czasu trwania.

Administrator danych osobowych dopuszczając **możliwość zdalnego dostępu** do systemu informatycznego powinien przeprowadzić analizę ryzyka związanego z takim działaniem. Zdalny dostęp do systemu informatycznego Administratora danych osobowych musi być bezwzględnie zabezpieczony metodami kryptograficznymi.

Bezwzględnie wszystkim pracownikom, którzy będą realizowali jakiekolwiek prace związane z dostępem do systemu informatycznego, Administrator danych osobowych musi wydać właściwe „**Upoważnienia do przetwarzania** danych osobowych"[279]. Zakres tych upoważnień powinien być adekwatny do zadań poszczególnych pracowników.

W związku z tym, że realizacja tego rodzaju usług nie oznacza rzeczywistego powierzenia danych do przetwarzania, a w szczególności przekazania ich do podmiotu zewnętrznego, nie ma konieczności sprawdzania czy wdrożył on obowiązkowe zabezpieczenia organizacyjno-techniczne oraz dokumentację bezpieczeństwa w swojej organizacji.

Jednocześnie istnieje obowiązek **zapoznania** wszystkich zewnętrznych pracowników z własnymi zasadami bezpieczeństwa oraz odebranie zobowiązań do zachowania poufności.

Przykładowy zapis umowy:

§3.
1. Warunkiem rozpoczęcia przez Zleceniobiorcę wykonywania usługi określonej w §1 jest zapoznanie się przez jego pracowników z zasadami ochrony danych osobowych obowiązującymi u Zleceniodawcy.
2. Wszyscy pracownicy Zleceniobiorcy zobowiązani są do podpisania oświadczenia o zachowaniu poufności.

Jednocześnie przyjmuje się, że Administrator danych osobowych powinien zabezpieczyć sobie w umowie możliwość **regularnych kontroli**[280].

Ważnym elementem umowy powinna być kwestia możliwości zlecania zadań **podwykonawcom**, wraz z ich zakresem[281].

Przykładowy zapis umowy:

§5.
1. Zleceniobiorca nie może zlecić wykonania jakiejkolwiek części niniejszej Umowy innemu podmiotowi bez uzyskania pisemnej zgody Zleceniodawcy.
2. Zleceniobiorca pragnący powierzyć część umowy podwykonawcy musi przedłożyć Zleceniodawcy informacje o tym podmiocie i planowany zakresie podzlecenia, wraz z analizą ryzyka.

[278] A. Krasuski, D. Skolimowska: *Dane osobowe* …, s. 139 i nast.
[279] J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 573.
[280] A. Krasuski, D. Skolimowska: *Dane osobowe* …, s. 149-150.
[281] P. Barta, P. Litwiński: *Ustawa o ochronie* …, s. 326-327.

Ostatnim z obowiązkowych elementów jaki powinien być umieszczony w umowie powierzenia, to kwestia **odpowiedzialności** Przetwarzającego za niezgodne z prawem oraz zapisami umownymi przetwarzanie danych osobowych[282].

Przykładowy zapis umowy:

§6.

1. Zleceniobiorca ponosi pełną odpowiedzialność za nieprzestrzeganie zasad określonych w Ustawie, w szczególności za działania lub zaniechania sprzeczne z zapisami niniejszej umowy.
2. Zleceniobiorca ponosi odpowiedzialność za wszelkie działania lub zaniechania swoich pracowników, które doprowadziły lub mogły doprowadzić do naruszenia zasad bezpieczeństwa danych osobowych.

6.3.2. PRZETWARZANIE DANYCH OSOBOWYCH W „CHMURZE"[283]

Korzystanie przez przedsiębiorcę z „chmury obliczeniowej" nie jest w żaden sposób określone w polskim prawie, nie jest jednak również zakazane[284]. Należy ją więc na tym etapie traktować wyłącznie jako **usługę przetwarzania danych osobowych** przez podmiot zewnętrzny. Z tego też względu obowiązkiem Administratora danych osobowych, który zamierza z niej skorzystać, jest właściwe przeprowadzenie procesu powierzenia danych osobowych do przetwarzania. Z uwagi na swoją specyfikę różni się ona jednak znacząco od tych opisanych już w tym rozdziale.

Podjęcie decyzji o chęci korzystania z usługi „chmurowej" należy poprzedzić przede wszystkim **rzetelną analizą zagrożeń,** jakie się wiążą z tego rodzaju powierzeniem danych osobowych. Wskazać należy chociażby na najważniejszy z argumentów jej przeciwników, a mianowicie znikoma możliwość bezpośredniego nadzoru nad procesem przetwarzania i działaniami podejmowanymi przez dostawcę tej usługi[285]. Brak zakazu prawnego nie może być traktowany jako całkowita swoboda Administratora danych osobowych w tym względzie, w szczególności w odniesieniu do obowiązków „**szczególnej staranności**" (art. 26) i „**właściwego zabezpieczenia**" (art. 36 ust. 1).

Pierwszym warunkiem decydującym o wyborze usługodawcy i dalszego postępowania w celu powierzenia danych osobowych do przetwarzania, powinna być **identyfikacja miejsca**:

1) siedziby dostawcy „chmury";
2) fizycznej lokalizacji serwerów[286].

Pozwoli to na określenie, czy zasady przetwarzania powierzonych danych osobowych będą mogły być bezpośrednio obwarowane wymogami określonymi w:

1) **Ustawie** – dla usługi realizowanej w całości w Polsce,
2) **Dyrektywie 95/46/WE** – dla usługi realizowanej na terytorium Europejskiego Obszaru Gospodarczego,

czy będzie wymagane szczegółowe przeniesienie wszystkich zasad bezpieczeństwa do **umowy**[287].

Należy także ustalić ewentualnych **podwykonawców** dostawcy „chmury", ich zakresy odpowiedzialności, siedzibę oraz fizyczną lokalizację ich systemów informatycznych, które będą wykorzystywane do świadczenia usługi.

Studium przypadku:

Przedsiębiorca zawierając umowę o świadczenie usług „chmurowych" z dostawcą, który ma swoją siedzibę we Francji, ale do przetwarzania danych wykorzystuje infrastrukturę serwerową zlokalizowaną w Algierii, nie może ograniczyć się wyłącznie do oceny prawa europejskiego czy francuskiego.

Drugim elementem kreującym procedurę przygotowania i zarządzania przetwarzaniem danych osobowych w „chmurze" jest wybór **modelu usługi**:

1) Infrastruktura chmury jako usługa (ang.: *Infrastructure as a Service – IaaS*) – korzystanie z zasobów obliczeniowych, sieciowych, przechowywania danych i innych.

---

[282] Szerzej: J. Barta, P. Fajgielski, R. Markiewicz: *Ochrona danych osobowych* …, s. 576-580.

[283] Rozdział ten dotyczy wyłącznie tzw. „chmur publicznych", a nie dedykowanych rozwiązań biznesowych, tzw. „chmur prywatnych".

[284] Patrz: M. Maj: GIODO: Przetwarzanie danych osobowych w chmurach jest dopuszczalne, ale .... Rozmowa z dr Wojciechem R. Wiewiórowskim – Generalnym Inspektorem Ochrony Danych Osobowych, „Dziennik Internautów", 24.05.2011. Dostęp pod adresem: http://di.com.pl/giodo-przetwarzanie-danych-osobowych-w-chmurach-jest-dopuszczalne-ale-38127, (10.11.2015).

[285] Patrz: Opinia 5/2012 *w sprawie przetwarzania danych w chmurze obliczeniowej*, Grupa Robocza Artykułu 29 ds. Ochrony Danych, Komisja Europejska, (01037/12/PL, WP 196), s. 5 i nast.

[286] *Dekalog chmuroluba. Dziesięć zasad stosowania usług chmurowych przez administrację publiczną*, Generalny Inspektor Ochrony Danych Osobowych. Dostęp pod adresem: http://www.giodo.gov.pl/259/id_art/6271/j/pl, (10.11.2015), pkt 1, 3.

[287] B. Fischer: Podział odpowiedzialności za chmurowe przetwarzanie danych osobowych z uwzględnieniem kształtowania regulacji umownych – wybrane zagadnienia, „Monitor Prawniczy", nr 9, 2014 – Dodatek, s. 16-17.

2) Platforma chmury jako usługa (ang.: *Platform as a Service – PaaS*) – korzystanie z zasobów obliczeniowych, sieciowych, przechowywania danych i innych oraz wsparcia technicznego.
3) Oprogramowanie chmury jako usługa (ang.: *Software as a Service – SaaS*) –korzystanie z aplikacji umieszczonych w chmurze oraz zasobów obliczeniowych, sieciowych, przechowywania danych i innych[288].

Tworzą one rodzaj piramidy usług. Im bardziej zaawansowana – od dzierżawy miejsca na dysku, po kompleksową obsługę całego procesu – tym przedsiębiorca ma mniejszy wpływ na przetwarzanie powierzonych danych osobowych, a tym samym winien lepiej zabezpieczyć umowne warunki takiej usługi[289].

Trzecim elementem decydującym o wyborze usługi „chmurowej" jest potwierdzenie wypełniania przez dostawcę wymagań związanych z organizacyjno-technicznymi zabezpieczeniami danych osobowych. Mając na uwadze obiektywną trudność w osobistym skontrolowaniu zabezpieczeń „chmury", należy zobowiązać dostawcę usługi do umożliwienia **wglądu do dokumentacji bezpieczeństwa** dla poszczególnych miejsc przetwarzania danych. Informacja taka choć stanowi ważną tajemnicę dostawcy usługi, wydaje się być jednak niezbędna do możliwości oceny wypełniania minimalnych standardów zabezpieczeń dla zapewnienia ochrony powierzonych danych osobowych[290].

Studium przypadku:
Przedsiębiorca, który w żaden sposób nie potwierdzi zastosowanych przez dostawcę usługi „chmurowej" środków bezpieczeństwa może się liczyć z odpowiedzialnością karną za niewłaściwe zabezpieczenie danych osobowych.

Przedsiębiorca decydujący się na korzystanie z usług przetwarzania swoich danych osobowych w „chmurze obliczeniowej" musi zawrzeć w tym celu **umowę powierzenia danych osobowych** (art. 31 ust. 1).

Poza wymienionymi już uprzednio generalnymi zapisami każdej tego rodzaju umowy, ta z dostawcą usługi „chmurowej" musi określać ponadto szersze **gwarancje** dla Administratora danych osobowych w postaci:
1) przekazywania wyprzedzających informacji o zmianie lokalizacji serwerów służących do realizacji usługi;
2) przekazywania informacji o istotnych zmianach technicznych funkcjonalności usługi;
3) obowiązku rejestracji wszelkich operacji na powierzonych danych osobowych;
4) obowiązku wspierania w realizacji praw osób, których dane dotyczą, w zakresie dostępu do swoich danych, ich poprawienia lub usunięcia;
5) całkowitego zakazu dalszego przekazywania powierzonych danych osobowych jakimkolwiek podmiotom, poza znanych w chwili zawierania umowy podwykonawców;
6) obowiązku zawiadamiania o wszelkim udostępnieniu powierzonych danych osobowych dla organów egzekwowania prawa;
7) zobowiązania dostawcy do zawiadamiania o wszelkich przypadkach naruszeń bezpieczeństwa infrastruktury „chmurowej", które mogą mieć wpływ na ochronę powierzonych danych osobowych;
8) określenia warunków zwrotu danych osobowych lub ich zniszczenia po zakończeniu realizacji usługi;
9) wyznaczenia właściwych sankcji finansowych lub innych w przypadku niezapewnienia zgodności postępowania dostawcy z zapisami umowy[291].

Ponadto zaleca się, aby w procesie zawierania umowy o świadczenie usług przetwarzania danych osobowych w „chmurze" **wykorzystywać**:
- standardowe klauzule umowne;
- wiążące reguły korporacyjne[292].

W związku z powyższym, w szczególności **niedozwolone** jest zawieranie przez przedsiębiorcę umów związanych z usługą przetwarzania „chmurowego" na warunkach określonych wyłącznie przez dostawcę, tzw. umowa adhezyjna[293]. W szczególności gdy jej zapisy nie gwarantują minimalnego poziomu ochrony danych osobowych określonego przez Ustawę.

---

[288] Opinia 5/2012 w sprawie przetwarzania danych …, s. 38.
[289] P. Kawczyński: Przetwarzanie danych w chmurze – cz. 1, „Portal ODO", 10.06.2014. Dostęp pod adresem: https://www.portalodo.com/entry/przetwarzanie-danych-w-chmurze-cz-1, (20.11.2015).
[290] Dekalog chmuroluba. …, pkt. 2.
[291] Opinia 5/2012 w sprawie przetwarzania danych …, s. 18-20.
[292] Szerzej: B. Fischer: Ponadgraniczne przekazywanie danych osobowych – charakter prawny regulacji z uwzględnieniem uzupełniającej roli „soft law", (w:) A. Mednis (red.): Prywatność a ekonomia. ochrona danych osobowych w obrocie gospodarczym, Warszawa: Stowarzyszenie Absolwentów Wydziału Prawa i Administracji UW, 2013, s. 81-90; J. Byrski, X. Konarski: Wiążące reguły korporacyjne jako podstawa prawna przekazywania danych osobowych do państwa trzeciego, (w:) A. Mednis (red.): Prywatność a ekonomia …, s. 91-102.
[293] B. Fischer: Podział odpowiedzialności za chmurowe …, s. 15.

7. NADZÓR NAD OCHRONĄ DANYCH OSOBOWYCH

mgr Bartosz Mendyk

Europejski ustawodawca uchwalając Dyrektywę 95/46/WE zdawał sobie sprawę, że nawet najlepsze prawo, które nie ma narzędzi do jego egzekwowania, staje się iluzoryczne. Ponieważ Unia Europejska stara się gwarantować ochronę praw jednostki na najwyższym poziomie, zabiega o to, żeby z jednej strony jednostki miały proceduralne środki pozwalające dochodzić swoich praw, z drugiej zaś, żeby w państwach członkowskich funkcjonowały odpowiednie instytucje, stojące na straży przestrzegania ustanowionego prawa[294].

7.1. INSTYTUCJA GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH

W Dyrektywie 95/46/WE znalazł się przepis mówiący, że „każde Państwo Członkowskie zapewni, że jeden lub więcej organów władzy publicznej będzie odpowiedzialny za kontrolę stosowania na jego terytorium przepisów przyjętych przez Państwa Członkowskie na mocy dyrektywy"[295]. W Polsce funkcję tę sprawuje **Generalny Inspektor Ochrony Danych Osobowych (GIODO)**, który ma za zadanie dbać, żeby standardy ochrony danych osobowych były należycie przestrzegane[296]. Pomimo, że jego miejsce w porządku prawnym jest niedookreślone w ustawie, można przyjąć, iż jest to centralny organ państwa[297].

Lista zadań, które postawiono przed Generalnym Inspektorem postawiono, jest obszerna[298]. Omówione zostaną te przydatne dla przedsiębiorców.

Przede wszystkim są to uprawnienia **związane z prowadzeniem kontroli prawidłowości przetwarzania danych osobowych** z przepisami o ochronie danych. Wyróżnić można:

1) **kontrole** zgodności przetwarzania danych z przepisami o ochronie danych osobowych w drodze postępowań inspekcyjnych[299],
2) rozpatrywanie skarg na działania administratorów danych w sprawach związanych z wykonaniem przepisów o ochronie danych czy postępowania rejestracyjnego poprzez wydawanie decyzji administracyjnych; nie wprowadzono szczególnej procedury rozpatrywania skarg, ani ich szczególnej formy składania, w związku z tym do postępowań z zakresu ochrony danych osobowych stosuje się ogólne przepisy postępowania administracyjnego[300];
3) zapewnienie wykonania przez zobowiązanych obowiązków o charakterze niepieniężnym wynikających z decyzji administracyjnej przez zastosowanie środków egzekucyjnych przewidzianych w ustawie o postępowaniu egzekucyjnym w administracji; egzekucji administracyjnej podlegają wszystkie decyzje administracyjne Generalnego Inspektora nakładające na strony obowiązek (nakaz) do wykonania, którym nadano rygor natychmiastowej wykonalności; są one ostateczne, czyli nie można się od nich odwołać; obowiązek do wykonania jest nakładany w formie pisemnej[301] na stronę (zobowiązanego) i może polegać na:
   a) **usunięciu uchybień w danych osobowych** – każda osoba, która dobrowolnie podała dane osobowe, może w każdej chwili zażądać usunięcie jej danych osobowych ze zbiorów danych (np. wykreślenia z listy mailingowej);

---

[294] Porównanie doświadczeń europejskich i amerykańskich dowodzi, że UE lepiej chroni prawa jednostki. Por. P. Zegarek , *Czy program „Safe Harbor" faktycznie trafił do kosza? Jak jest naprawdę?,* http://blog-daneosobowe.pl/czy-program-safe-harbor-faktycznie-trafil-do-kosza-jak-jest-naprawde/ (dostęp 09.12.2015).

[295] Zob. art. 28 Dyrektywy 95/46/WE

[296] Urząd ten został powołany art. 13 ust. 1 Ustawy.

[297] M. Kawecki, Generalny Inspektor Ochrony Danych Osobowych jako centralny organ administracji państwowej, „Przegląd Prawa Technologii Informacyjnych. ICT Law Review", nr 1/2013, s. 38-44

[298] Niestety są one niewspółmierne do kompetencji. Jak zauważa B. Przywora, należały Generalnego Inspektora doposażyć w większą ilość kompetencji np. inicjatywy ustawodawczej, czy prawo wniesienia skargi konstytucyjnej. Por. B. Przywora, O potrzebie wzmocnienia kompetencji Generalnego Inspektora Ochrony Danych Osobowych w zakresie bezpieczeństwa państwa, Program Narodowego Centrum Badania i Rozwoju, dostępny pod adresem http://mrj.uksw.edu.pl/sites/default/files/Repozytorium/Prezentacje/Zadania_i_kompetencje_organow_publicznych_w_zakresie_jawnosci_i_jej_ograniczen/dr_boguslaw_przywora.pdf. (dostęp: 09.12.2015).

[299] Opisane szczegółowo przez B. Przywora, Z problematyki kontroli przetwarzania i ochrony danych osobowych przez Generalnego Inspektora Ochrony Danych Osobowych, *(w:)* Jawność i jej ograniczenia. Zadania i kompetencje, red. B. Szmulik B., G. Szpor G., C.H. Beck, Warszawa 2015.

[300] Zob. E. Kulesza, Ochrona Danych osobowych w pomocy społecznej, Warszawa, Wydawnictwo: „Centrum Rozwoju Zasobów Ludzkich", 2013, s. 95-96.

[301] Generalny Inspektor nie może nakładać obowiązków w formie ustnej zob. P. Przybysz, Kompetencje egzekucyjne Generalnego Inspektora Ochrony Danych Osobowych oraz postępowanie egzekucyjne prowadzone przez organ ochrony danych osobowych, dodatek do Monitor Prawniczy, nr 3, 2011, s. 1032.

b) uzupełnieniu danych osobowych;
c) uaktualnieniu danych osobowych – każda osoba, której są zbierane dane osobowe ma prawo, aby były one aktualne; w związku z powyższym, jeżeli administrator danych odmawia uaktualnienia danych osobowych, Generalny Inspektor może nakazać uaktualnienie danych osobowych;
d) sprostowaniu danych osobowych – sytuacja analogiczna do nakazania uaktualnienia;
e) udostępnieniu lub nieudostępnieniu danych osobowych[302]; z żądaniem wydania decyzji zakazującej udostępniania danych do Generalnego Inspektora może wystąpić osoba, której dane dotyczą[303];
f) zastosowaniu dodatkowych środków zabezpieczających zgromadzone dane osobowe, jeśli w wyniku kontroli uznał, że dotychczasowe narzędzia są niewystarczające;
g) wstrzymaniu przekazywania danych osobowych do państwa trzeciego;
h) zabezpieczeniu danych lub przekazaniu ich innym podmiotom;
i) usunięciu danych osobowych, w szczególności wtedy, kiedy klienci wycofali zgody na ich przetwarzanie;

4) nakaz ponownego zgłoszenia zbioru danych osobowych do rejestracji u Generalnego Inspektora wolnego od wad, które były powodem odmowy pierwotnej rejestracji.
5) prowadzenie rejestru zbiorów danych oraz udzielanie informacji o zarejestrowanych zbiorach. Prowadzenie zbiorów umożliwia m.in. sprawowanie kontroli nad prawidłowością procesu ich przetwarzania; jest to szczególnie istotne w przypadku danych szczególnie chronionych (tzw. danych wrażliwych). W 2014 r. zgłoszono 43 300 zbiorów, w tym z sektora prywatnego 16 597 zbiorów;
6) prowadzenie rejestru Administratorów bezpieczeństwa informacji – obowiązek ten został nałożony na Generalnego Inspektora od 2015 r;
7) udzielanie informacji o zarejestrowanych zbiorach danych i zarejestrowanych Administratorach bezpieczeństwa informacji; obowiązek zawiadomienia przez Generalnego Inspektora – w przypadku podejrzenia popełnienia przestępstwa określonego w ustawie – organów ścigania.

Uprawnienia te mają duże znaczenie dla MŚP. Co roku biuro Generalnego Inspektora podejmuje coraz więcej interwencji kontrolnych. Z każdym rokiem nakłada też coraz więcej kar za nieprzestrzeganie przepisów, dlatego spełnienie przez przedsiębiorców wszelkich obowiązków nie powinno być odwlekane na przyszłość.

7.2. ZASADY KONTROLI GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH

Jedną z funkcji Generalnego Inspektora Ochrony Danych Osobowych jest przeprowadzenie kontroli zarówno w sektorze prywatnym, jak i publicznym. Skarg wpływających do Generalnego Inspektora jest co roku więcej. W 2014 r. liczba skarg wyniosła 2 481 a w kolejnych latach będzie ich zapewne coraz więcej. Wiąże się to z tym, że konsumenci coraz większą wagę przywiązują do bezpieczeństwa i prawidłowego korzystania z ich danych osobowych.

Zgodnie z prawem kontrolę u przedsiębiorców wszczyna się nie wcześniej niż po upływie 7 dni i nie później niż przed upływem 30 dni od dnia doręczenia zawiadomienia o zamiarze wszczęcia kontroli. Jeżeli kontrola nie zostanie wszczęta w terminie 30 dni od dnia doręczenia zawiadomienia, wszczęcie kontroli wymaga ponownego zawiadomienia[304].

Uważa się, że czynności kontrolne **spełniają dwie funkcje**:

1) środka pozwalającego stwierdzić, czy istnieją podstawy do wszczęcia postępowania administracyjnego i stanowiącego jednocześnie przesłankę wszczęcia tego postępowania w trybie art. 17 Ustawy;
2) **środka dowodowego w już toczącym się postępowaniu administracyjnym**[305].

Inspektor może przystąpić do wykonywania czynności kontrolnych po wydaniu mu imiennego upoważnienia do ich przeprowadzenia. W upoważnieniu powinny być wskazane informacje istotne dla przebiegu kontroli. W szczególności będą to:

1) dane inspektora,
2) przedmiot i zakres kontroli,
3) data rozpoczęcia i przewidywany termin zakończenia kontroli.

Upoważnienie powinno być podpisane przez Generalnego Inspektora bądź jego zastępcę.

W ramach przygotowania do kontroli Administrator danych osobowych powinien przygotować:

1) **wymaganą dokumentację** przetwarzania danych osobowych:
   a) **Politykę bezpieczeństwa informacji**,
   b) **Instrukcję zarządzania systemami informatycznymi;**

[302] W zakresie nieudostępnienia danych osobowych zob. P. Fajgielski, Udostępnianie danych osobowych – zagadnienia wybrane, …, s.10-11.
[303] zob. P. Fajgielski, Udostępnianie danych osobowych – zagadnienia wybrane, .., s.12.
[304] Artykuł 79 ust. 4 Ustawy z 2 lipca 2004 roku o swobodzie działalności gospodarczej. (Dz.U. 2004 nr 173 poz. 1807).
[305] G. Sibiga, Postępowanie w sprawach ochrony danych osobowych, Warszawa, Dom Wydawniczy ABC, 2003, s. 149-150.

2) **ewidencję osób upoważnionych** do przetwarzania danych osobowych oraz **upoważnienia do przetwarzania danych osobowych**;
3) **rejestr zbiorów przetwarzanych danych**;
4) **pełnomocnictwa Administratora bezpieczeństwa informacji** do występowania w imieniu Administratora danych osobowych.

Niezależnie od powyższego **kontrolerzy mogą wystąpić o dokumenty regulujące działanie całej jednostki**, czyli np. jej statut lub regulamin organizacyjny.

W trakcie kontroli można spodziewać się pytań pozornie niezwiązanych z ochroną danych osobowych, które będą dotyczyły:
1) sposobu zapewnienia ochrony fizycznej budynku,
2) gospodarki kluczami,
3) umowy z firmą sprzątającą[306].

Kontrole w imieniu Generalnego Inspektora przeprowadzają zespoły inspektorów[307]. Zazwyczaj w ich składzie jest prawnik i informatyk.

Podczas kontroli inspektorzy Generalnego Inspektora sprawdzają m.in.:
1**)** czy w kontrolowanym podmiocie **została opracowana polityka prywatności** i **instrukcja zarządzania systemem informatycznym**,
2) **w jaki sposób są chronione dane osobowe pracowników**,
3) **w jaki sposób są chronione dane osobowe klientów**.

Kolejną czynnością przeprowadzaną w ramach kontroli jest sprawdzenie czy przedsiębiorca zarejestrował zbiory danych osobowych, które podlegają ustawowemu obowiązkowi.

Kontroli podlegają **systemy teleinformatyczne**, za pomocą których są przetwarzane dane osobowe. Powyższe systemy są rozumiane szeroko i obejmują:
1) system klasy ERP czy CRM, czyli systemy informatyczne służące wspomaganiu zarządzania przedsiębiorstwem poprzez gromadzenie danych; umożliwiają one ustalenie uprawnień dostępu dla poszczególnych użytkowników;
2) komputery;
3) smartfony,
4) tablety.

Do najważniejszych uprawnień inspektorów należy:
1) **prawo wejścia do każdego pomieszczenia**, **w którym jest zlokalizowany zbiór danych**, oraz do pomieszczenia, w którym są przetwarzane dane poza zbiorem danych (np. serwerownia, dział kadr i płac, dział marketingu[308]);
2) **prawo do przeprowadzenia niezbędnych badań oraz innych czynności kontrolnych w celu oceny zgodności przetwarzania danych** z Ustawą; jeżeli inspektorzy uznają, że przedstawiona im dokumentacja lub ogląd miejsc są niewystarczające do ustalenia stanu faktycznego, mogą np. zażądać złożenia pisemnych lub ustnych wyjaśnień od osób, które przetwarzają dane osobowe[309];
3) **prawo do wzywania i przesłuchiwania osoby** w zakresie niezbędnym do ustalenia stanu faktycznego, w zakresie zbadania zgodności przetwarzania danych osobowych z ustawą;
4) **prawo do przeprowadzania oględzin** urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

W trakcie trwania kontroli do obowiązków Administratora danych osobowych należy:
1) **umożliwienie inspektorowi przeprowadzenie czynności służbowych**, czyli dokonania kontroli dokumentów, oględziny miejsc przetwarzanie danych osobowych itd.;
2) **spełnienie żądań związanych z kontrolą**, a w szczególności dopuszczenie inspektora do pomieszczeń przetwarzania danych, umożliwienie przesłuchania osób, które przetwarzają dane osobowe, udostępnienie dokumentów itd.; nadużyciem ze strony kontrolera będzie jednakże żądanie umożliwienia nieograniczonego poruszania się po kontrolowanym podmiocie, w szczególności np. żądanie dostępu do gabinetu prezesa, jeśli nie ma w nim dokumentów objętych przedmiotem kontroli[310];

---

306 P. Kowalik, Kontrola GIODO w jednostce – praktyczne porady, „Informacja w administracji publicznej", nr 3, 2015, s. 21.

307 Ustawa ani Rozporządzenie nie określa żadnych wymagań wobec pracowników kontrolerów Biura Generalnego Inspektora. Każdy zatem pracownik Biura Generalnego Inspektora, niezalenie od stosunku pracy czy służbowego, wykształcenia, stażu pracy i kwalifikacji, jeżeli ma stosowne upoważnienie, może wykonywać czynności kontrolne. P. Szustakiewicz, Kontrole Generalnego Inspektora Ochrony Danych Osobowych, "Kontrola Państwowa", nr 6, 2007, s. 5.Ch

308 B. Pilc, Rola administratora bezpieczeństwa informacji podczas inspekcji prowadzonej przez Generalnego Inspektora Ochrony Danych Osobowych, dodatek „Monitor Prawniczy", nr 7, 2012, s. 40-41.

309 Por. B. Pilc, Rola administratora bezpieczeństwa informacji podczas inspekcji prowadzonej ..., s .1046.

310 P. Szustakiewicz, Kontrole Generalnego Inspektora …, s. 52

3) **umożliwienie w godzinach od 6.00 do 22.00 wstępu na teren przedsiębiorstwa inspektorom**, (w praktyce kontrole odbywają się w godzinach pracy przedsiębiorstwa);
4) **umożliwienie wglądu do wszelkich** dokumentów **i wszelkich danych mających bezpośredni związek** z przedmiotem kontroli oraz umożliwienie sporządzania ich kopii[311].

Utrudnianie pracy kontrolerom jest karalne grzywną, karą ograniczenia wolności lub karą pozbawienia wolności do lat dwóch[312].

Warto, aby **Administrator danych osobowych oddelegował pracownika do stałej współpracy z inspektorami**. Osoba ta powinna oczywiście mieć rozeznanie w przedmiocie kontroli. Jej zadanie będzie polegało na udzielaniu inspektorom wstępnych wyjaśnień, kontaktowaniu ich z innymi pracownikami, pomaganiu w zapoznaniu się z niuansami działania jednostki itd.

Czas kontroli to z reguły od trzech do dziesięciu dni.

W przypadku naruszenia przepisów Ustawy Generalny Inspektor z urzędu lub na wniosek osoby zainteresowanej w drodze decyzji administracyjnej[313] nakazuje przywrócenie stanu zgodnego z prawem[314], czyli:
1) **usunięcie uchybień** – np. zebranie zgód na przetwarzanie danych od osób, których dane są przetwarzane bez uzyskania na to zezwolenia;
2) **uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych**;
3) **zastosowanie dodatkowych środków zabezpieczających** zgromadzone dane osobowe – np. wprowadzenie dłuższych i bardziej skomplikowanych haseł;
4) **wstrzymanie przekazywania** danych osobowych do państwa trzeciego;
5) **zabezpieczenie danych lub przekazanie ich innym podmiotom**;
6) **usunięcie danych osobowych**.

Z czynności kontrolnych inspektorzy sporządzają **protokół**, którego jeden egzemplarz doręczają kontrolowanemu administratorowi danych. Protokół kontroli powinien zawierać:
1) nazwę podmiotu kontrolowanego w pełnym brzmieniu i jego adres;
2) imię i nazwisko, stanowisko służbowe, numer legitymacji służbowej oraz numer upoważnienia inspektorów;
3) imię i nazwisko osoby reprezentującej podmiot kontrolowany oraz nazwę organu reprezentującego ten podmiot (zgodnie z Krajowym Rejestrem Sądowym);
4) datę rozpoczęcia i zakończenia czynności kontrolnych, z wymienieniem dni przerw w kontroli;
5) określenie przedmiotu i zakresu kontroli;
6) opis stanu faktycznego stwierdzonego w toku kontroli oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
7) wyszczególnienie załączników stanowiących składową część protokołu;
8) omówienie dokonanych w protokole poprawek, skreśleń i uzupełnień;
9) parafy inspektora i osoby reprezentującej podmiot kontrolowany na każdej stronie protokołu;
10) wzmiankę o doręczeniu egzemplarza protokołu osobie reprezentującej podmiot kontrolowany;
11) wzmiankę o wniesieniu lub niewniesieniu zastrzeżeń i uwag do protokołu;
12) datę i miejsce podpisania protokołu przez inspektora oraz przez osobę lub organ reprezentujący podmiot kontrolowany.

Protokół z kontroli podpisują: **inspektorzy** dokonujący inspekcji oraz **kontrolowany Administrator danych osobowych,** który może wnieść do protokołu umotywowane zastrzeżenia i uwagi. Mogą one się odnosić zarówno do ustaleń zawartych w protokole, jak i do sposobu przeprowadzenia kontroli[315]. W razie odmowy podpisania protokołu przez kontrolowanego Administratora danych osobowych, inspektor czyni o tym wzmiankę w protokole, a odmawiający podpisu może w terminie 7 dni kalendarzowych przedstawić Generalnemu Inspektorowi swoje stanowisko na piśmie. Żaden przepis nie określa jednak, jakie konsekwencje prawne wywołuje takie zachowanie kierownika jednostki kontrolowanej. Inspektor nie może utrudniać podmiotowi kontrolowanemu korzystania z tych uprawnień.

W razie stwierdzenia, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby fizycznej będącej Administratorem danych osobowych wyczerpuje znamiona przestępstwa określonego w Ustawie o ochronie danych osobowych, Generalny Inspektor kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa lub o podejrzeniu popełnienia przestępstwa, dołączając dokumentujące je dowody, które zostały zgromadzone w wyniku kontroli.

Warto w tym miejscu zaznaczyć, że pod koniec 2012 r. Generalny Inspektor **podpisał porozumienie z Państwową Inspekcją Pracy (PIP)**, na podstawie którego obie instytucje dokonują kontroli zarówno pod kątem przestrzegania

311 Por. B. Pilc, Rola administratora bezpieczeństwa informacji podczas inspekcji …, s. 37.
312 D. Ossowska-Salamonowicz, Ochrona danych osobowych w działalności dziennikarskiej, Olsztyn Wydawnictwo „Uniwersytetu Warmińsko- Mazurskiego", 2015, s. 117.
313 Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 13-03-2014 o sygn. (II SA/Wa 1988/13).
314 Decyzja Generalnego Inspektora z dnia 20-02-2013 o sygn. (DOLiS/DEC-196/13/10633).
315 D. Ossowska-Salamonowicz, *Ochrona danych osobowych w działalności* …, s. 120.

przepisów prawa pracy, jak i ochrony danych osobowych. Tylko w 2014 r. PIP przeprowadziła ok. 88 tys. kontroli. W sytuacji gdy PIP stwierdził nieprawidłowości w zakresie przetwarzania danych osobowych, przekazuje informację o uchybieniach Generalnemu Inspektorowi.

7.3. RODZAJE ODPOWIEDZIALNOŚCI

Naruszenie przepisów Ustawy staje się powodem poniesienia różnych rodzajów odpowiedzialności.

1) **Administracyjnej (finansowej)** – jest to grzywna, której wysokość dla osoby fizycznej wynosi maksymalnie 10 000 PLN, a dla osoby prawnej oraz jednostki organizacyjnej nieposiadającej osobowości prawnej – 50 000 PLN; jest ona nakładana decyzją administracyjną Generalnego Inspektora w przypadku niewykonania przez Administratora danych osobowych decyzji Generalnego Inspektora, np. wezwania do zaprzestania przetwarzania danych osobowych[316].
2) **Karnej** – jest to grzywna, kara ograniczenia wolności lub pozbawienia wolności (od 1 roku do 3 lat) podmiotem właściwym do rozstrzygania w tym zakresie jest sąd oraz prokuratura[317]. Należy podkreślić, że przestępstwa wymienione w Ustawie ścigane są z urzędu[318].

Osoba przetwarzająca dane osobowe, a zwłaszcza ta, która administruje zbiorem (czyli Administrator Danych lub, jeśli został powołany, Administrator bezpieczeństwa informacji), odpowiada za:

- **przetwarzanie** danych na które nie uzyskała zgody (art. 49);
- **udostępnienie zbioru danych osobom nieuprawnionym**, czy to wewnątrz jednostki organizacyjnej, czy to podmiotowi zewnętrznemu (art. 49);
- **brak należytego zabezpieczenia zbioru danych osobowych** (np. trzymanie zbioru danych wrażliwych na dysku, do którego mają dostęp wszyscy pracownicy danej firmy (art. 52);
- **zaniechanie czynności rejestracji zbioru** u Generalnego Inspektora, o ile zarejestrowanie było konieczne (art. 53);
- **niedopełnienie obowiązku poinformowania osoby zainteresowanej o przysługujących jej prawach** (art. 54);
- **udaremnienie wykonania czynności kontrolnej** (art. 54 a);

Przestępstwa te zagrożone są **grzywną, karą ograniczenia wolności** albo **pozbawienia wolności** (w zależności od kwalifikacji przestępstwa od 1 roku do 3 lat).

Należy również pamiętać, że osoba, która uważa, że jej dane osobowe są przetwarzane w sposób niewłaściwy może **samodzielnie** na podstawie przepisów Kodeksu cywilnego dochodzić odpowiedzialności w postępowaniu **cywilnym**. Przewidziano następujące podstawy takiej odpowiedzialności:

1) **z tytułu naruszenia dóbr osobistych** – ten, kto naruszył czyjeś dobra osobiste (np. wykorzystał bez zgody wizerunek na stronie internetowej), jest zobowiązany **do naprawienia tego stanu** (np. usunięcia zamieszczonego wizerunku ze strony i przeproszenia za to co zrobił).
2) **z tytułu zadośćuczynienia pieniężnego** – uznaje się, że jeżeli Administrator danych osobowych lub Administrator bezpieczeństwa informacji nie dopełnili obowiązków zachowania danych osobowych w tajemnicy, to osoba, której te dane dotyczą, doznaje **niematerialnej krzywdy**; wówczas może się ona domagać zadośćuczynienia w formie finansowej.
3) z tytułu **wyrządzenia szkody** – uznaje się, że jeżeli w wyniku naruszenia przepisów z zakresu danych osobowych nastąpiła szkoda majątkowa, np. osoba ma prawo domagać się finansowego wyrównania szkody **odszkodowania pieniężnego.**

Studium przypadku:
nielegalne udostępnienie danych osobowych osoby chorej przewlekle sprawiło, że ubezpieczyciel zawczasu wypowiedział umowę i koszty leczenia osoba chora musiała ponieść sama.

Oprócz tego Kodeks pracy przewiduje **odpowiedzialność dyscyplinarną** – gdy naruszenie przepisów dotyczących ochrony danych osobowych nastąpiło przy okazji stosunku pracy (np. w sposób bezprawny udostępniono dane osobowe pracowników firmie marketingowej lub portalowi randkowemu). W tej sytuacji pracownicy mogą rozwiązać stosunek pracy bez wypowiedzenia na podstawie art. 55 § 11 Kodeksu pracy z powodu ciężkiego naruszenia obowiązków wobec pracownika.

---

316 Generalny Inspektor Ochrony Danych Osobowych, *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2014, s. 99 i n.*

317 Tak też orzekł Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 7.3.2007 r. o sygn. (II SA/WA 2260/06).

318 M. Bidziński, Odpowiedzialność za nieprawidłową ochronę danych osobowych, Informacja w administracji publicznej, nr 2, 2015.

8. PERSPEKTYWA ROZPORZĄDZENIA UNIJNEGO

mgr Bartosz Mendyk

Obecnie Komisja Europejska opracowuje kompleksową reformę przepisów o ochronie danych osobowych. Dwa podstawowe cele, które przyświecają Komisji, to wzmocnienie prawa do prywatności w internecie oraz nadanie impulsu gospodarce cyfrowej w Europie. Proponowane zmiany będą służyć również przedsiębiorcom.

Aktualnie trwają negocjacje pomiędzy Komisją Europejską, Radą Unii Europejskiej oraz Parlamentem. Obecny stan negocjacji jest na ukończeniu. Pod koniec 2016 roku jest planowane przyjęcie Rozporządzenia, które zastąpi obecną dyrektywę oraz w dużej mierze polską Ustawę. W Rozporządzeniu zostanie zastąpione prawo merytoryczne. Nie będzie natomiast zastępowane prawo proceduralne. W ustawie polskiej dalej będą uregulowane takie kwestie jak:

- kształt polskiego organu ochrony danych osobowych (Generalnego Inspektora),
- kształt procedur kontroli sądowej nad działaniami takiego organu,
- wyjątki uregulowane np. w prawie pracy lub na podstawie prawa prasowego.

Nowe przepisy będą opierać się na czterech podstawowych filarach:

1) **jeden kontynent – jedno prawo** ze skutecznymi sankcjami dla przedsiębiorców ze wszystkich 28 państw UE niezależnie od kraju pochodzenia przedsiębiorców;
2) **punkt kompleksowej usługi** (tzw. zasada *one stop shop*) – przedsiębiorstwa, które prowadzą działalność w kilku państwach UE oraz ich klienci będą mieli do czynienia z jednym krajowym organem nadzorczym;

Studium przypadku:
Przedsiębiorca zarejestrowany w Polsce i w niej prowadzący działalność gospodarczą pozyskał klientów w Niemczech. W związku z tym postanowił otworzyć tam dodatkowe biuro, w którym zbiera dane osobowe swoich kontrahentów. W obecnym stanie prawnym podlega on dwóm Generalnym Inspektorom, czyli polskiemu oraz niemieckiemu. Wejście w życie Rozporządzenia spowoduje, że **będzie** podlegać wyłącznie polskiemu.

3) **te same zasady** dla wszystkich przedsiębiorstw, niezależnie od miejsca ich siedziby – przedsiębiorstwa spoza Unii Europejskiej będą musiały przestrzegać europejskiego prawa ochrony danych, jeżeli będą prowadzić działalność gospodarczą na rynku europejskim; obecnie widać znaczącą dyskryminację przedsiębiorstw z Unii Europejskiej względem tych pochodzących spoza UE;
4) **prawo do bycia zapomnianym**, znane też jako prawo żądania usunięcia danych, które dopiero jest kształtowane.[319].

Najważniejszą korzyścią związaną z reformą ochrony danych osobowych będzie pobudzenie wzrostu gospodarczego poprzez redukcję kosztów i biurokracji dla europejskich przedsiębiorstw, w szczególności dla małych i średnich przedsiębiorstw (MŚP). Wynika to z tego, że Komisja Europejska zaproponowała zwolnienie MŚP z szeregu postanowień rozporządzenia o ochronie danych, podczas gdy obecnie obowiązująca Dyrektywa ma zastosowanie do wszystkich europejskich przedsiębiorstw niezależnie od ich wielkości.

Zgodnie z nowymi przepisami MŚP skorzystają z czterech ograniczeń biurokracji:

a) **zwolnienie z obowiązku powoływania osoby odpowiedzialnej za ochronę danych osobowych** (np. Administrator bezpieczeństwa informacji) jako osobnej funkcji; w Polsce powyższy obowiązek już został zniesiony, ale np. w Niemczech jest nadal (o ile przetwarza dane w sposób zautomatyzowany); rozporządzenie ujednolici ten stan prawny w całej Unii Europejskiej;
b) **brak konieczności dokonywania zgłoszeń zbiorów** danych do instytucji odpowiedzialnej za nadzór nad prawidłowym przetwarzaniem danych osobowych (Generalnego Inspektora);
c) **możliwość pobierania przez przedsiębiorców opłat za zapewnienie dostępu do danych osobowych**, ich poprawiania itd. w przypadku, gdy wnioski w tych sprawach będą powtarzały się zbyt często;
d) **MŚP nie będą miały obowiązku przeprowadzenia oceny wpływu na ochronę prywatności**.

[319] Sprawozdane Generalnego Inspektora Ochrony Danych Osobowych, *Sprawozdanie z działalności generalnego Inspektora Ochrony Danych Osobowych w roku 2014*, dostępny pod adresem: http://www.giodo.gov.pl/data/filemanager_pl/sprawozdaniaroczne/2014.pdf.

Zgodnie z nowym rozporządzeniem w podmiotach publicznych (np. urząd gminy, ministerstwo czy inny organ centralny), w przedsiębiorstwach zatrudniających więcej niż 250 stałych pracowników oraz w MŚP, których przetwarzanie danych osobowych jest podstawową działalnością gospodarczą (np. portal randkowy) zostanie **wprowadzony obowiązek** powołania **osoby odpowiedzialnej za ochronę danych osobowych (z ang. *data protecion officer*)**. Jego **zadania będą zbliżonego do tych, które w Polsce wykonuje Administrator bezpieczeństwa informacji** na podstawie przepisów obowiązujących od początku 2015 r. W przypadku pozostałych MŚP sytuacja **nie ulegnie** zmianie, czyli to Administrator danych osobowych zadecyduje, czy powoła osobę odpowiedzialną za przetwarzanie danych osobowych.

Doświadczenia ustawodawcze wskazały, że **sankcje karne** (np. kara pozbawienia wolności) nie przynoszą spodziewanego rezultatu . **Znacznie większą skuteczność nadają kary o charakterze administracyjnym tzn. finansowym**. Rozporządzenie Unii Europejskiej zawiera dosyć rozbudowany system tych kar. Zaczynają się one od ostrzeżeń na piśmie do kar w wysokości 1 mln EUR lub do 1% jego rocznego światowego obrotu. (Eurodeputowani żądają nawet 100 mln euro albo 5 proc. rocznych obrotów firmy.) Wysokość kar cały czas jest negocjowana i wzbudza duże dyskusje w Parlamencie Europejskim.

9. BIBLIOGRAFIA

1. Banaszak B.: *Konstytucja Rzeczpospolitej Polskiej. Komentarz*, 2. wydanie, Warszawa: C.H. Beck, 2012.
2. Banaszak B., Wygoda K.: *Pojęcie Funkcji Publicznej jako przesłanka modyfikująca zakres ochrony danych osobowych*, (w:) *Ochrona danych osobowych, wczoraj, dziś, jutro*, Warszawa: Wydawnictwo GIODO, 2006.
3. Barlow M.: *Real-Time Big Data Analytics: Emerging Architecture*, Sebastopol:. O'Reilly Media, 2013.
4. Barta J., Fajgielski P., Markiewicz R.: *Ochrona danych osobowych. Komentarz*, 5. wydanie, Warszawa: Wolters Kluwer Polska, 2011.
5. Barta P.: *Klauzula prawnie usprawiedliwionego celu w ustawie o ochronie danych osobowych*, (w:) Konarski X., Sibiga G. (red.): *Ochrona danych osobowych. Aktualne problemy i nowe wyzwania*, Warszawa: Wolters Kluwer Polska, 2007.
6. Barta P., Litwiński P.: *Ustawa o ochronie danych osobowych. Komentarz*, 3. wydanie, Warszawa: C.H. Beck, 2015.
7. Bidziński M.: *Odpowiedzialność za nieprawidłową ochronę danych osobowych*, „Informacja w administracji publicznej", nr 2, 2015.
8. Byczkowski M.: *Zarządzanie procesami przetwarzania danych osobowych*, (w:) Konarski X., Sibiga G. (red.): *Ochrona danych osobowych. Aktualne problemy i nowe wyzwania*, Warszawa: Wolters Kluwer Polska, 2007.
9. Byrski J., Konarski X.: *Wiążące reguły korporacyjne jako podstawa prawna przekazywania danych osobowych do państwa trzeciego*, (w:) A. Mednis (red.): *Prywatność a ekonomia. ochrona danych osobowych w obrocie gospodarczym*, Warszawa: Stowarzyszenie Absolwentów Wydziału Prawa i Administracji UW, 2013.
10. Czajka A., Pacut A.: *Biometria podpisu odręcznego,* (w:) P. Zając, S. Kwaśniowski (Red.), Automatyczna identyfikacja w systemach logistycznych, Warszawa: Oficyna Wydawnicza Politechnik i Wrocławskiej, 2004.
11. Czarnecki K.: *Ochrona danych osobowych w systemie Rady Europy na przykładzie Konwencji nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych*, (w:) Goździewicz G., Szabłowska M. (red.): *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów*, Toruń: Wydawnictwo „Dom Organizatora", 2008.
12. Drozd A.: *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Wydanie 3, Warszawa: LexisNexis, 2007.
13. Drozd A.: *Zabezpieczenie danych osobowych*, Wrocław: Presscom, 2008.
14. Fajgielski P.: *Obowiązki związane z zabezpieczeniem danych osobowych*, (w:) Fajgielski P. (red.): *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Lublin: Wydawnictwo KUL, 2008.
15. Fajgielski P.: *Udostępnianie danych osobowych – zagadnienia wybrane*, „Monitor Prawniczy" nr 7, 2012 – Dodatek.
16. Fajgielski P.: *Zasady ogólne przetwarzania i ochrony danych osobowych*, (w:) Goździewicz G., Szabłowska M. (red.): *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów*, Toruń: Wydawnictwo „Dom Organizatora", 2008.
17. Fischer B.: *Podział odpowiedzialności za chmurowe przetwarzanie danych osobowych z uwzględnieniem kształtowania regulacji umownych – wybrane zagadnienia*, „Monitor Prawniczy", nr 9, 2014 – Dodatek.
18. Fischer B.: *Ponadgraniczne przekazywanie danych osobowych – charakter prawny regulacji z uwzględnieniem uzupełniającej roli „soft law"*, (w:) A. Mednis (red.): *Prywatność a ekonomia. ochrona danych osobowych w obrocie gospodarczym*, Warszawa: Stowarzyszenie Absolwentów Wydziału Prawa i Administracji UW, 2013.
19. Gajda A.: *Ochrona danych osobowych i kierunki zmian w tej dziedzinie w prawie Unii Europejskiej*, „Kwartalnik Kolegium Ekonomiczno-Społecznego", nr 4, 2014.
20. Gałach A.: *Instrukcja ochrony danych osobowych w systemie informatycznym*, Gdańsk: Ośrodek Doradztwa i Doskonalenia Kadr, 2004.
21. Gersdorf M.: *Ochrona danych osobowych kandydata do pracy – problem stale dyskusyjny*, [w] *Ochrona danych osobowych, wczoraj, dziś, jutro*, Warszawa: Wydawnictwo GIODO, 2006.
22. Iwaszko B.: *Ochrona informacji niejawnych w praktyce*, Wrocław: Presscom, 2012.
23. Kaczmarek A. (opr.): *Wskazówki dotyczące sposobu opracowania instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji*, Warszawa: Biuro Generalnego Inspektora Ochrony Danych Osobowych, bdw. Dostępne pod adresem:http://www.giodo.gov.pl (10.11.2015).
24. Kaczmarek A. (opr.): *Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa*, Warszawa: Biuro Generalnego Inspektora Ochrony Danych Osobowych, bdw. Dostępne pod adresem: http://www.giodo.gov.pl, (10.11.2015);
25. Kaczmarek A.: *ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych*, Warszawa: GIODO, 2009.
26. Kaczorowski M.: *Przetwarzanie danych osobowych w działaniach marketingowych prowadzonych on-line*, „Monitor Prawniczy", nr 9, 2014
27. Kaszubski R. W.: *Biometria w bankowości i administracji publicznej,* Warszawa: Związek Banków Polskich, 2009.
28. Kawczyński P.: *Przetwarzanie danych w chmurze – cz. 1*, „Portal ODO", 10.06.2014. Dostęp pod adresem: https://www.portalodo.com/entry/przetwarzanie-danych-w-chmurze-cz-1, (20.11.2015).
29. Kawecki M.: *Generalny Inspektor Ochrony Danych Osobowych jako centralny organ administracji państwowej*, „Przegląd Prawa Technologii Informacyjnych. ICT Law Review", nr 1, 2013.

30. Kępa L.: *Dane osobowe w firmie. Praktyczny poradnik przedsiębiorcy*, Warszawa: Diffin, 2011.
31. Kister Ł., Gaśpierik M.: *Polityka kontroli dostępu do obiektów biurowych*, „Ochrona Mienia i Informacji", nr 2, 2012.
32. Kister Ł., Serafin T.: *Biometric Security Systems – Protection vs. Privacy*, (w:) *Riešenie krízových situácií v špecifickom prostredí*, Žilina: Žilinska univerzita, 2015.
33. Kister Ł.: *Audyt jako narzędzie oceny bezpieczeństwa informacji w organizacji*, (w:) Gajos M. (red.): *Ochrona informacji niejawnych, biznesowych i danych osobowych*, Katowice: KSOIN – UŚ, 2010.
34. Kister Ł.: *Bezpieczeństwo danych osobowych w systemach informatycznych*, „Ochrona Mienia i Informacji", nr 5, 2009.
35. Kister Ł.: *Ochrona danych osobowych – funkcjonalność systemu informatycznego*, „Ochrona Mienia i Informacji", nr 4, 2009.
36. Kister Ł.: *Ochrona danych osobowych – zabezpieczenia organizacyjno-techniczne. Część II*, „Ochrona Mienia i Informacji", nr 3, 2009.
37. Kister Ł.: *Polityka bezpieczeństwa danych osobowych*, „Ochrona Mienia i Informacji", nr 6, 2009.
38. Kister Ł.: *Prawne aspekty dopuszczalności monitoringu wizyjnego – ochrona wizerunku osób*, „Ochrona Mienia i Informacji", nr 6, 2010
39. Kister Ł.: *Proces rekrutacji jako czynnik bezpieczeństwa informacyjnego organizacji*, „Ochrona mienia i informacji", nr 3, 2010.
40. Kister Ł.: *Wikiekcja dla biznesu*, „Bussines Security Magazine", nr 1, 2011.
41. Kister Ł.: *Zabezpieczenia „Data Center" – Wymagania prawa i praktyki*, (w:) *Praktyczne aspekty funkcjonowania serwerowni. Centra przetwarzania danych – dostosowanie do potrzeb organizacji*, Warszawa: Centrum Promocji Informatyki, 2011.
42. Konarski X.: *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa: Difin, 2004.
43. Kopff A.: *Koncepcja praw do intymności i do prywatności życia osobistego*, „Studia Cywilistyczne", t. XX, 1972.
44. Kowalik P.: *Kontrola GIODO w jednostce – praktyczne porady,* „Informacja w administracji publicznej", nr 3, 2015.
45. Kral P.: *Wzorcowa dokumentacja ochrony danych osobowych z komentarzem*, Gdańsk: Ośrodek Doradztwa i Doskonalenia Kadr, 2007.
46. Krasuski A., Skolimowska D.: *Dane osobowe w przedsiębiorstwie*, Warszawa: Lexis Nexis, 2007.
47. Krzysztofek M.: *„Prawo do bycia zapomnianym" i inne aspekty prywatności w epoce Internetu w prawie UE*, „Europejski Przegląd Sądowy" nr 8, 2012.
48. Krzysztofek M.: *Tajemnica bankowa i ochrona danych osobowych w praktyce bankowej*, Warszawa: LexisNexis, 2010.
49. Kuczyński T.: *Ochrona danych osobowych w stosunku zatrudnienia*, „Przegląd sądowy", nr 11-12, 1998.
50. Kulesza E.: *Ochrona Danych osobowych w pomocy społecznej*, Warszawa: Centrum Rozwoju Zasobów Ludzkich, 2013.
51. Lewiński A.: *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów. 10-lecie polskiej Ustawy o ochronie danych osobowych*, (w:) Goździewicz G., Szabłowska M. (red.): *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów*, Toruń: Wydawnictwo „Dom Organizatora", 2008.
52. Lipowicz I.: *Konstytucyjne podstawy ochrony danych osobowych*, (w:) Fajgielski P. (red.): *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Lublin: Wydawnictwo KUL, 2008.
53. Litwiński P.: *Monitoring pracownika w miejscu pracy a ochrona danych osobowych pracownika*, „Monitor Prawa Pracy", nr 2, 2008.
54. Łuczejko K.: D*ane osobowe w internecie – wybrane zagadnienia administracyjnoprawne*, „Acta Iursi Stetinensis", nr 5, 2014.
55. Maj M.: *GIODO: Przetwarzanie danych osobowych w chmurach jest dopuszczalne, ale .... Rozmowa z dr Wojciechem R. Wiewiórowskim – Generalnym Inspektorem Ochrony Danych Osobowych*, „Dziennik Internautów", 24.05.2011. Dostęp pod adresem: http://di.com.pl/giodo-przetwarzanie-danych-osobowych-w-chmurach-jest-dopuszczalne-ale-38127, (10.11.2015).
56. Mayer-Schonberger V., Cukier K.: *Big Data. Rewolucja, która zmieni nasze myślenie, pracę i życie*, Warszawa: MT Biznes, 2014.
57. Mączyński A.: *Uznanie nazwiska w świetle konwencji nr 31 Międzynarodowej Komisji Stanu Cywilnego z 2005*, (w:) Ochrona danych osobowych, wczoraj, dziś, jutro, Warszawa: Wydawnictwo GIODO, 2006.
58. Mednis A.: *Obowiązki podmiotów prywatnych wykorzystujących dane osobowe*, „Monitor Prawniczy", nr 8, 1998.
59. Mednis A.: *Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej*, „Ochrona Danych Osobowych", nr 1, 2000.
60. Mednis A.: *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa: Wydawnictwo Prawnicze, 1999.
61. Michalik Ł.: *Odcisk palca zamiast PIN-u. MasterCard testuje biometryczne karty płatnicze,* Portal „Gadżetomania". Dostępny: http://gadzetomania.pl/2034,odcisk-palca-zamiast-pin-u-mastercard-testuje-biometryczne-karty-platnicze, (09.12.2015).
62. Mitnick K., W. Simon: *Sztuka podstępu. Łamałem ludzi nie hasła*, Gliwice: Helion, 2003.
63. Niklas J., *Prywatność w internecie,* Warszawa: Biuro Analiz Sejmowych, nr 13, 2014.
64. Nowińska E., du Vall M.: *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz*, Wydanie 5, Warszawa: LexisNexis, 2010.
65. Oniszczuk J.: *Konstytucja Rzeczpospolitej Polskiej w orzecznictwie Trybunału Konstytucyjnego*, Kraków: ABC, 2000.

66. Ossowska-Salamonowicz D.:, *Ochrona danych osobowych w działalności dziennikarskiej*, Olsztyn: Wydawnictwo Uniwersytetu Warmińsko-Mazurskiego, 2015.
67. Ossowski M. (red.): *Prawo w email marketingu*, Warszawa: GetResponse, 2013.
68. Pacut A., Czajka A., Putz-Leszczyńska J., Stasiak Ł., Wardziński R.: *Metody Biometrii*, „Biuletyn NASK", nr 3, 2006.
69. Pawlik K.: *Lista Robinsona jako instrument ochrony danych osobowych*, (w:) Goździewicz G., Szabłowska M. (red.): *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów*, Toruń: Wydawnictwo „Dom Organizatora", 2008.
70. Polok M.: *Bezpieczeństwo danych osobowych*, Warszawa: C.H. Beck, 2008.
71. Pilc B.: *Rola administratora bezpieczeństwa informacji podczas inspekcji prowadzonej przez Generalnego Inspektora Ochrony Danych Osobowych*, „Monitor Prawniczy", nr 7, 2012 – Dodatek.
72. Posiadła A., Winiecka S.: *Ochrona danych osobowych w świetle wybranych orzeczeń Europejskiego Trybunału Praw Człowieka*, (w:) Goździewicz G., Szabłowska M. (red.): *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów*, Toruń: Wydawnictwo „Dom Organizatora", 2008.
73. Przywora B.: *O potrzebie wzmocnienia kompetencji Generalnego Inspektora Ochrony Danych Osobowych w zakresie bezpieczeństwa państwa,* Program Narodowego Centrum Badań i Rozwoju. Dostępny m. in. pod adresem http://mrj.uksw.edu.pl/sites/default/files/Repozytorium/Prezentacje/Zadania_i_kompetencje_organow_publicznych_w_zakresie_jawnosci_i_jej_ograniczen/dr_boguslaw_przywora.pdf, (09.12.2015).
74. Przywora B.: *Z problematyki kontroli przetwarzania i ochrony danych osobowych przez Generalnego Inspektora Ochrony Danych Osobowych, (w:)* Szmulik B., Szpor G. (red.): *Jawność i jej ograniczenia. Zadania i kompetencje*, Warszawa: CH. Beck, 2015.
75. Sadlik R.: *Zakaz konkurencji jako sposób ochrony interesów pracodawcy*, Warszawa: Difin, 2007.
76. Sadło K.: *Ochrona danych osobowych w organizacjach pozarządowych*, Warszawa: Wydawnictwo Fundacja Rozwoju Społeczeństwa Obywatelskiego, 2013.
77. Sakowska M., Młynarska-Sobaczewska A.: *„Klauzula prasowa" z ustawy o ochronie danych osobowych*, „Państwo i Prawo", nr 1, 2005.
78. Sibiga G.: *Ochrona informacji niejawnych i ochrona danych osobowych. Wybrane zagadnienia wzajemnych relacji*, (w:) Gajos M. (red. nauk.): *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały V Kongresu*, Katowice: KSOIN, 2009.
79. Sibiga G.: *Postępowanie w sprawach ochrony danych osobowych*, Warszawa : Dom Wydawniczy ABC 2003
80. Sibiga G.: *Zakres stosowania ustawy o ochronie danych osobowych do przetwarzania danych pracowników i osób ubiegających się o zatrudnienie*, „Monitor Prawa Pracy", nr 3, 2012.
81. Szustakiewicz P.: *Kontrole Generalnego Inspektora Ochrony Danych Osobowych*, „Kontrola Państwowa", nr 6, 2007.
82. Szymorek K.: *Aspekty prawne kontrolowania pracowników za pomocą technologii identyfikacji radiowej (RFID)* „Monitor Prawa Pracy", nr 10, 2012.
83. Śleszyńska E.: *Administrowanie danymi osobowymi przez zarządców i właścicieli nieruchomości*, Chotomów: MINI GO, 2009.
84. Tadeusiewicz R., Izworski A., Majewski J.: *Biometria,* Kraków: Akademia Górniczo Hutnicza, 1993.
85. Urbanowicz J. A.: *Pięć lat paszportów biometrycznych*, „Gazeta.pl", http://technologie.gazeta.pl/internet/2029020,04665,10186491,Piec_lat_paszportow_biometrycznych__UZUPELNIENIE_.html, (09.12.2015).
86. Walczak K.: *Ochrona danych osobowych kandydata do pracy w trakcie rekrutacji*, (w:) Wyka T., Nerka A. (red.): *Ochrona danych osobowych podmiotów objętych prawem pracy i prawem ubezpieczeń społecznych. Stan obecny i perspektywy zmian*, Warszawa: Wolters Kluwer Polska, 2012.
87. Wiewiórowski W.: *Nowe ramy ochrony danych osobowych w Unii Europejskiej,* dodatek „Monitor Prawniczy" nr 7, 2012.
88. Wiewiórowski W.: *Prawna ochrona danych biometrycznych w systemach teleinformatycznych pracodawcy. Cele przetwarzania, a zakres ochrony*, (w:) Wyka T., Nerka A. (red.): *Ochrona danych osobowych podmiotów objętych prawem pracy i prawem ubezpieczeń społecznych. Stan obecny i perspektywy zmian*, Warszawa: Wolters Kluwer Polska, 2012.
89. Wołyniec A.: *Granice uprawnienia pracodawcy do zbierania danych osobowych*, „Radca Prawny", nr 3, 2015.
90. Wyskwarski M.: *Przetwarzanie w chmurze z punktu widzenia małych przedsiębiorstw*, „Zeszyty naukowe Politechniki Śląskiej – Organizacja i Zarządzanie" nr 74, 2014.
91. Zegarek P.: *Czy program „Safe Harbor" faktycznie trafił do kosza? Jak jest naprawdę?,* http://blog-daneosobowe.pl/czy-program-safe-harbor-faktycznie-trafil-do-kosza-jak-jest-naprawde/, (09.12.2015).
92. Zgajewski M.: *Cloud Computing w sektorze finansowych*, Warszawa: Forum Technologii Bankowych Związku Banków Polskich, 2013.

Odsyłacze do aktów prawnych, wyroków, uchwał, decyzji, opinii, sprawozdań, norm technicznych i innych materiałów nie będących publikacjami zwartymi zostały umieszczone wyłącznie w przypisach dolnych.

Recenzja publikacji pt. „Ochrona danych osobowych w przedsiębiorstwie – poradnik dla MŚP" autorstwa dr Łukasza Kistera i mgr Bartosza Mendyka

Tematyka szeroko pojmowanej ochrony prywatności, a w ujęciu wąskim – tematyka ochrony danych osobowych – nabrała w ostatnich latach bardzo istotnego znaczenia. Z jednej strony, rozwój nowoczesnych, zautomatyzowanych technik przetwarzania danych osobowych otwiera przed przedsiębiorcami nieznane dotąd możliwości analizy danych osobowych; nie bez przyczyny pojęcie „big data" jest dzisiaj tak popularne wśród osób zajmujących się ochroną danych osobowych. Z drugiej strony, minione lata to także stały wzrost zagrożeń dla bezpieczeństwa danych osobowych i innych informacji przetwarzanych przez przedsiębiorców; wycieki danych osobowych i włamania do systemów teleinformatycznych, także tych uchodzących dotąd za bezpieczne, stają się coraz częstsze.

Zjawiskom tym towarzyszy, w sposób naturalny, rozwój regulacji prawnych z zakresu prawa ochrony danych osobowych: prócz uchwalonej w 1997 r. ustawy o ochronie danych osobowych uchwalane są regulacje sektorowe, określające zasady ochrony danych osobowych w konkretnych sektorach gospodarki. Zmieniana jest również sama ustawa o ochronie danych osobowych – od czasu swojego uchwalenia w 1997 r., ustawa była nowelizowana 20 razy; zmieniają się również rozporządzenia wykonawcze do ustawy. Co istotne, poszczególne zmiany układają się pewien schemat, według którego ewoluuje filozofia ochrony danych osobowych: stopniowo ograniczane są bowiem obowiązki czysto administracyjne, takie jak rejestracja zbiorów danych osobowych, na rzecz nakładania obowiązków organizacyjnych i technicznych bezpośrednio na przedsiębiorców przetwarzających dane osobowe. Tendencja ta osiągnie apogeum w projektowanym rozporządzeniu Parlamentu Europejskiego i Rady w sprawie ochrony danych osobowych, które w niedalekiej przyszłości zastąpi dyrektywę o ochronie danych osobowych oraz polską ustawę – na gruncie nowych przepisów, stosowanie rozwiązań ***privacy by design*** (uwzględnianie postulatu ochrony prywatności już na etapie projektowania poszczególnych rozwiązań) oraz ***risk based approach*** (podejście oparte na ryzyku) stanie się prawnym obowiązkiem przedsiębiorców przetwarzających dane osobowe.

Przedsiębiorcy przetwarzający dane osobowe – a pamiętajmy, że wystarczy zatrudnienie jednego pracownika, by mówić o przetwarzaniu danych osobowych, o danych klientów, czy danych pochodzących z faktur, nie wspominając – od dłuższego czasu muszą więc zmagać się ze stałym wzrostem ilości regulacji prawnych, które ich dotyczą; nakłada się na to, nieraz sprzeczne, orzecznictwo Generalnego Inspektora Ochrony Danych Osobowych i sądów. Stąd nie można nie docenić wartości, jaką niesie ze sobą recenzowana publikacja. Jest to praktyczny, napisany przez praktyków i dla praktyków, Poradnik stanowiący rodzaj przewodnika po stosowaniu przepisów o ochronie danych osobowych.

Poradnik został podzielony na rozdziały, tematyką odpowiadające najważniejszym zagadnieniom prawnym, technicznym i organizacyjnym powstającym przy stosowaniu ustawy o ochronie danych osobowych niektórych przepisów sektorowych z zakresu ochrony danych osobowych. Począwszy od syntetycznego przedstawienia systemu prawa ochrony danych osobowych w Unii Europejskiej i w Polsce, poprzez szczegółowe omówienie poszczególnych obowiązków ciążących na przedsiębiorcach, aż po perspektywę reformy europejskiego prawa ochrony danych osobowych, Autorzy omawiają najważniejsze dla przedsiębiorców obowiązki związane ze stosowaniem przepisów. Publikacja została opracowana w sposób bardzo szczegółowy, z uwzględnieniem najnowszego orzecznictwa sądów polskich i europejskich, a także z przywołaniem stanowisk nauki prawa. Jednocześnie język używany w Poradniku, a także sposób przedstawiania nierzadko skomplikowanych prawnie zagadnień sprawia, że przedsiębiorcy nie powinni mieć praktycznych trudności ze stosowaniem rozwiązań proponowanych przez Autorów, także samodzielnie, bez korzystania z wsparcia prawnego. Niewątpliwą wartość publikacji stanowią również (bardzo liczne i przygotowanie w niezwykle kreatywny sposób) praktyczne przykłady zastosowania przepisów o ochronie danych osobowych w formie tzw. studiów przypadku – pozwalają lepiej zrozumieć tą niewątpliwie skomplikowaną materię.

Poradnik, który miałem przyjemność przeczytać i zrecenzować, stanowi ogromną wartość na polskim rynku wydawniczym – dotychczas bowiem nie było na nim pozycji omawiającej prawne, techniczne i organizacyjne aspekty ochrony danych osobowych, która od początku do końca skierowana byłaby do przedsiębiorców i która dawałaby im praktyczne narzędzie rozwiązywania problemów, przed którymi stają na co dzień. Z tym większym zadowoleniem należy przywitać inicjatywę Autorów i Wydawcy. Sam Poradnik natomiast powinien stać się obowiązkową lekturą każdego przedsiębiorcy, który zamierza przestrzegać obowiązujących przepisów w zakresie ochrony danych osobowych.

dr Paweł Litwiński, adwokat,
członek sekcji własności intelektualnej Instytutu Allerhanda

dr Łukasz KISTER

Niezależny ekspert bezpieczeństwa informacji. Doktor nauk o bezpieczeństwie, w specjalizacji zarządzanie bezpieczeństwem. Biegły sądowy przy Sądzie Okręgowym w Warszawie, z zakresu ochrony danych osobowych. Projektant i audytor systemów bezpieczeństwa danych osobowych. Aktywny Administrator bezpieczeństwa informacji.

Wdrożył systemy zarządzania bezpieczeństwem danych osobowych – lub był ich kluczowym konsultantem, w takich instytucjach i przedsiębiorstwach, jak: Ministerstwo Sprawiedliwości, Narodowy Instytut Audiowizualny, Państwowe Muzeum Auschwitz-Birkenau w Oświęcimiu, Krajowy Ośrodek Mieszkalno-Rehabilitacyjny dla Osób Chorych na SM, Louvre Hotels, Hewitt, Oticon Polska, Flextronics Logistics Poland, Impaq i wielu innych.

Realizował projekty edukacyjne z zakresu prawa do prywatności we współpracy z Generalnym Inspektorem Ochrony Danych Osobowych, Biurem Informacyjnym Parlamentu Europejskiego w Polsce, Fundacją Panoptykon, Polską Izbą Systemów Alarmowych oraz Instytutem Jagiellońskim.

Opublikował kilkadziesiąt prac dotyczących różnorodnych aspektów bezpieczeństwa informacji, w językach: polskim, słowackim, ukraińskim i angielskim.

Redaktor naczelny czasopisma naukowego „Securitologia", Członek Rady Naukowej rocznika naukowego „Studia nad Bezpieczeństwem", redaktor merytoryczny ds. bezpieczeństwa informacji czasopisma specjalistycznego „Ochrona Mienia i Informacji".

www.bezpiecznenformacje.pl.

mgr Bartosz Mendyk

Doktorant nauk prawnych, prawnik, szkoleniowiec w licznych instytucjach samorządowych, autor publikacji książkowych oraz publicystycznych i naukowych w takich czasopismach jak Dziennik Gazeta Prawna oraz Biuletyn Euro Info. Prace zostały opublikowane w prasie polskiej, ukraińskiej, rosyjskiej, kazachskiej, azerbejdżańskiej i białoruskiej.

Polska Agencja Rozwoju Przedsiębiorczości (PARP) jest agencją rządową, która od 15 lat wspiera rozwój przedsiębiorczości w Polsce. Celem działania PARP jest rozwój małych i średnich firm – powstawanie nowych podmiotów, podnoszenie kwalifikacji i wzrost potencjału, wzmocnienie pozycji konkurencyjnej w oparciu o innowacyjność i nowoczesne technologie, kształtowanie przyjaznego otoczenia biznesowego, tworzenie warunków do prowadzenia działalności gospodarczej. Realizując działania wspierające przedsiębiorców (a także: instytucje otoczenia biznesu, jednostki samorządu terytorialnego, państwowe jednostki budżetowe, uczelnie), PARP korzysta ze środków budżetu państwa oraz funduszy europejskich. Zarówno w okresie przedakcesyjnym, jak i po wejściu przez Polskę do Unii Europejskiej, PARP oferowała przedsiębiorcom wsparcie finansowe, szkoleniowo-doradcze i informacyjne. Do 2015 r. Agencja jest odpowiedzialna za realizację działań w ramach trzech programów operacyjnych: **Innowacyjna Gospodarka**, **Kapitał Ludzki** oraz **Rozwój Polski** Wschodniej, a od 2015 r. dodatkowo programów perspektywy 2014–2020: **Inteligentny Rozwój**, **Polska Wschodnia** oraz **Wiedza, Edukacja i Rozwój**.

PARP posiada doświadczenie nie tylko w przekazywaniu unijnej pomocy przedsiębiorcom. Od kilku lat w Agencji działa **Ośrodek Badań nad Przedsiębiorczością**, którego zadaniem jest prowadzenie badań z zakresu przedsiębiorczości, innowacyjności, zasobów ludzkich i usług wspierających prowadzenie działalności gospodarczej. W oparciu o ich wyniki powstają założenia dla kolejnych programów pomocowych, które odpowiadają na zidentyfikowane potrzeby przedsiębiorców. Od 2013 r. PARP realizuje projekt pilotażowy służący analizie wpływu projektowanych i istniejących regulacji na sektor małych i średnich przedsiębiorstw (MSP).

Aby pomoc była skuteczna, przedsiębiorca musi mieć łatwy dostęp do informacji na jej temat. PARP zainicjowała utworzenie **Krajowego Systemu Usług dla MSP** (KSU). KSU oferuje doradztwo dla firm na każdym etapie prowadzenia działalności: od rejestracji działalności, poprzez sprawne prowadzenie i zarządzanie firmą, aż po zawieszenie lub zakończenie działalności. Wszystkie ośrodki KSU (około 200) działają na podstawie wypracowanych Standardów Usług, dzięki czemu przedsiębiorca może być pewien, że otrzyma usługę najwyższej jakości.

Działający przy PARP ośrodek sieci **Enterprise Europe Network** daje szansę przedsiębiorcom na skorzystanie z możliwości rynku ogólnoeuropejskiego. Ośrodek oferuje nieodpłatne kompleksowe usługi obejmujące informacje, szkolenia i doradztwo, przede wszystkim z zakresu prawa i polityki Unii Europejskiej, prowadzenia działalności gospodarczej w Polsce i za granicą, dostępu do źródeł finansowania, internacjonalizacji przedsiębiorstw, transferu technologii oraz udziału w programach ramowych UE. Ponadto, sieć Enterprise Europe Network pomaga przedsiębiorcom w znalezieniu partnerów zagranicznych oraz w organizacji ich udziału w targach i misjach gospodarczych.

PARP systematycznie dopasowuje ofertę informacyjno-doradczą do zmieniających się potrzeb przedsiębiorców oraz pojawiających się nowych kanałów komunikacji. Obecnie Agencja dysponuje kilkunastoma specjalistycznymi portalami internetowymi i społecznościowymi, oferującymi szkolenia e-learningowe, e-booki, transmisje ze spotkań szkoleniowych i konferencji, informacje na temat możliwości ubiegania się o wsparcie, bazy wiedzy, publikacje, wyniki badań. Z informacji i narzędzi zawartych we wszystkich portalach PARP, dostępnych za pośrednictwem głównego portalu Agencji www.parp.gov.pl, korzysta blisko milion internautów miesięcznie.

Osoby zainteresowane uzyskaniem informacji na temat programów wsparcia oferowanych przez PARP dla przedsiębiorców oraz instytucji otoczenia biznesu, mogą skorzystać z infolinii prowadzonej w ramach **Informatorium** PARP.

Zapraszamy do skorzystania z naszych usług!

Polska Agencja Rozwoju Przedsiębiorczości
ul. Pańska 81/83; 00-834 Warszawa
tel.: +48 22 432 80 80 fax: +48 22 432 86 20
www.parp.gov.pl e-mail: biuro@parp.gov.pl

Infolinia dla przedsiębiorców:
tel.: + 48 22 432 89 91
tel.: + 48 22 432 89 92
tel.: + 48 22 432 89 93
e-mail: info@parp.gov.pl

enterprise europe network

Wsparcie dla biznesu w zasięgu ręki

Usługi Enterprise Europe Network

Sieć Enterprise Europe Network funkcjonuje od 1 stycznia 2008 r. Obecnie jej działania są współfinansowane przez Komisję Europejską ze środków pochodzących z programu COSME na lata 2014-2020 oraz ze środków budżetu państwa w ramach programu wieloletniego pod nazwą „Udział Polski w programie na rzecz konkurencyjności przedsiębiorstw oraz małych i średnich przedsiębiorstw (COSME) oraz w instrumentach finansowych programów UE wspierających konkurencyjność przedsiębiorstw w latach 2015-2021".

Enterprise Europe Network oferuje małym i średnim przedsiębiorstwom kompleksowe usługi, które mają im pomóc w pełni rozwinąć ich potencjał i zdolności innowacyjne. Sieć jest także pośrednikiem umożliwiającym instytucjom Unii Europejskiej pełniejszą orientację w potrzebach małych i średnich przedsiębiorstw.

Ośrodki Enterprise Europe Network są afiliowane przy rozmaitych organizacjach wspierających rozwój gospodarczy, takich jak izby przemysłowo-handlowe, agencje rozwoju regionalnego, centra wspierania przedsiębiorczości, itp. Działają na zasadzie non-profit. Finansowanie Enterprise Europe Network pochodzi ze środków unijnych oraz ze środków budżetu państwa.

Obecnie działa blisko 600 ośrodków w Europie, na Bliskim Wschodzie, w Azji i w Ameryce. Enterprise Europe Network to więcej niż pojedyncze ośrodki rozmieszczone w różnych krajach i regionach. Wyjątkowa wartość i możliwości sieci wynikają ze ścisłej współpracy ośrodków. Wszystkie biura mogą komunikować ze sobą, co zapewnia szybkie przekazywanie i uzyskiwanie dokładnych informacji, a także mają dostęp do wspólnych baz zawierających profile firm szukających partnerów zagranicznych.

Działalność ośrodków Enterprise Europe Network opiera się na zasadzie „zawsze właściwych drzwi". Oznacza to, że wszyscy przedsiębiorcy z sektora MSP, którzy zwrócą się z konkretnym zapytaniem, otrzymają niezbędne informacje i dostęp do zindywidualizowanych usług dostosowanych do ich potrzeb, przy wykorzystaniu nowoczesnych technologii i zaangażowaniu adekwatnych merytorycznie ośrodków sieci.

Działania sieci umożliwiają przedsiębiorcom korzystanie z możliwości rynku ogólnoeuropejskiego, oferując nieodpłatne, kompleksowe usługi obejmujące informacje, szkolenia i doradztwo, przede wszystkim z zakresu prawa i polityk Unii Europejskiej, prowadzenia działalności gospodarczej w Polsce i za granicą, dostępu do źródeł finansowania, internacjonalizacji przedsiębiorstw, transferu technologii oraz udziału w programach ramowych UE.

Ośrodek Enterprise Europe Network
Polska Agencja Rozwoju Przedsiębiorczości
ul. Pańska 81/83
00-834 Warszawa

e-mail: coordinator_cpbsn@parp.gov.pl
www.een.org.pl
tel. + 48 22 432 71 02, faks + 48 22 432 70 46
czynny w godz. 9:00–16:00

ISBN 978-83-7633-369-4