Polityka Ochrony Danych Osobowych

RODO

w Spółdzielni Mieszkaniowej Lokatorsko – Własnościowej w Raciążu

zwanej dalej SMLW

MAJ 2018r.

Spis treści

Rozdział 1. Postanowienia ogólne

§ 1

1. „Polityka ochrony danych”, zwana dalej „Polityką”, jest zintegrowanym zbiorem zasad, procedur, praw wewnętrznych, opracowanych przy uwzględnieniu praktycznych doświadczeń regulujących sposób zarządzania, ochrony, użytkowania, przetwarzania i przechowywania danych osobowych gromadzonych przez Administratora zarówno w postaci elektronicznej, jak i w postaci dokumentów w wersji papierowej.
2. Uzupełnieniem niniejszej Polityki jest System Zarządzania Bezpieczeństwem Informacji zawierający wytyczne dotyczące bezpiecznego przetwarzania danych przy użyciu systemów informatycznych.
3. Polityka ma charakter obligatoryjny – dotyczy wszystkich pracowników. Pracownik zobowiązany jest do zapoznania się z Polityką przed dopuszczeniem do pracy w SMLW.
4. SMLW realizując postanowienia niniejszej Polityki, dokłada najwyższej staranności w celu ochrony praw i wolności osób, których dane dotyczą, a w szczególności zapewnia:
   1) przetwarzanie danych zgodnie z prawem, rzetelnie i w sposób przejrzysty;
   2) zbieranie danych wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzanie ich dalej w sposób niezgodny z tymi celami, dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami;
   3) minimalizację danych, poprzez przetwarzanie danych adekwatnych, stosownych oraz ograniczonych do niezbędnych celów przetwarzania;
   4) realizację zasady, zgodnie z którą dane powinny być prawidłowe i w razie potrzeby uaktualniane oraz podejmowanie wszelkich rozsądnych działań, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
   5) przechowywanie danych w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne;

6) integralność i poufność danych poprzez odpowiednie zapewnienie bezpieczeństwa, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych i organizacyjnych;
7) realizację zasady rozliczalności poprzez wdrożenie odpowiednich procedur i zasad, pozwalających na wykazanie przestrzegania przepisów Rozporządzenia, ze szczególnym uwzględnieniem udziału w tych działaniach inspektora ochrony danych.

5. Politykę opracowano w oparciu o:
   1) art. 47 i 51 Konstytucji Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997r.;
   2) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych);
   3) Ustawę z dnia 26 czerwca 1974r. Kodeks pracy.
6. Politykę stosuje się:
   1) do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania danych w sposób inny niż zautomatyzowany, danych osobowych stanowiących część zbioru lub mających stanowić część zbioru danych;
   2) w celu dopasowania obowiązków do wymogów odnoszących się do ryzyka naruszenia praw i wolności osób fizycznych;
   3) w celu ograniczania ryzyka naruszenia praw i wolności osób fizycznych, jakie może nieść przetwarzanie danych osobowych, poprzez zabezpieczenie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz ich zmianą, utratą, uszkodzeniem lub zniszczeniem.
7. Użyte w Polityce określenia oznaczają:
   1) Rozporządzenie lub RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
   2) IOD – Inspektor Ochrony Danych;

3) administrator lub SMLW – **Spółdzielnia Mieszkaniowa Lokatorsko – Własnościowa w Raciążu;**
4) czynności statutowe – czynności określone w statucie Administratora;
5) dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
6) zbiór danych – uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest scentralizowany czy rozproszony funkcjonalnie lub geograficznie;
7) organ nadzorczy – Prezes Urzędu Ochrony Danych Osobowych;
8) identyfikator – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę w systemie informatycznym;
9) odbiorca danych – osoba fizyczna, lub prawna, organ publiczny lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane w ramach konkretnego postępowania nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosowne do celów przetwarzania;
10) ryzyko – pojęcie odnoszące się do oceny prawdopodobieństwa wystąpienia i wadze zagrożenia naruszenia praw i wolności osób fizycznych;
11) powierzenie przetwarzania danych – zlecenie przetwarzania danych osobowych podmiotowi przetwarzającemu (procesorowi) w drodze umowy zawartej na piśmie;
12) podmiot przetwarzający (procesor) – osoba fizyczna lub prawna, jednostka lub inny podmiot, która przetwarza dane osobowe w imieniu Administratora;
13) pracownik w rozumieniu Polityki:
    a) każda osoba zatrudniona w SMLW na podstawie umowy o pracę lub umowy cywilnoprawnej, w tym praktykanci i stażyści,
    b) członek władz SMLW;

14) przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
15) sprawdzenie zgodności – czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
16) system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
17) tajemnica firmowa – wszystkie informacje dotyczące czynności SMLW, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której SMLW tę czynność wykonuje;
18) ograniczenie przetwarzania – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
19) profilowanie – dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
20) pseudonimizacja – przetworzenie danych osobowych w taki sposób, by nie można ich już było przypisać konkretnej osobie, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje przechowywane są osobno i objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie;
21) zgoda osoby, której dane dotyczą – dobrowolne, konkretne, świadome i jednoznaczne wyrażenie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie;

22) naruszenie ochrony danych osobowych – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
23) strona trzecia – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, Administrator, podmiot przetwarzający czy osoby, które z upoważnienia Administratora lub podmiotu przetwarzającego mogą przetwarzać dane osobowe.

8. Niniejsza Polityka została opracowana w celu stworzenia i utrzymania wysokiego poziomu bezpieczeństwa zbiorów danych osobowych zgodnie z wymogami Rozporządzenia rozumianego jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań.
9. Ze względu na zmieniający się charakter zagrożeń, a także pojawianie się nowych, Administrator traktuje zabezpieczenie danych osobowych nie jako stan, ale jako proces wymagający ciągłego doskonalenia, modyfikowania dostosowywania rozwiązań technicznych i organizacyjnych do możliwości pojawienia się nowych kategorii niebezpieczeństw i zagrożeń.

Rozdział 2. Osoby odpowiedzialne

§ 2

1. Do zadań Administratora należy m.in.:
   1) zapewnianie odpowiednich środków technicznych i organizacyjnych gwarantujących ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów ochrony danych osobowych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem i zapewnia rozliczalność tych działań;
   2) wdrożenie polityki ochrony danych, w tym w szczególności regulacji z zakresu bezpieczeństwa informacji, zarządzania ryzykiem, ochrony danych osobowych;
   3) wydawanie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.

2. W SMLW przed rozpoczęciem przetwarzania danych osobowych przeprowadza się analizę ryzyka, a w przypadku możliwości wystąpienia wysokiego ryzyka naruszenia praw i wolności osób fizycznych także ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych.
3. W SMLW wdraża się takie rozwiązania techniczne i organizacyjne aby zapewnić realizację zasady ochrony danych w fazie projektowania.
4. W SMLW wdraża się takie rozwiązania techniczne i organizacyjne aby zapewnić realizację zasady domyślnej ochrony danych.
5. Administrator podejmując współpracę z innym administratorem wspólnie ustala cel i sposoby przetwarzania, a w szczególności podejmuje uzgodnienia w formie pisemnej, określając zakresy odpowiedzialności, obowiązki oraz punkt kontaktowy dla osób, których dane dotyczą.
6. Administrator wyznacza IOD i włącza go we wszystkie sprawy dotyczące ochrony danych osobowych zapewniając mu niezależność w wykonywaniu zadań i niezbędne do tego zasoby.

§ 3

1. Do podstawowych zadań IOD należy:
   1) informowanie Administratora oraz pracowników, w szczególności pracowników przetwarzających dane osobowe, o spoczywających na nich obowiązkach;
   2) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
   3) współpraca z organem nadzorczym;
   4) pełnienie funkcji punktu kontaktowego dla organu nadzorczego oraz osób, których dane dotyczą;
   5) monitorowanie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
      a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla Administratora;
      b) monitorowanie podziału obowiązków oraz przeprowadzanie działań zwiększających świadomość w zakresie ochrony danych osobowych, szkolenia pracowników uczestniczących w operacjach przetwarzania;

c) doradztwo przy opracowaniu i aktualizacji dokumentacji opisującej sposób przetwarzania danych osobowych, a także w tym celu wdrażane środki organizacyjne i techniczne oraz przestrzeganie zasad w niej określonych;

d) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

6) prowadzenie rejestru czynności przetwarzania i rejestru wszystkich kategorii czynności przetwarzania;

7) obsługa zdarzeń oraz incydentów związanych z naruszeniem bezpieczeństwa danych osobowych;

8) prowadzenie szkoleń dla pracowników SMLW w zakresie ochrony danych osobowych.

2. Do dodatkowych zadań IOD należy:

1) prowadzenie rejestru zapytań o kontrole przetwarzania danych;

2) prowadzenie rejestru sprzeciwów/żądań zaprzestania przetwarzania danych;

3) nadzorowanie prawidłowości udostępniania danych osobowych odbiorcom danych oraz powierzania przetwarzania danych innym podmiotom;

4) prowadzenie postępowań wyjaśniających w przypadku naruszenia bezpieczeństwa danych osobowych.

§ 4

1. Administrator jest obowiązany do:

1) zgłaszania IOD:

a) rozpoczęcia przetwarzania danych osobowych;

b) zmiany w sposobie przetwarzania danych osobowych;

c) zaprzestania przetwarzania danych osobowych;

2) przeprowadzania wstępnej analizy ryzyka naruszenia praw lub wolności osób fizycznych;

3) w przypadku wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, wykonuje rozszerzoną analizę ryzyka, konsultując się z IOD. Jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, pomimo zastosowania przez Administratora dostępnych środków w celu jego zmniejszenia, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym;

4) zapewnienia rozliczalności w postaci kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone oraz komu są przekazywane, zarówno poprzez systemy IT, jak i operacje odbywające się poza tymi systemami;
5) zapewnienia ochrony przetwarzanych danych osobowych przed dostępem osób nieuprawnionych zgodnie z systemem zarządzania bezpieczeństwem informacji;
6) wprowadzania do regulacji wewnętrznych / wniosków / umów dotyczących przetwarzania danych osobowych klauzul informacyjnych spełniających obowiązek informacyjny i każdorazowe przedstawienie zmian tych regulacji do akceptacji IOD;
7) spełniania obowiązków wynikających z:
   a) prawa do informacji (obowiązek informacyjny);
   b) prawa dostępu do danych lub otrzymania kopii danych;
   c) prawa do sprostowania danych;
   d) prawa do usunięcia danych;
   e) prawa do ograniczenia przetwarzania;
   f) prawa do przenoszenia danych;
   g) prawa do sprzeciwu.

§ 5

Właściciel systemu informatycznego jest obowiązany do:

1) uzyskania pozytywnej opinii IOD oraz komórki organizacyjnej odpowiedzialnej za zarządzanie bezpieczeństwem informacji, przed zakupem nowego systemu informatycznego lub wprowadzeniem zmian do aktualnie eksploatowanego, zgodnie z procedurą zarządzania zmianą IT;
2) wdrożenia w systemie informatycznym służącym do przetwarzania danych osobowych środków technicznych i organizacyjnych, o których mowa w RODO, zapewniających ochronę przetwarzanych danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną oraz zapewnienia realizacji praw lub wolności osób fizycznych. W szczególności system informatyczny winien dla każdej osoby, której dane są przetwarzane, odnotowywać:
   a) datę pierwszego wprowadzenia danych do systemu;
   b) identyfikator użytkownika wprowadzającego dane;
   c) źródło danych, w przypadku zbierania ich nie od osoby, której dotyczą;
   d) informację o odbiorcach danych i dacie oraz zakresie udostępnienia;
   e) informację o ograniczeniu przetwarzania.

§ 6

Każdy pracownik przetwarzający dane osobowe jest zobowiązany do:

1) przestrzegania zasad określonych w niniejszej Polityce;
2) zgłoszenia IOD każdego przypadku:
   a) naruszenia ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia;
   b) otrzymania wniosku o udzielenie informacji, żądania zaprzestania przetwarzania danych osobowych lub ograniczenia przetwarzania danych osobowych, sprzeciwu wobec przetwarzania danych osobowych, wniosku o przeniesienie danych osobowych;
3) uczestniczenia w cyklicznych szkoleniach organizowanych przez Administratora, dotyczących przetwarzania danych osobowych (nie rzadziej niż raz na dwa lata lub w przypadku istotnych zmian w tym zakresie);
4) zachowania w tajemnicy, również po ustaniu zatrudnienia, wszelkich danych osobowych oraz sposobie ich zabezpieczenia.

Rozdział 3. Przetwarzanie danych osobowych

§ 7

1. Do przetwarzania danych osobowych mogą być dopuszczeni wyłącznie pracownicy posiadający upoważnienie nadane przez Administratora.
2. Ewidencja pracowników upoważnionych do przetwarzania danych prowadzona jest w postaci elektronicznej.
3. Nadanie upoważnienia do przetwarzania danych następuje na podstawie wniosku.
4. Ewidencja pracowników upoważnionych do przetwarzania danych zawiera:
   1) imię i nazwisko osoby upoważnionej;
   2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
   3) numer ewidencyjny;
   4) jednostkę/komórkę organizacyjną;
   5) datę - zakres zmiany danych (zatrudnienia, zwolnienia, zablokowania konta i odebrania uprawnień).

PODSTAWY PRAWNE PRZETWARZANIA DANYCH

§ 8

1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy spełniony zostanie, co najmniej jeden warunek:
   1) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych;
   2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
   3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na SMLW;
   4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
   5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej SMLW;
   6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez SMLW, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.
2. Za prawnie usprawiedliwiony cel, o którym mowa w ust. 1 pkt 6) niniejszego paragrafu, uważa się w szczególności:
   1) realizację działań zmierzających do zapewnienia ochrony i odporności systemów informatycznych na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjazne działania naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych osobowych oraz zapewnienia bezpieczeństwa związanych z nim usług oferowanych lub udostępnianych poprzez te systemy informatyczne;
   2) ciągłego i niezakłóconego prowadzenia działalności poprzez zapewnienie integralności kopii zarchiwizowanych/zapasowych/awaryjnych od momentu ich utworzenia aż do ich likwidacji;
   3) archiwizacyjnym (dowodowym) dla zabezpieczenia się przed różnymi rodzajami twierdzeń i roszczeń (zarzutów); dotyczy to zwłaszcza danych osobowych

znajdujących się we wnioskach kredytowych niezakończonych zawarciem umowy kredytowej;

4) realizacji zadań związanych z zapobieganiem przestępstwom dokonywanym na szkodę SMLW, w tym w szczególności w celu zapobiegania oszustwom, a także zarządzania ryzykiem operacyjnym w działalności SMLW;
5) analityki biznesowej, celów naukowych lub dla celów wewnętrznych analiz statystycznych;
6) ustalenie, dochodzenie lub obronę roszczeń z tytułu prowadzonej działalności przez SMLW;
7) monitoring wizyjny w celu ochrony mienia SMLW oraz zapewnienia bezpieczeństwa klientów i pracowników.

3. Administrator zobowiązany jest, po konsultacji z IOD, do ustalenia podstawy prawnej przetwarzania danych osobowych w związku z realizacją zadań przypisanych do danej jednostki/komórki organizacyjnej.

WARUNKI POZYSKIWANIA ZGODY

§ 9

1. Jeśli zgoda osoby ma stanowić wyłączną podstawę prawną przetwarzania danych w określonym celu lub celach, wyrażenie zgody przez osobę powinno nastąpić przed faktycznym rozpoczęciem przetwarzania danych w tym celu/celach.
2. Zapytanie o zgodę musi być wyrażone w zrozumiałej, łatwo dostępnej formie, jasnym i prostym językiem, a także stanowić odrębną deklarację.
3. Za wyrażenie zgody nie uznaje się m.in. milczenia osoby, braku sprzeciwu, niepodjęcia przez nią działań oraz zaznaczenia domyślnie okienek wyboru w systemie informatycznym.
4. SMLW umożliwia osobie, która wyraziła zgodę, wycofanie tej zgody w dowolnym momencie oraz w sposób równie łatwy, jak jej wyrażenie. Nie oznacza to jednak, że wycofanie zgody musi nastąpić dokładnie w taki sam sposób jak jej wyrażenie.

§ 10

1. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

2. Przetwarzanie danych, o których mowa w ust. 1 niniejszego paragrafu, jest dopuszczalne, jeżeli spełniony jest jeden z poniższych warunków:
   1) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że obowiązujące przepisy prawa przewidują, iż osoba, której dane dotyczą nie może uchylić zakazu, o którym mowa w ust. 1;
   2) przetwarzanie jest niezbędne do wypełnienia obowiązku i wykonywania szczegółowych praw przez Administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone obowiązującymi przepisami prawa;
   3) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora;
   4) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń;
   5) przetwarzanie jest niezbędne do wykonania zadań Administratora odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie;
   6) przetwarzanie dotyczy danych osobowych w sposób oczywisty, upublicznionych przez osobę, której dane dotyczą;
   7) przetwarzanie danych jest prowadzone przez Administratora w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym;
   8) przetwarzanie jest niezbędne dla celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 Rozporządzenia, na podstawie obowiązujących przepisów.

§ 11

1. Administrator przetwarza dane osobowe dziecka, zgodnie z obowiązującymi przepisami na podstawie zgody tej osoby.
2. Administrator przetwarza dane osobowe dziecka, które nie ukończyło wieku wskazanego zgodnie z obowiązującymi przepisami, wyłącznie gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody; w takich przypadkach, Administrator uwzględniając dostępną

technologię, podejmuje rozsądne starania, by zweryfikować, czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła zgodę lub ją zaaprobowała.

§ 12

1. Administrator ma prawo żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących:
   1) imię (imiona) i nazwisko;
   2) datę urodzenia;
   3) adres do korespondencji;
   4) adres poczty elektronicznej albo numer telefonu;
   5) wykształcenie;
   6) przebieg dotychczasowego zatrudnienia.
2. Administrator ma prawo żądać od pracownika podania, niezależnie od danych osobowych, o których mowa w ust. 1, także:
   1) innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy;
   2) numeru PESEL pracownika.
3. Udostępnienie danych osobowych następuje w formie oświadczenia osoby, której one dotyczą.
4. Administrator ma prawo żądać udokumentowania danych, o których mowa w ust. 1 i 2 niniejszego paragrafu.
5. Administrator może żądać podania innych danych osobowych, niż określone w ust. 1 i 2 niniejszego paragrafu, jeżeli obowiązek ich podania wynika z odrębnych przepisów.

§ 13

1. Pracownik komórki organizacyjnej ds. kadrowych jest zobowiązany do niezwłocznego przekazania IOD informacji (w formie elektronicznej) o podjęciu, zmianie lub zakończeniu współpracy z pracownikiem.
2. Informacja powinna obejmować: imię i nazwisko, numer ewidencyjny, jednostkę/komórkę organizacyjną, datę (zatrudnienia, zmiany danych, zwolnienia, zablokowania konta i odebrania uprawnień), zakres zmiany danych.

Rozdział 4. Prawa osób, których dane dotyczą

ZASADY OGÓLNE

§ 14

1. SMLW realizuje prawa osób, których dane dotyczą, w tym:
   1) prawo do informacji (obowiązek informacyjny);
   2) prawo dostępu do danych lub otrzymania kopii danych;
   3) prawo do sprostowania danych;
   4) prawo do usunięcia danych;
   5) prawo do ograniczenia przetwarzania;
   6) prawo do przenoszenia danych;
   7) prawo do sprzeciwu.
2. Osoba, której dane dotyczą jest uprawniona do zgłoszenia żądania, o którym mowa w ust. 1 powyżej.
3. W zakresie realizacji praw osoby, której dane dotyczą, udzielanie tej osobie informacji oraz komunikacja z tą osobą powinna odbywać się w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem; informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie lub jeżeli osoba, której dane dotyczą, tego żąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość tej osoby.
4. Ponadto Administrator:
   1) bez zbędnej zwłoki, najpóźniej w terminie miesiąca od otrzymania żądania udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem;
   2) w przypadku konieczności wydłużenia terminu realizacji żądania osoby, której dane dotyczą, najpóźniej w terminie miesiąca od otrzymania żądania, SMLW udziela informacji o przedłużeniu terminu rozpatrzenia żądania oraz podaje przyczyny opóźnienia. Wydłużenie terminu może nastąpić z uwagi na skomplikowany charakter żądań lub liczbę żądań, lecz nie więcej niż o dwa miesiące;
   3) w przypadku niepodjęcia działań w związku z żądaniem osoby, której dane dotyczą, niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.
5. SMLW komunikuje się z osobami, których dane dotyczą w języku polskim.

6. Udzielenie informacji w zakresach wskazanych w ust. 1, komunikacja z osobą, której dane dotyczą oraz podejmowanie działań na żądanie tej osoby, są wolne od opłat, z zastrzeżeniem, że jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, SMLW może:
   1) pobrać opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań;

   albo
   2) odmówić podjęcia działań w związku z żądaniem.
7. Administrator ma obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter.
8. Administrator jest uprawniony do odmowy podjęcia działań w związku z żądaniem osoby, której dane dotyczą, pragnącej wykonać swoje prawa, jeżeli wykaże iż nie jest w stanie zidentyfikować osoby, której dane dotyczą a ponadto w sytuacji, gdy:
   1) żądanie ma zostać zrealizowane w formacie lub na nośniku nieznanym lub niestosowanym przez SMLW;
   2) wniosek jest niejasny i osoba, której dane dotyczą składając wniosek, mimo prośby SMLW nie wyjaśniła w sposób jednoznaczny niejasności związanych z wnioskiem;
   3) tożsamość wnioskodawcy jest nieustalona i mimo prób, nie udało się potwierdzić tożsamości wnioskującego;
   4) osoba, której dane dotyczą nie uiściła opłaty, o której mowa w ust. 3 powyżej;
   5) realizacja żądania mogłaby spowodować ujawnienie tajemnicy SMLW lub tajemnicy przedsiębiorstwa lub innej tajemnicy prawnie chronionej;
   6) po weryfikacji wewnętrznej możliwości technicznej realizacji wniosku, SMLW ustali, że jego realizacja powodowałaby nałożenie na osobę, której dane dotyczą, nieracjonalnie wysokich kosztów;
   7) w przypadku, kiedy wnioskodawca zażąda wydania kopii danych lub przeniesienia danych w języku innym niż język, w jakim dane są przetwarzane.
9. Czas na realizację żądania, o którym mowa w ust.1 powyżej, biegnie ponownie od dnia ustalenia tożsamości osoby, której dane dotyczą oraz wniesienia opłaty lub złożenia przez osobę, której dane dotyczą, wyjaśnień lub uzupełnienia żądania.

OBOWIĄZEK INFORMACYJNY

§ 15

1. Na zgłoszenia żądania dotyczącego prawa do informacji osoby, której dane dotyczą, odpowiedzi udziela się w terminie miesiąca od dnia otrzymania wniosku.
2. W przypadku zbierania danych osobowych, jak również w przypadku zmiany celów przetwarzania danych osobowych, SMLW dopełnia obowiązku informacyjnego.
3. W przypadku zbierania danych osobowych bezpośrednio od osoby, której dane dotyczą, informacja jest przekazywana podczas pozyskiwania danych, natomiast w przypadku zbierania danych osobowych nie od osoby, której dane dotyczą:
   1) w rozsądnym terminie, nie później jednak niż w ciągu miesiąca od pozyskania danych;
   2) najpóźniej przy pierwszej komunikacji z osobą, której dane dotyczą, jeżeli dane osobowe mają być stosowane do komunikacji z tą osobą;
   3) najpóźniej przy pierwszym ujawnieniu danych, jeżeli SMLW planuje ujawnić dane osobowe innemu odbiorcy danych.
4. Informacje, o których mowa w ust. 1, mogą być przekazywane m.in. jako klauzule informacyjne zawarte w dokumentach przeznaczonych dla osoby, której dane dotyczą, klauzule informacyjne w systemie informatycznym, ustna informacja przekazana przez konsultanta, po potwierdzeniu tożsamości osoby, której dane dotyczą, czy też informacja przekazana drogą elektroniczną z zastosowaniem zasad bezpieczeństwa.
5. Odstępstwa od wypełnienia obowiązku informacyjnego w stosunku do osoby, której dane dotyczą, są możliwe jeśli m.in.:
   1) osoba posiada stosowne informacje;
   2) udzielenie informacji osobie, której dane zostały zebrane nie bezpośrednio od niej, jest niemożliwe lub wymagałoby niewspółmiernego dużego wysiłku albo wymagałoby pozyskiwania informacji dodatkowych z innych źródeł zewnętrznych;
   3) pozyskanie lub ujawnienie danych osoby, której dane są zebrane nie bezpośrednio od niej, uregulowane jest w przepisach prawa przewidujących ochronę prawnie uzasadnionych interesów osoby, której dane dotyczą;
   4) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy firmowej oraz innych tajemnic ustawowo chronionych.
6. SMLW zapewnia rozliczalność w zakresie realizacji obowiązków informacyjnych w szczególności poprzez zbieranie dokumentów przekazywanych osobom zawierające klauzule informacyjne, rejestrację rozmów telefonicznych, backup'y/zrzuty z ekranu

systemu informatycznego, kopie listów lub wiadomości wysyłanych drogą elektroniczną do klienta zawierających klauzule informacyjne, analizy oraz procedury wewnętrzne SMLW, skrypty rozmów z Klientami.

7. Spełnienie obowiązku informacyjnego może nastąpić również przez wskazanie kategorii odbiorców.

PRAWO DOSTĘPU DO DANYCH OSOBY, KTÓREJ DANE DOTYCZĄ

§ 16

1. Osoba, której dane dotyczą jest uprawniona do uzyskania potwierdzenia, czy SMLW przetwarza jej dane osobowe, a jeżeli ma to miejsce, osoba ta jest uprawniona do uzyskania dostępu do danych oraz następujących informacji o:
   1) celu przetwarzania, który powinien być konkretny, wyraźnie określony i prawnie uzasadniony;
   2) kategorii odnośnych danych osobowych;
   3) odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub mogą zostać ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
   4) w miarę możliwości planowany okres przetwarzania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   5) prawie do żądania od SMLW sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
   6) informacje o prawie wniesienia skargi do organu nadzorczego;
   7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
   8) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana przez SMLW o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem.

3. SMLW dostarcza Klientowi kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się Klient, SMLW może pobrać opłatę zgodnie z tabelą opłat i prowizji.

PRAWO DO SPROSTOWANIA DANYCH

§ 17

1. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych:
   a) które są nieprawidłowe;
   b) uzupełnienia niekompletnych danych osobowych.

PRAWO DO USUNIĘCIA DANYCH (PRAWO DO BYCIA ZAPOMNIANYM)

§ 18

1. Osoba, której dane dotyczą, może żądać w formie wyraźnego oświadczenia usunięcia danych osobowych jej dotyczących, wskazując przedmiotowy zakres żądania.
2. SMLW ustali, odrębną regulacją, okresy przechowywania danych, uwzględniając okres nie dłuższy, niż jest to niezbędne dla celów, w których dane są przetwarzane oraz okres dla przechowywania danych w celach archiwalnych lub statystycznych.
3. SMLW może przechowywać dane po osiągnięciu pierwotnych celów przetwarzania, pod warunkiem, że ich dalsze przechowywanie znajduje podstawę prawną.

Rozdział 5. Przechowywanie i usuwanie danych osobowych

§ 19

1. SMLW może nie uwzględnić żądania usunięcia danych wynikającego z cofnięcia zgody przez osobę, której dane dotyczą na przetwarzanie jej danych, w przypadku gdy zgoda osoby, której dane dotyczą nie była jedyną przesłanką przetwarzania jej danych.
2. Przetwarzanie danych osobowych osoby, której dane dotyczą, pomimo jej żądania usunięcia danych, jest zgodne z prawem, jeżeli jest niezbędne w szczególności do wywiązania się z obowiązku prawnego, do zadania realizowanego w interesie publicznym, do celów statystycznych lub do ustalenia, dochodzenia lub obrony roszczeń.
3. Po usunięciu danych SMLW jest uprawniona do zachowania informacji o tym, czyj i jaki wniosek wykonała. W tym celu SMLW może przetwarzać w szczególności imię i nazwisko, PESEL, adres wnioskującego, adres poczty elektronicznej, numer telefonu oraz informację o zakresie usuniętych danych i terminie ich usunięcia.

4. Usunięcie danych następuje poprzez ich zniszczenie lub anonimizację.
5. Jednostki/komórki organizacyjne SMLW przetwarzające dane osobowe oraz właściciele systemów informatycznych przetwarzających dane osobowe zobowiązani są na bieżąco przeglądać zbiór danych osobowych w celu uniknięcia przechowywania danych przez okres dłuższy niż jest to niezbędne.

PRAWO DO OGRANICZENIA PRZETWARZANIA DANYCH OSOBOWYCH

§ 20

1. Żądanie ograniczenia przetwarzania danych powinno być złożone w formie wyraźnego oświadczenia wskazującego przedmiotowy zakres żądania.
2. Ograniczenie przetwarzania danych SMLW może realizować w szczególności poprzez ich pseudonimizację.
3. SMLW może dodatkowo, w celu ograniczenia przetwarzania danych osobowych, w szczególności:
   1) czasowo przenieść wybrane dane osobowe do innego systemu przetwarzania;
   2) uniemożliwić użytkownikom dostęp do wybranych danych;
   3) czasowo usunąć ze strony internetowej opublikowane dane;
   4) ograniczyć środkami technicznymi przetwarzanie w zautomatyzowanych zbiorach danych w taki sposób, by dane osobowe nie podlegały dalszemu przetwarzaniu ani nie mogły być zmieniane.
4. SMLW może przechowywać dane osobowe, co do których zostało zgłoszone żądanie ograniczenia przetwarzania.
5. Realizacja żądania ograniczenia przetwarzania danych nie powoduje zaprzestania przetwarzania, które jest niezbędne do wykonania obowiązków wynikających z przepisów prawa, zaleceń lub rekomendacji organu nadzorczego.

OBOWIĄZEK POWIADOMIENIA O SPROSTOWANIU LUB USUNIĘCIU DANYCH OSOBOWYCH LUB O OGRANICZENIU PRZETWARZANIA

§ 21

1. Administrator podejmując stosowne działania informuje o sprostowaniu, usunięciu danych osobowych lub ograniczeniu przetwarzania każdego odbiorcę, któremu SMLW ujawniła dane osobowe klienta z wyłączeniem:
   1) gdy zawiadomienie okaże się niemożliwe lub wymagać będzie nadmiernie dużego wysiłku;

2) gdy zmiana, sprostowanie, ograniczenie lub usunięcie nie jest widoczne dla odbiorcy, lecz wymaga ustanowienia odrębnego kanału komunikacji;
3) odbiorca dalej nie funkcjonuje wskutek likwidacji lub wykreślenia z rejestru;
4) z okoliczności wynika, że dane nie będą dalej przetwarzane.

2. SMLW na żądanie osoby, której dane dotyczą informuje o odbiorcach, którym przekazano jej dane.
3. Jeśli obowiązek, o którym mowa w ust. 2, okaże się niewykonalny lub wymaga niewspółmiernie dużego wysiłku, SMLW powinna udokumentować podjęcie racjonalnych działań z uwzględnieniem dostępnych technologii i środków w celu wypełnienia tego obowiązku.

PRAWO DO PRZENOSZENIA DANYCH

§ 22

1. Osobie, której dane dotyczą przysługuje prawo do żądania przenoszenia danych go dotyczących. Oznacza to prawo do otrzymania oraz prawo do żądania przesłania danych innemu administratorowi.
2. Przenoszeniu podlegają tylko dane przetwarzane w sposób zautomatyzowany.
3. Przenoszeniu nie podlegają dane znajdujące się w zbiorach papierowych.
4. Dane podlegające przenoszeniu to dane, które zostały przekazane SMLW przez osobę, której dane dotyczą, świadomie i aktywnie oraz dane wygenerowane przez jej działanie, w tym dane dotyczące transakcji.
5. Osoba, której dane dotyczą może złożyć wniosek w celu skorzystania z przysługującego mu prawa do przenoszenia danych osobiście lub przez osobę upoważnioną.
6. SMLW przekaże dane w postaci pliku stosując powszechnie używany format XML
7. W przypadku żądania do przesłania danych innemu administratorowi Klient składa Administratorowi oświadczenie o wyrażeniu zgody na przeniesienie danych do innego administratora.
8. Dane mogą być przenoszone, o ile jest to technicznie możliwe. Prawo do przenoszenia danych nie może negatywnie wpływać na prawa i wolności innych osób, w tym osób, których dane znajdują się w historiach transakcji.
9. SMLW przesyłając dane podejmie należyte starania w celu zapewnienia, aby dane osobowe zostały bezpiecznie przesłane.

PRAWO SPRZECIWU

§ 23

1. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją wobec przetwarzania jej danych osobowych, wskazując jednocześnie, wobec jakiego konkretnego celu przetwarzania składa sprzeciw i wykazać, na czym polega szczególny charakter jej sytuacji.
2. SMLW ma prawo odmowy uwzględnienia sprzeciwu po dokonaniu analizy, czy szczególna sytuacja osoby, której dane dotyczą, ma charakter nadrzędny wobec prawnie uzasadnionych podstaw do przetwarzania. Jednocześnie SMLW wyjaśni przyczyny, dla których uważa, że interesy, prawa i wolności tej osoby, nie mają charakteru nadrzędnego.
3. W przypadku złożenia sprzeciwu wobec przetwarzania danych na potrzeby marketingu bezpośredniego, SMLW nie przetwarza dłużej danych w tym celu.
4. SMLW może przetwarzać dane dla celów statystycznych.
5. SMLW może odmówić uwzględnienia sprzeciwu, w przypadku gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym, w jasny i przystępny sposób wyjaśniając przyczyny odmowy. Odmowa jest poprzedzona analizą szczególnej sytuacji tej osoby.

Rozdział 6. Zautomatyzowane przetwarzanie, w tym profilowanie

1. SMLW nie profiluje klientów.
2. SMLW nie profiluje danych osobowych dzieci.

POWIADOMIENIA O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

§ 24

1. Administrator zgłasza naruszenia ochrony danych osobowych, o których mowa w ust. 2, organowi nadzorczemu.
2. Za naruszenie ochrony danych, podlegające obowiązkowi zgłoszenia organowi nadzorczemu uznać należy każdą sytuację wywołującą prawdopodobieństwo naruszenia praw lub wolności osób fizycznych. W szczególności do naruszenia mogą prowadzić następujące sytuacje:
   1) utrata danych osobowych uniemożliwiająca wykonanie zobowiązania SMLW;
   2) naruszenie integralności danych osobowych niosące ryzyko błędnego wykonania zobowiązania SMLW;

3) utrata poufności danych osobowych będąca następstwem:
    a) skompromitowania lub błędnego działania systemu informatycznego;
    b) zdarzeń losowych / środowiskowych;
    c) niepożądanych działań osób, w tym osób trzecich (kradzież, zniszczenie, uniemożliwienie dostępu, modyfikacja, ujawnienie danych);
    d) błędu ludzkiego;
    e) utraty danych osobowych uniemożliwiających wykonanie zobowiązania SMLW.

3. Obowiązek notyfikacji powinien zostać wykonany bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Wzór zawiadomienia organu nadzorczego o naruszeniu ochrony danych osobowych stanowi załącznik nr 1 do niniejszej Polityki.
4. W sytuacji, w której naruszenie ochrony danych osobowych powodowałoby wysokie ryzyko naruszenia praw lub wolności osób fizycznych, SMLW bezzwłocznie powiadamia osoby, których dane dotyczą, a jeśli powiadomienie takie wymagałoby niewspółmiernie dużego wysiłku, wydaje publiczny komunikat o naruszeniu. Wzór zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych stanowi załącznik nr 2 do Polityki.
5. Z każdego naruszenia ochrony danych osobowych sporządza się dokumentację opisującą w szczególności:
    1) okoliczności naruszenia:
        a) data i godzina stwierdzenia naruszenia ochrony danych osobowych;
        b) dane osoby zgłaszającej naruszenie;
        c) szczegółowy opis charakteru naruszenia i kontekstu, w którym do naruszenia doszło;
        d) przyczyna naruszenia;
        e) zaistniałe oraz prawdopodobne skutki naruszenia;
    2) podjęte działania zaradcze.

Rozdział 7. Ocena skutków przetwarzania danych

§ 25

1. Właściciel procesu/właściciel systemu będzie przeprowadzał wstępne lub rozszerzone oceny skutków dla ochrony danych osobowych:

1) przed wdrożeniem lub użyciem w SMLW:
    a) nowych technologii;
    b) nowych procesów;
    c) nowych funkcjonalności istniejących systemów lub dokonywania w nich zmian, w których przeprowadzane są operacje w zakresie przetwarzania danych klientów SMLW czy też innych danych osobowych;
2) przed rozpoczęciem profilowania danych osobowych klientów niezależnie od celu dla którego będzie to robione, które jest podstawą do decyzji wywołującej skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływające na osobę fizyczną;
3) z przypadku naruszenia ochrony danych osobowych;
4) w przypadku zmiany przepisów prawa w zakresie ochrony danych osobowych;
5) przed przetwarzaniem przez SMLW danych biometrycznych lub innych szczególnych kategorii danych klientów w celu podjęcia decyzji wobec klienta;
6) przed wprowadzeniem nowej usługi lub produktu pod warunkiem, że dany charakter, zakres, kontekst i cele powoduje z dużym prawdopodobieństwem wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

2. Dla podobnych operacji przetwarzania danych wiążących się z podobnym ryzykiem można przeprowadzić pojedynczą ocenę po uzyskaniu akceptacji IOD.
3. Ocena skutków dla ochrony danych, przeprowadzana jest w porozumieniu z IOD (w drodze konsultacji).

SPRAWDZANIE ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

§ 26

1. Sprawdzenie zgodności przetwarzania danych jest dokonywane przez IOD dla Administratora.
2. Sprawozdanie ze sprawdzenia zgodności powinno zawierać:
    1) oznaczenie Administratora i adres jego siedziby;
    2) imię i nazwisko IOD;
    3) wykaz czynności podjętych przez IOD w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach;
    4) datę rozpoczęcia i zakończenia sprawdzenia;
    5) określenie przedmiotu i zakresu sprawdzenia;

6) opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
7) stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem;
8) wyszczególnienie załączników stanowiących składową część sprawozdania;
9) podpis IOD, a w przypadku sprawozdania w postaci papierowej – dodatkowo parafy IOD na każdej stronie;
10) datę i miejsce podpisania sprawozdania przez IOD; sprawdzenie doraźne jest przeprowadzane niezwłocznie po powzięciu wiadomości przez IOD o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.

3. IOD zawiadamia Administratora o rozpoczęciu sprawdzenia doraźnego.
4. IOD 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.
5. Dokumentowanie czynności w toku sprawdzenia może polegać w szczególności na utrwaleniu danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych na informatycznym nośniku danych lub dokonaniu wydruku tych danych oraz na:
   1) sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
   2) odebraniu wyjaśnień osoby, której czynności objęto sprawdzeniem;
   3) sporządzeniu kopii otrzymanego dokumentu;
   4) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;
   5) sporządzeniu kopii rejestrów systemu informatycznego służącego do przetwarzania danych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.
6. W systemie informatycznym służącym do przetwarzania lub zabezpieczania danych osobowych czynności IOD mogą być wykonywane przy udziale osób upoważnionych do przetwarzania danych osobowych.

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

§ 27

1. Osoba odpowiedzialna za przetwarzanie danych osobowych, której dotyczy sprawdzenie, bierze udział w sprawdzeniu lub umożliwia IOD przeprowadzenie czynności w toku sprawdzenia.
1. Sprawując nadzór nad przetwarzaniem danych IOD dokonuje weryfikacji:
   1) opracowania i kompletności dokumentacji przetwarzania danych;
   2) zgodności dokumentacji przetwarzania danych z obowiązującymi przepisami prawa;
   3) stanu faktycznego w zakresie przetwarzania danych osobowych;
   4) zgodności ze stanem faktycznym przewidzianych w dokumentacji przetwarzania danych środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych;
   5) przestrzegania zasad i obowiązków określonych w dokumentacji przetwarzania danych.

§ 28

1. W przypadku wykrycia podczas weryfikacji nieprawidłowości IOD:
   1) zawiadamia Administratora o nieopracowaniu lub brakach w dokumentacji przetwarzania danych lub jej elementach oraz działaniach podjętych w celu doprowadzenia dokumentacji do wymaganego stanu, w szczególności może przedstawić mu do wdrożenia projekty dokumentów usuwające stan niezgodności;
   2) zawiadamia Administratora o nieaktualności dokumentacji przetwarzania danych osobowych oraz może przedstawić Administratora do wdrożenia projekty dokumentów aktualizujących;
   3) poucza osobę nieprzestrzegającą zasad określonych w dokumentacji przetwarzania danych o prawidłowym sposobie ich realizacji lub zawiadamia Administratora, wskazując osobę odpowiedzialną za naruszenie tych zasad oraz jego zakres.
2. Zawiadomienia mogą być zawarte w sprawozdaniu albo w odrębnym dokumencie.
3. Pouczenia są zawarte w odrębnym dokumencie skierowanym do osoby nieprzestrzegającej zasad określonych w dokumentacji przetwarzania danych.
4. Dokumenty, o których mowa w ust. 2 i 3 niniejszego paragrafu są sporządzane w postaci papierowej albo elektronicznej.

REJESTR CZYNNOŚCI PRZETWARZANIA ORAZ REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA

§ 29

1. Rejestr czynności przetwarzania oraz rejestr wszystkich kategorii czynności przetwarzania danych osobowych, prowadzone są w postaci elektronicznej.
2. Wzór rejestru czynności przetwarzania stanowi załącznik nr 3 do niniejszej Polityki.
3. W rejestrze czynności przetwarzania znajdują się następujące informacje:
   1) oznaczenie Administratora, adres jego siedziby, dane kontaktowe oraz numer identyfikacyjny rejestru podmiotów gospodarki narodowej;
   2) cel przetwarzania danych osobowych;
   3) opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych;
   4) planowane terminy usunięcia poszczególnych kategorii danych;
   5) kategorie odbiorców, którym dane mogą być przekazywane;
   6) informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego;
   7) opis technicznych i organizacyjnych środków bezpieczeństwa.
4. Rejestr kategorii czynności przetwarzania stanowi załącznik nr 4 do niniejszej Polityki.
5. W rejestrze wszystkich kategorii czynności przetwarzania znajdują się następujące informacje:
   1) oznaczenie podmiotu przetwarzającego, adres jego siedziby, dane kontaktowe oraz numer identyfikacyjny rejestru podmiotów gospodarki narodowej;
   2) kategorie przetwarzań dokonywanych w imieniu Administratora;
   3) kategorie odbiorców, którym dane mogą być przekazywane;
   4) informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego;
   5) opis technicznych i organizacyjnych środków bezpieczeństwa.
6. W rejestrach podaje się datę wpisu każdego zbioru danych, a także datę ostatniej aktualizacji informacji dotyczących każdego zbioru danych.
7. W przypadku wykreślenia zbioru danych z rejestrów pozostawia się nazwę zbioru danych, datę wpisania zbioru danych oraz datę ostatniej aktualizacji informacji dotyczących tego zbioru wraz z adnotacją, że jest to data wykreślenia zbioru z rejestru.
8. IOD w ramach prowadzenia rejestrów:
   1) wpisuje zbiór danych do rejestru przed rozpoczęciem przetwarzania;
   2) aktualizuje informacje dotyczące zbioru danych w rejestrach – w przypadku zmiany informacji objętych wpisem;

3) wykreśla zbiór danych z rejestrów – w przypadku zaprzestania przetwarzania w nim danych osobowych;
4) udostępnia rejestry do przeglądania.

9. Czynności, o których mowa w ust. 3 - 8 powyżej dokonuje się niezwłocznie po otrzymaniu informacji od dyrektora jednostki/komórki organizacyjnej - po otrzymaniu wniosku o dokonanie wpisu w rejestrze czynności przetwarzania.
10. IOD udostępnia organowi nadzorczemu rejestr do przeglądania przez sporządzenie wydruku rejestru.
11. IOD odnotowuje historię zmian w rejestrze zawierającą:
    1) informację o rodzaju zmiany (nowy wpis, aktualizacja, wykreślenie);
    2) datę dokonania zmiany;
    3) informację o zakresie zmiany.

Rozdział 8. Udostępnianie i powierzanie danych osobowych

§ 30

1. Administrator udostępnia dane osobowe, stanowiące jednocześnie tajemnicę SMLW, innym podmiotom niż określone w ust. 1 niniejszego paragrafu, jedynie wtedy gdy osoba, której dane dotyczą, pisemnie upoważni SMLW do przekazania danych stanowiących tajemnicę SMLW wskazanemu przez siebie podmiotowi lub osobie fizycznej.
2. Administrator powierzając przetwarzanie danych osobowych podmiotom zewnętrznym współpracuje jedynie z takimi podmiotami, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi Rozporządzenia i chroniło prawa osób, których dotyczą.
3. Administrator może powierzyć przetwarzanie danych osobowych innemu pomiotowi, bądź inny podmiot może powierzyć dane do przetwarzania Administratorowi, jedynie w drodze umowy zawartej na piśmie lub innego instrumentu prawnego, a zasady na których podstawie następuje powierzenie wyczerpują co najmniej wymagania zawarte w art. 28 RODO.
5. Powierzenie przetwarzania danych osobowych innemu administratorowi poprzedzone jest weryfikacją podmiotu przetwarzającego (procesora).
6. Administrator może powierzyć przetwarzanie danych osobowych innemu pomiotowi, bądź inny podmiot może powierzyć dane do przetwarzania Administratorowi, jedynie w

drodze umowy zawartej na piśmie. Wzór umowy o powierzenie przetwarzania danych osobowych stanowi załącznik nr 5 do niniejszej Polityki.

7. Administrator udostępnia dane odbiorcom tych danych lub powierzając dane do przetwarzania innemu podmiotowi jest zobowiązany do:
   1) uzyskania pozytywnej opinii IOD, przed udostępnieniem danych lub zawarciem umowy o powierzeniu danych osobowych zgodnie z obowiązującą w SMLW procedurą opiniowania umów;
   2) pisemnego poinformowania bez zbędnej zwłoki innych administratorów danych, którym udostępnił zbiór danych, o dokonanym uaktualnieniu lub sprostowaniu danych.

Rozdział 9. Postanowienia końcowe

§ 31

1. Osoby naruszające postanowienia niniejszej Polityki ponoszą odpowiedzialność dyscyplinarną określoną w obowiązującym w SMLW regulaminie pracy i/lub karną określoną w obowiązujących przepisach prawa.
2. Wszelkie działania podejmowane przez pracownika mające na celu nieprzestrzeganie postanowień niniejszej Polityki traktowane będą przez SMLW jako rażące naruszenie podstawowych obowiązków pracowniczych.
3. Szczegóły dotyczące zadań i podział obowiązków ciążących na Administratorze, wynikające z niniejszej Polityki zostały szczegółowo opisane w „Instrukcji Ochrony Danych Osobowych”.

Lista załączników:

Nr 1 Wzór zawiadomienia organu o naruszeniu ochrony danych osobowych.

Nr 2 Wzór zawiadomienia osoby o naruszeniu ochrony danych osobowych.

Nr 3 Wzór rejestru czynności przetwarzania.

Nr 4 Wzór rejestru kategorii czynności przetwarzania.

Nr 5 Wzór umowy powierzenia przetwarzania danych osobowych.