POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH
W PROFISUN SP. Z O.O.

ROZDZIAŁ I

Postanowienia ogólne

§ 1

1. Polityka bezpieczeństwa zwana dalej „Polityką", określa środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, sposób przepływu danych pomiędzy poszczególnymi systemami, zawiera wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, a także tryb postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych w systemach informatycznych lub kartotekach, albo w sytuacji powzięcia podejrzenia o takim naruszeniu.
2. Instrukcja została opracowana zgodnie z wymogami określonymi w Rozporządzeniu Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE.L nr 119)- dalej RODO.

§ 2

1. Ilekroć w Polityce jest mowa o:
   1) zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
   2) przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
   3) systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
   4) kartotece - rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierającej dane osobowe,
   5) Administratorze Danych - rozumie się przez to PROFISUN Sp. z o.o. z siedzibą w Krakowie,
   6) Prezesie - rozumie się przez to Prezesa Zarządu PROFISUN Sp. z o.o. działającego w imieniu Administratora Danych.
   7) Administratorze Bezpieczeństwa Informacji - rozumie się przez to osobę nadzorującą przestrzeganie zasad ochrony, która jest obowiązana zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochron. W szczególności powinna ona zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmian, utrat, uszkodzeniem lub zniszczeniem. Do jej obowiązków należy między innymi podejmowanie odpowiednich działań w przypadku stwierdzenia naruszenia ochrony danych osobowych w systemach informatycznych lub kartotekach, a także nadzór i kontrola w zakresie określonym przepisami o ochronie danych osobowych oraz regulacjami wewnętrznymi Administratora Danych,

8) osobie odpowiedzialnej za prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwację - rozumie się przez to informatyka odpowiedzialnego za powyższe zadania wyznaczonego przez Prezesa, zwanego dalej Informatykiem lub Administratorem Systemu Informatycznego,

9) komórce organizacyjnej - rozumie się przez to każdą wydzieloną organizacyjnie i funkcjonalnie komórkę wewnętrzną, zgodnie z regulaminem organizacyjnym,

10) użytkowniku – rozumie się przez to osobę wyznaczoną przez Prezesa lub osobę przez niego upoważnioną, uprawnioną do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym oraz kartotekach, posiadającą ustalony identyfikator i hasło,

11) pracowniku ochrony - rozumie się przez to osobę wykonującą zadania z zakresu ochrony osób i mienia na rzecz Administratora Danych,

12) pomieszczeniach - rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz gromadzone w kartotekach.

13) inspektor ochrony danych – osoba wyznaczona przez administratora danych osobowych, nadzorująca przestrzeganie zasad i wymogów ochrony danych osobowych określonych w RODO i przepisach krajowych,

14) Jednostce nadzorującej- organowi administracji państwowej powołanemu przez przepisy prawa do nadzorowania przestrzegania przepisów o ochronie danych osobowych, w tym RODO; wg stanu prawnego obowiązującego w maju 2018 r. powyższe funkcje pełni Prezes Urzędu Ochrony Danych Osobowych.

2. Na potrzeby wymogów określonych w art. 39 RODO ustala się nadto, iż w zakresie działalności Administratora Danych nie zachodzą aktualnie (stan na maj 2018 r.) przesłanki, które obowiązywałyby w/w podmiot do powołania Inspektora Ochrony Danych, to jest w szczególności:
   1) zgodnie z powołanym przepisem- Inspektora Ochrony Danych powołuje się, gdy „przetwarzania dokonuje organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości" - Administrator Danych nie jest organem lub podmiotem publicznym,
   2) zgodnie z powołanym przepisem- Inspektora Ochrony Danych powołuje się, gdy „główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę " - działalność główna Administratora Danych lub podmiotu przetwarzającego nie polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę, gdyż w/w działalność w ramach przedmiotu działalności ujawnionego w KRS nie polega na operacjach przetwarzania, jak i nie jest działalnością na dużą skalę.
   3) zgodnie z powołanym przepisem- Inspektora Ochrony Danych powołuje się, gdy „główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę wrażliwych danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa" - działalność główna Administratora Danych lub podmiotu przetwarzającego nie polega na przetwarzaniu na dużą skalę wrażliwych danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.
3. Administratora Danych w ramach bieżącej analizy ryzyk i potrzeb związanych z ochroną danych osobowych w ramach prowadzonej działalności oceniać będzie konieczność powołania Inspektora Ochrony Danych, stosownie do wymogów określonych m.in. w art. 39 RODO.
4. Do zadań Administratora Systemu Informatycznego należy w szczególności:
   1) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
   2) optymalizację wydajności systemu informatycznego, instalacje i konfiguracje sprzętu sieciowego i serwerowego,
   3) instalacje i konfiguracje oprogramowania systemowego, sieciowego,

4) konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem,
5) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
6) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
7) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
8) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
9) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
10) przyznawanie na wniosek administratora danych osobowych lub inspektora ochrony danych ściśle określonych praw dostępu do informacji w danym systemie,
11) wnioskowanie do administratora danych osobowych lub inspektora ochrony danych w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,
12) zarządzanie licencjami, procedurami ich dotyczącymi,
13) prowadzenie profilaktyki antywirusowej.

§ 3

1. W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.
2. Zastosowane zabezpieczenia gwarantują:
1) poufność danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
2) integralność danych - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
3) rozliczalność - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
4) integralność systemu - rozumie się przez to nienaruszalność systemu, niemożność jakiejkolwiek manipulacji,
5) uwierzytelnianie - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
6) dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
7) zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.
3. Za przestrzeganie zasad ochrony i bezpieczeństwa danych w komórkach organizacyjnych odpowiedzialni są kierownicy tych komórek.

§ 4

1. Realizację zamierzeń określonych w § 3 ust. 2 powinny zagwarantować następujące założenia:
1) wdrożenie procedur określających postępowanie osób zatrudnionych przy przetwarzaniu danych osobowych oraz ich odpowiedzialność za bezpieczeństwo tych danych,
2) przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych,

3) przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory), zapewniających im dostęp do różnych poziomów baz danych osobowych – stosownie do indywidualnego zakresu upoważnienia,
4) podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń,
5) okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych,
6) opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii,
7) śledzenie osiągnięć w dziedzinie bezpieczeństwa systemów informatycznych i- w miarę możliwości organizacyjnych i techniczno-finansowych - wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemami informatycznymi, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

§ 5

Za naruszenie ochrony danych osobowych uważa się w szczególności:
1) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują,
2) wszelkie modyfikacje danych osobowych lub próby ich dokonania przez osoby nieuprawnione (np. zmian zawartości danych, utrat całości lub części danych),
3) naruszenie lub próby naruszenia integralności systemu,
4) zmianę lub utratę danych zapisanych na kopiach zapasowych,
5) naruszenie lub próby naruszenia poufności danych lub ich części,
6) nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
7) udostępnienie osobom nieupoważnionym danych osobowych lub ich części,
8) zniszczenie, uszkodzenie lub wszelkie próby nieuprawnionej ingerencji w systemy informatyczne zmierzające do zakłócenia ich działania bądź pozyskania w sposób niedozwolony (lub w celach niezgodnych z przeznaczeniem) danych zawartych w systemach informatycznych lub kartotekach,
9) inny stan systemu informatycznego lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu pracy,
2. Za naruszenie ochrony danych osobowych uważa się również włamanie do budynku lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań.

ROZDZIAŁ II

Przedsięwzięcia zabezpieczające przed naruszeniem ochrony danych osobowych

§ 6

1. Każdy nowo zatrudniany pracownik - przed dopuszczeniem do dostępu do danych osobowych – podlega przeszkoleniu w zakresie przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków.
2. Wszyscy użytkownicy podlegają okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmian wewnętrznych regulacji.

§ 7

1. Za organizację szkoleń, odpowiedzialny jest Administrator Bezpieczeństwa Informacji.
2. Szkolenia odbywają się na wniosek kierowników komórek organizacyjnych.

§ 8

1. Użytkownicy powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych.
2. W tym celu należy:
1) zwracać szczególną uwagę przy wchodzeniu i wychodzeniu z obiektu na podejrzane osoby lub samochody parkujące w pobliżu,
2) przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych,
3) informować Administratora Bezpieczeństwa Informacji lub pracowników ochrony o podejrzanych osobach, tj.:
a) osobach zachowujących się nienormalnie np. nieodpowiednio ubranych do pory roku, dnia i pogody;
b) osobach przebywających w obiekcie bez wyraźnego celu;
c) osobach posiadających przy sobie podejrzane bagaże, w których mogą być ukryte niebezpieczne przedmioty;
4) przestrzegać zasad i procedur ochrony danych osobowych, w czasie pracy a także po jej zakończeniu.
3. Kierownicy komórek organizacyjnych, a także osoby na stanowiskach samodzielnych oraz użytkownicy zobowiązani są, na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać Administratorowi Bezpieczeństwa Informacji projekty i propozycje stosownych rozwiązań, których celem jest zabezpieczenie przed naruszeniem ochrony danych osobowych.

§ 9

1. Do podstawowych zabezpieczeń przed naruszeniem ochrony danych osobowych należą:
1) ochrona obiektu przez wszystkie dni w roku,
2) wydzielanie pomieszczeń,
3) wyposażenie pomieszczeń w specjalne szafy,
4) zabezpieczenie wejść do pomieszczeń odpowiednimi zamkami.

§ 10

1. Klucze do pomieszczeń wydawane są wyłącznie osobom do tego uprawnionym.
2. Klucze zapasowe do pomieszczeń, przechowywane są w specjalnej szafie i mogą być wydawane w sytuacjach awaryjnych.
3. Klucze zapasowe do szaf, w których przechowywane są kartoteki powinny być umieszczone w specjalnej szafie i mogą być wydawane w sytuacjach awaryjnych.
4. Każdorazowe zdanie i pobranie kluczy zapasowych podlega wpisowi do rejestru, w rejestrze odnotowuje się datę, godzinę i nazwisko osoby zdającej lub pobierającej klucze oraz potwierdza jej podpisem.

§ 11

1. Kartoteki przechowywane są w przeznaczonych do tego szafach, do których dostęp mają wyłącznie użytkownicy.
2. Użytkownicy, o których mowa w ust. 1, odpowiedzialni są za rzetelne prowadzenie kartotek, ich kompletność oraz ochronę.

ROZDZIAŁ III
Przetwarzanie danych osobowych

§ 12

1. Przetwarzanie danych osobowych z użyciem stacjonarnego sprzętu komputerowego oraz karotek odbywa się wyłącznie na obszarze wyznaczonym przez Administratora Danych.
2. Przetwarzanie danych osobowych za pomoc urządzeń przenośnych może odbywać się poza obszarem przetwarzania danych wyłącznie za zgodą Administratora Bezpieczeństwa Informacji.
3. Szczegółowy wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe określa załącznik Nr 1 do Polityki.

§ 13

1. W celu ograniczenia dostępu osób postronnych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych, należy zapewnić, aby:
1) drzwi wejściowe były zabezpieczone tak, aby otwarcie z zewnątrz mogło nastąpić wyłącznie przez uprawnione osoby,
2) wydawanie kluczy do pomieszczeń podlegało rejestracji, z jednoczesnym poświadczeniem przez osobę odbierającą, faktu otrzymania kluczy o oznaczonym numerze,
3) pomieszczenia, w których znajdują się serwery były wyposażone w miarę możliwości w sprawne systemy klimatyzacji, ochrony przeciwpożarowej i przeciwwłamaniowej,
4) pracownicy Administratora Danych oraz pracownicy ochrony byli zobowiązani do przestrzegania zasad określających dopuszczalne sposoby przemieszczania się osób trzecich w obrębie pomieszczeń, w których przetwarzane są dane osobowe,
5) przebywanie osób trzecich w pomieszczeniach może odbywać się wyłącznie w obecności użytkowników lub za zgodą Administratora Danych.

§ 14

1. Stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe, mają tylko użytkownicy oraz Informatyk.
2. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe, osób innych, niż wymienione w ust. 1, jest możliwy wyłącznie w obecności, co najmniej jednego użytkownika lub za zgodą Administratora Danych.
3. Zakaz wyrażony w ust. 2 dotyczy innych niż określeni w ust. 1, pracowników Administratora Danych oraz pracowników służb technicznych, porządkowych, itp.
4. Przebywanie użytkownika po godzinach pracy w pomieszczeniach, w których przetwarzane są dane osobowe jest dopuszczalne jedynie za zgodą kierownika komórki organizacyjnej.

§ 15

W trakcie prac technicznych wykonywanych przez osoby trzecie w pomieszczeniach, przetwarzanie danych jest zabronione.

§ 16

1. Administrator Bezpieczeństwa Informacji jest odpowiedzialny za całość zagadnień dotyczących ochrony i bezpieczeństwa danych osobowych.

2. W celu sprawnego wykonywania swoich zadań Administrator Bezpieczeństwa Informacji jest uprawniony do wnioskowania do Prezesa w celu wyznaczania kierownikom komórek organizacyjnych oraz użytkownikom wykonywania określonych zadań.
3. Kierownicy komórek organizacyjnych zobowiązani są do przestrzegania przepisów o ochronie danych osobowych na terenie podległych komórek organizacyjnych, a także do ścisłej współpracy z Administratorem Bezpieczeństwa Informacji. W tym celu zobowiązani są do:
1) pisemnego wnioskowania o rejestrację nowych zbiorów danych osobowych,
2) okresowego składania pisemnej informacji z przebiegu bieżącej kontroli i oceny funkcjonowania mechanizmów zabezpieczeń i ochrony,
3) występowania z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych.

§ 17

1. Administrator Danych przetwarza dane osobowe – kontrahentów, klientów, wykonawców i podwykonawców, pracowników, osób zatrudnionych na podstawie umów cywilno- prawnych oraz innych osób - zebranych w zbiorach danych osobowych.
2. Informacje te są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej.
3. Polityka bezpieczeństwa zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.
4. Szczegółowy wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania określa załącznik Nr 2 do Polityki.

§ 18

1. Zgodnie z wymogami RODO Administrator Danych prowadzi opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych, którego wzór określa załącznik nr 3 do Polityki.
2. Administrator Danych prowadzi nadto wewnętrzny rejestr czynności przetwarzania danych z oceną skutków przetwarzania danych oraz rejestr kategorii przetwarzania danych.

Rozdział IV

Kontrola przestrzegania zasad zabezpieczenia ochrony danych osobowych

§ 19

1. Administrator Bezpieczeństwa Informacji sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych.
2. W przypadku nieobecności Administratora Bezpieczeństwa Informacji, osobę zastępującą wyznacza Prezes.
3. Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona dokonuje okresowych kontroli i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad postępowania w przypadku naruszenia ochrony danych osobowych.
4. Przedmiotem kontroli, o których mowa w ust. 3 powinno być w szczególności:
1) funkcjonowanie zabezpieczeń systemowych,
2) prawidłowo funkcjonowania mechanizmów kontroli dostępu do zbioru danych,
3) funkcjonowanie zastosowanych zabezpieczeń fizycznych,
4) zasady przechowywania kartotek,
5) zasady i sposoby likwidacji oraz archiwizowania zbiorów archiwalnych,

6) realizacja procedur wdrożonych przez Administratora Danych w zakresie ochrony danych.
5. Administrator Bezpieczeństwa Informacji prowadzi rejestr dokonywanych kontroli oraz ustaleń, wniosków i zaleceń z nich wynikających, a także nadzoruje ich wykonywanie.
6. Z kontroli, o których mowa w ust. 3 należy sporządzać protokoły, które przechowuje Administrator Bezpieczeństwa Informacji.

Rozdział V

Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

§ 20

1. Przed przystąpieniem do pracy użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.
2. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Administratora Bezpieczeństwa Informacji lub upoważnioną przez niego osobę.
3. Obowiązek określony w ust. 2 ciąży równie na pozostałych pracownikach Administratora Danych.
4. Postanowienia ust. 2 i 3 mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych gromadzonych w systemach informatycznych, jak i w kartotekach.

§ 21

1. Do czasu przybycia Administratora Bezpieczeństwa Informacji lub upoważnionej przez niego osoby, zgłaszający:
1) powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,
2) zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osób nieupoważnionych,
3) podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
2. Postanowienia ust. 1 mają zastosowanie zarówno w przypadku naruszenia, jak i w przypadku podejrzenia naruszenia ochrony danych.

§ 22

1. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona, po przybyciu na miejsce:
1) ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane oraz stan urządzeń, a także identyfikuje wielkość negatywnych następstw incydentu,
2) wysłuchuje relacji osoby, która dokonała powiadomienia,
3) podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych. W uzasadnionych przypadkach niezwłocznie powiadamia Prezesa.

§ 23

1. Administrator Bezpieczeństwa Informacji lub upoważniona przez niego osoba sporządza z przebiegu zdarzenia raport, w którym powinny się znaleźć w szczególności informacje o:
1) dacie i godzinie powiadomienia,
2) godzinie pojawienia się w pomieszczeniach, w których przetwarzane są dane,
3) sytuacji, jaką zastał,
4) podjętych działaniach i ich uzasadnieniu.
2. Kopia raportu przekazywana jest bezzwłocznie Prezesowi, w przypadku, gdy raport sporządzony został przez osobę upoważnioną przez Administratora Bezpieczeństwa Informacji, także Administratorowi Bezpieczeństwa Informacji.

§ 24

1. Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona podejmuje kroki zmierzające do likwidacji naruszeń zabezpieczeń danych osobowych i zapobieżenia wystąpieniu ich w przyszłości. W tym celu:
1) w miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu,
2) relacjonuje Prezesowi przedsięwzięte czynności,
3) o ile taka potrzeba zachodzi, postuluje wprowadzenie nowych form zabezpieczenia, a w razie ich wprowadzenia nadzoruje zaznajamianie z nimi osób zatrudnionych przy przetwarzaniu danych osobowych.
2. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej u Administratora Danych dyscypliny pracy, Administrator Bezpieczeństwa Informacji lub upoważniona przez niego osoba wnioskuje do Prezesa o wyjaśnienie wszystkich okoliczności incydentu i o podjęcie stosownych działań wobec osób, które dopuściły się tego uchybienia.

§ 25

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od Administratora Bezpieczeństwa Informacji lub osoby przez niego upoważnionej.

§ 26

1. W przypadku zaginięcia komputera lub nośników magnetycznych, na których były zgromadzone dane osobowe, użytkownik posługujący się komputerem niezwłocznie powiadamia Administratora Bezpieczeństwa Informacji lub upoważnioną przez niego osobę, a w przypadku kradzieży występuje o powiadomienie jednostki policji.
2. W sytuacji, o której mowa w ust. 1 Administrator Bezpieczeństwa Informacji lub upoważniona przez niego osoba podejmuje niezbędne kroki do wyjaśnienia okoliczności zdarzenia, sporządza protokół z zajęcia, który powinna podpisać także osoba, której skradziono lub której zaginął sprzęt oraz powiadamia Prezesa.
3. W przypadku kradzieży komputera razem z nośnikiem magnetycznym Administrator Bezpieczeństwa Informacji lub upoważniona przez niego osoba podejmuje działania zmierzające do odzyskania utraconych danych oraz nadzoruje proces przebiegu wyjaśnienia sprawy.

§ 27

Administrator Danych jest zobowiązany do zgłoszenia Jednostce nadzorującej wszystkich incydentów które spowodowały wyciek danych osobowych, bądź godziły w bezpieczeństwo ich przechowywania. W

przypadku naruszenia lub zagrożenia naruszenia danych osobowych klientów, Administrator Danych jest zobowiązany do powiadomienia wszystkich osób, których ten incydent dotyczył.

Rozdział VI

Procedura postępowania w przypadku wystąpienia wniosku informacyjnego od osoby, której dane dotyczą lub złożenia sprzeciwu co do przetwarzania danych osobowych do celów marketingu bezpośredniego

§ 28

1. Każdej osobie, której dane przetwarza Administrator Danych, przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorze danych Administratora Danych, a zwłaszcza prawo do: żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.
2. W przypadku udzielenia przez osobę zgody na przetwarzanie danych w celu marketingu bezpośredniego własnych produktów lub usług administratora zgoda może być odwołana w każdym czasie.
3. Przy uwzględnieniu powyższego dana osoba w odniesieniu do powyższych danych osobowych ma prawo do:
a) żądania dostępu do danych osobowych,
b) sprostowania danych,
c) żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia,
d) usunięcia danych lub ograniczenia przetwarzania,
e) wniesienia sprzeciwu wobec dalszego przetwarzania Państwa danych osobowych,
f) przeniesienia Twoich danych osobowych
4. W przypadku wątpliwości co do prawidłowości przetwarzania Państwa danych osobowych przez Administratora, mają Państwo prawo wniesienia skargi do organu nadzorczego.
5. W celu realizacji uprawnień, o których mowa powyżej, osoba zainteresowana może się kontaktować z Administratorem Danych poprzez przesłanie stosownej wiadomości pisemnie lub pocztą elektroniczną na adres Administratora Danych wskazany na jego stronie internetowej lub też przekazany bezpośrednio w dokumentach i oświadczeniach udostępnionych danej osobie.

§ 29

Osoba zatrudniona przy przetwarzaniu danych osobowych za naruszenie obowiązków wynikających z niniejszej Polityki bezpieczeństwa oraz przepisów o ochronie danych osobowych ponosi odpowiedzialność przewidzianą w Regulaminie Pracy, Kodeksie Pracy oraz wynikające z przepisów RODO.

ROZDZIAŁ VI

Postępowanie w wypadku klęski żywiołowej

§ 30

Klęską żywiołową jest katastrofa, spowodowana działaniem sił przyrody takich jak ogień, huragan, woda lub ich przejawami.

§ 31

W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe, mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczególnych.

§ 32

1. O zagrożeniu, jego skali i podjętych krokach zaradczych pracownik ochrony zobowiązany jest niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji lub osobę przez niego upoważnioną w każdy możliwy sposób. W razie niemożności skontaktowania się z nim pracownik ochrony zawiadamia, co najmniej jedną z niej wymienionych osób:
1) osobę wyznaczoną przez Prezesa,
2) Prezesa.
2. Numery telefonów Administratora Bezpieczeństwa Informacji i osób, z którymi należy się kontaktować na wypadek klęski żywiołowej powinny być znane pracownikom.

§ 33

Osoby biorce udział w akcji ratunkowej, mają prawo wejść do pomieszczeń w których przetwarzane są dane osobowe bez dopełniania obowiązku, o którym mowa w § 14 ust. 2 Polityki.

§ 34

W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy, przebywający w pomieszczeniach, w których przetwarzane są dane osobowe, obowiązani są do przerwania pracy, a w miarę możliwości przed opuszczeniem tych pomieszczeń do:
1) zamknięcia systemu informatycznego,
2) zabezpieczenia danych osobowych gromadzonych w kartotekach.

§ 35

1. W czasie trwania akcji ratunkowej i po jej zakończeniu Administrator Bezpieczeństwa Informacji oraz obecni użytkownicy powinni, w miarę możliwości, zabezpieczać dane osobowe przed nieuprawnionym do nich dostępem.
2. Obowiązek ten ciąży w równym stopniu na innych pracownikach Administratora Danych, obecnych przy akcji ratunkowej.

ROZDZIAŁ VII

Stosowanie zasad privacy by design oraz privacy by default.

§ 36

1. Administrator Danych obowiązany jest do uwzględnienia ochrony danych i prywatności na każdym etapie tworzenia oraz istnienia technologii obejmującej ich przetwarzanie. Zasady ochrony prywatności są częścią składową każdego projektu zakładającego przetwarzanie danych osobowych w taki sposób, od samego początku jego istnienia. Ustawienia aplikacji czy systemów przetwarzających dane domyślnie

powinny udostępniać minimalną ilość informacji o użytkowniku. Poszerzenie zakresu udostępnianych danych może nastąpić jedynie na podstawie zmiany ustawień dokonanych przez samego użytkownika.
2. Powyższe wynika ze stosowania zasad- **privacy by design** -nazywanej też „zasadą prywatności w fazie projektowania" oraz - **privacy by default-** nazywanej też „zasadą prywatności w ustawieniach domyślnych". Ich treść oraz zakres są ustalane poprzez wskazanie funkcji, jakie spełniać powinny wprowadzane do użytku programy (systemy) przetwarzające dane osobowe.
3. Zgodnie z zasadą **privacy by default**, ochrona prywatności jest domyślnym ustawieniem każdego programu (systemu), a zmiana takiego ustawienia powinna następować jedynie na wyraźne żądanie użytkownika programu. Zasada privacy by default przewiduje jak najszerszą domyślną ochronę prywatności wszystkich użytkowników danego systemu. Użytkownicy, którzy chcąc zrezygnować z części swej prywatności powinni podjąć aktywne działania w tym kierunku, bez wpływy na powyższe decyzje i prywatność twórców systemu.
4. Zgodnie z **zasadą privacy by design** zasady ochrony prywatności są wbudowane w każdy projekt zakładający przetwarzanie danych osobowych w taki sposób, aby od samego początku jego istnienia ochrona prywatności stanowiła jego część składową.
5. Zgodnie z art. 25 ust. 1 RODO: „Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą". (**Zasada privacy by design).** Oznacza to, że Administrator Danych jest zobowiązany zapewnić, aby już na etapie projektowania systemu oraz na etapie wykorzystywania go do przetwarzania danych wprowadzone do niego zostały odpowiednie środki techniczne i organizacyjne, które zapewnią ochronę danych użytkowników i ich przetwarzanie zgodnie z Rozporządzeniem. Administrator Danych na etapie projektowania nowego rozwiązania sporządza stosowny dokument obejmujący informacje o przeanalizowanych rozwiązaniach w zakresie ochrony danych osobowych, w tym sporządzone listy kontrolne (checklist).
6. Zgodnie z zasadą **privacy by default**, ochrona prywatności jest domyślnym ustawieniem każdego programu (systemu), a zmiana takiego ustawienia powinna następować jedynie na wyraźne żądanie użytkownika programu. Zasada privacy by default przewiduje jak najszerszą domyślną ochronę prywatności wszystkich użytkowników danego systemu. Użytkownicy, którzy chcąc zrezygnować z części swej prywatności powinni podjąć aktywne działania w tym kierunku, bez wpływy na powyższe decyzje i prywatność twórców systemu.

7. Zasadę **privacy by default** określa natomiast art. 25 ust. 2 RODO: Administrator jest zobowiązany wdrożyć takie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania. Dotyczyć to będzie ilości zbieranych danych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. Omawiane środki powinny zapewniać w szczególności, aby domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych. (**Zasada privacy by default).**

8**.** Realizacja powyższego obowiązku będzie realizowana w szczególności poprzez:
Obowiązek usunięcia lub ograniczenia przetwarzania danych:
a) rejestr zmian (np. logi transakcyjne),
b) realizacja zmian w trakcie odtworzenia z backupu
Obowiązek zapewnienia poufności danych:
a) szyfrowanie backupu danych (hardware, software),
b) fizyczne zabezpieczenie nośników,
c) podejście do wycofywanych nośników (niszczenie, zamazywanie),
d) brak dostępu do danych dla administratorów systemów backup.

ROZDZIAŁ VII

Ocena skutków dla ochrony danych

§ 37

1. Zgodnie z art. 35 RODO, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator Danych przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.
2. Dokonując oceny skutków dla ochrony danych, Administrator Danych konsultuje się z Inspektorem Ochrony Danych, jeżeli został on wyznaczony.
3. Ocena skutków dla ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w przypadku:
a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa; lub
c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.
4. Wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych jest ustanawiany i podany do publicznej wiadomości przez Organ nadzorujący. W podobny sposób Organ nadzorujący ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych.
5. Ocena skutków dla ochrony danych zawiera co najmniej:
a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez Administratora Danych;
b) ocenę czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz
d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.
6. Oceniając – w szczególności do celów oceny skutków dla ochrony danych – skutki operacji przetwarzania wykonywanych przez Administratora Danych lub podmiot przetwarzający, uwzględnia się przestrzeganie przez Administratora Danych lub taki podmiot przetwarzający zatwierdzonych kodeksów postępowania, o których mowa w art. 40 RODO, o ile zostaną wprowadzone.
7. W stosownych przypadkach Administrator Danych zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania.
8. W razie potrzeby, przynajmniej, gdy zmienia się ryzyko wynikające z operacji przetwarzania, Administrator Danych dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.
9. Wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z niniejszym rozporządzeniem. Jeżeli ocena skutków dla ochrony danych wykaże, że operacje przetwarzania powodują wysokie ryzyko, którego Administrator Danych nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej

technologii i kosztów wdrożenia, przed przetwarzaniem należy skonsultować się z Organem nadzorującym.

ROZDZIAŁ IX

Postanowienia końcowe

§ 38

Polityka jest dokumentem wewnętrznym i nie może być udostępniana osobom nieupoważnionym w żadnej formie.

§ 39

1. Kierownicy komórek organizacyjnych są obowiązani zapoznać z treści Polityki każdego użytkownika.
2. Użytkownik zobowiązany jest złożyć oświadczenie, o tym i został zaznajomiony z przepisami o ochronie danych osobowych, obowiązującą Polityką bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
3. Wzór oświadczenia, o którym mowa w ust. 2, określa załącznik do Instrukcji zarządzania informatycznym systemem służącym do przetwarzania danych osobowych.
4. Oświadczenia przechowywane są w aktach personalnych pracownika.

§ 40

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych.
2. Użytkownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.

ZARZĄD

PROFISUN

PODPIS ZAUFANY
GABRIEL
JAŹDZIKOWSKI
18.05.2022 14:26:48 [GMT+2]
Dokument podpisany elektronicznie
podpisem zaufanym

PODPIS ZAUFANY
MARCIN
NOWAK
18.05.2022 10:46:50 [GMT+2]
Dokument podpisany elektronicznie
podpisem zaufanym