POLITYKA BEZPIECZEŃSTWA INFORMACJI

PGR KOSZELEW SP. Z O.O.

Spis treści

1. Wstęp

1.1. Informacje ogólne

Niniejsza Polityka Bezpieczeństwa Informacji wdrażana jest przez PGR KOSZELEW Sp. z o.o. z siedzibą w Gąbinie (09-530), przy ul. Kutnowskiej 10A. Aktualizacja dokumentacji bezpieczeństwa informacji ma miejsce w związku z wejściem w życie rozporządzenia 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1) oraz wprowadzeniem zmian w polskim ustawodawstwie w zakresie ochrony danych osobowych.

Administrator Danych Osobowych postanawia wdrożyć niniejszy dokument przy zachowaniu wszelkich standardów ochrony danych osobowych. Misja PGR Koszelew realizowana jest również poprzez zapewnienie właściwego poziomu bezpieczeństwa informacji i ochronę prawa do prywatności. PGR Koszelew deklaruje zamiar podejmowania wszelkich działań niezbędnych dla zapewnienia ochrony praw jednostki związanych z bezpieczeństwem danych osobowych, zamiar nieustannego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe. PGR Koszelew deklaruje chęć rozwijania nowoczesnych rozwiązań dot. przetwarzania danych osobowych.

1.2. Cel i zakres unormowań

Głównym celem wprowadzenia Polityki Bezpieczeństwa Informacji jest zapewnienie bezpieczeństwa przetwarzanych danych osobowych w strukturze PGR Koszelew. Polityka została opracowana w celu realizacji wymogów wynikających z przepisów prawa, a w szczególności rozporządzenia 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, ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. Wskazuje się podstawowe cele wprowadzenia:

1. zastosowane zabezpieczenia mają zapewnić poufność, integralność, rozliczalność danych, integralność systemu, dostępność informacji oraz zarządzanie ryzykiem;
2. cele stosowania zabezpieczeń i ich rodzaj są dobierane na podstawie:
    a) przepisów obowiązujących aktów prawnych;
    b) wyników przeprowadzonej analizy ryzyka bezpieczeństwa danych osobowych;
    c) dobrych praktyk uznanych w obrocie profesjonalnym;
    d) aktualnych rozwiązań technologicznych;
3. zabezpieczenia występują w następujących obszarach:
    a) organizacyjnym;

b) technicznym.

Zakres obowiązywania Polityki Bezpieczeństwa Informacji obejmuje w szczególności:

1. istniejące lub wprowadzane w przyszłości systemy informatyczne, dokumenty w formie tradycyjnej, w których przetwarzane są lub będą dane osobowe;
2. wszystkie rodzaje nośników danych osobowych;
3. wszystkie osoby mające dostęp do danych osobowych, w szczególności pracowników;
4. wszelkie obszary, w których przetwarzane są dane osobowe.

Polityka Bezpieczeństwa Informacji określa podmioty odpowiedzialne za przetwarzanie danych osobowych oraz ich zadania, w szczególności Administratora Danych, Administratora Systemu oraz Inspektora, środki organizacyjne i techniczne niezbędne dla zapewnienia ochrony danych osobowych. Polityka przechowywana jest przez Administratora Danych. Polityka jest dostępna dla każdego członka Personelu.

Integralną częścią Polityki Bezpieczeństwa Informacji są następujące załączniki:

1. wzór klauzuli informacyjnej Administratora Danych;
2. wzór upoważnienia do przetwarzania danych osobowych;
3. wzór oświadczenia o zachowaniu w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
4. wzór ewidencji osób upoważnionych do przetwarzania danych osobowych;
5. wzór rejestru czynności przetwarzania danych osobowych;
6. wzór rejestru kategorii czynności przetwarzania;
7. wzór rejestru zgłoszeń i naruszeń ochrony danych osobowych;
8. wzór umowy powierzenia przetwarzania danych osobowych.

1.3. Skróty i definicje

Ilekroć w niniejszym dokumencie jest mowa o:

1. Administratorze Ochrony Danych (Administrator Danych) – rozumie się przez to PGR KOSZELEW Sp. z o.o. z siedzibą w Gąbinie (09-530), przy ul. Kutnowskiej 10A;
2. Administratorze Systemu Informatycznego (Administrator Systemu, ASI) – rozumie się przez to osobę upoważnioną, zarządzającą systemem informatycznym, w którym przetwarzane są dane osobowe przy wykorzystaniu mechanizmów uwierzytelniania

Użytkowników oraz nadzorującą bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych;

3. Bezpieczeństwie danych osobowych – rozumie się przez to zachowanie poufności, integralności i dostępności danych gromadzonych i przetwarzanych przez Administratora;
4. Danych osobowych – rozumie się przez to 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;
5. Danych osobowych szczególnych kategorii (Dane wrażliwe) – rozumie się dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby;
6. Eksporcie danych – rozumie się przez to przekazanie danych do państwa trzeciego lub organizacji międzynarodowej;
7. Haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
8. Identyfikatorze użytkownika (jeśli dotyczy) – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
9. Inspektorze Ochrony Danych (Inspektor) – rozumie się przez to osobę powołaną przez Administratora Danych w celu nadzorowania i przestrzegania zasad ochrony danych osobowych;
10. Instrukcji – rozumie się przez to Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
11. Integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
12. Incydencie – rozumie się naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia, lub nieuprawnionego dostępu do danych osobowych lub informacji przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

13. Odbiorcy – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią;
14. Osobie – rozumie się przez to osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu,
15. Osobie upoważnionej do przetwarzania danych osobowych – rozumie się przez to osobę, której zostało nadane upoważnienie do przetwarzania danych osobowych;
16. Personelu – rozumie się przez to osoby świadczące pracę na rzecz Administratora Danych na podstawie stosunku pracy, umów cywilnoprawnych, przedsiębiorców, praktykantów, stażystów, wolontariuszy, osoby skierowane do pracy w ramach umów z agencjami pracy tymczasowej wykonujące czynności związane z przetwarzaniem danych osobowych;
17. Podmiocie Przetwarzającym (Procesor) – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych;
18. Polityce – rozumie się przez to Politykę Bezpieczeństwa Informacji, o ile co innego nie wynika wyraźnie z kontekstu;
19. Poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
20. Profilowaniu – rozumie się przez to dowolną formę 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;
21. Powierzeniu przetwarzania danych osobowych – rozumie się przez to zlecenie wykonywania czynności przetwarzania danych osobowych przez Podmiot Przetwarzający na rzecz Administratora Danych na podstawie umowy powierzenia przetwarzania danych osobowych;
22. Przetwarzaniu – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
23. Pseudonimizacji – rozumie się przez to przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane

osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

24. Raporcie – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
25. Rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
26. Rozporządzeniu (RODO) – rozumie się przez to rozporządzenie 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 (ogólne rozporządzenie o ochronie danych);
27. Stacji roboczej – rozumie się przez to poszczególny egzemplarz sprzętu komputerowego, w konfiguracji umożliwiającej prawidłowe działanie, włączony do sieci informatycznej Administratora Danych (np. komputer klasy PC, laptop, iPad);
28. Systemie informatycznym – rozumie się zespół współpracujących ze sobą urządzeń, programów, aplikacji, sieci LAN, sieci WAN, stacje robocze, zasoby sieciowe (dyski, drukarki);
29. Teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
30. Urządzeniu – rozumie się przez to komputer stacjonarny i przenośny, laptop, tablet, telefon komórkowy oraz inny sprzęt elektroniczny, dzięki któremu można zalogować się do systemu;
31. Ustawie – rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych;
32. Usuwaniu danych – rozumie się przez to proces zniszczenia danych osobowych lub taką ich modyfikację, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą;
33. Uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
34. Użytkowniku – rozumie się przez to osobę upoważnioną do dostępu do systemów informatycznych i przetwarzania danych osobowych w nich zawartych, której nadano identyfikator (jeśli dotyczy) i przyznano hasło;
35. Urząd Ochrony Danych Osobowych – rozumie się przez to organ właściwy w sprawie ochrony danych osobowych;
36. Zagrożeniu – rozumie się przez to potencjalną przyczynę niepożądanego incydentu, którego skutkiem może być szkoda dla systemu.

2. Podmioty odpowiedzialne za ochronę danych osobowych

2.1. Wprowadzenie

Podmiotami odpowiedzialnymi za przetwarzanie danych osobowych oraz ich ochronę są:

1. Administrator Danych;
2. Administrator Systemu;
3. Inspektor Ochrony Danych;
4. Podmiot Przetwarzający;
5. Osoby upoważnione do przetwarzania danych osobowych.

2.2. Administrator Danych Osobowych

1. Administratorem Danych jest PGR KOSZELEW Sp. z o.o. z siedzibą w Gąbinie (09-530), przy ul. Kutnowskiej 10A.
2. Administrator Danych wykonuje obowiązki w zakresie ochrony danych osobowych, w szczególności:
    1) podejmuje działania mające na celu zabezpieczenie danych osobowych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, niekontrolowaną zmianą, utratą, w tym utratą przypadkową, uszkodzeniem bądź zniszczeniem;
    2) zapewnia przetwarzanie danych zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
    3) dokonuje przed rozpoczęciem przetwarzania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, przy czym ocena ta powinna w szczególności obejmować planowane środki, zabezpieczenia i mechanizmy mające minimalizować ryzyko naruszenia praw lub wolności osób fizycznych, zapewniać ochronę danych osobowych oraz wykazać przestrzeganie przepisów prawa;
    4) zapewnia zbieranie danych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzanie ich dalej w sposób niezgodny z tymi celami;
    5) zapewnia, aby dane osobowe były adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
    6) zapewnia, aby zbierane dane były prawidłowe i aktualizowane;
    7) zapewnia przechowywanie w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;

8) wykazuje, że osoba której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych, chyba że przetwarzanie danych osobowych następuje na innej podstawie prawnej niż zgoda;

9) jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, Administrator Danych podczas pozyskiwania danych osobowych podaje jej informacje, których zakres określają odrębne przepisy, w szczególności Ustawa oraz Rozporządzenie;

10) jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, Administrator Danych podaje osobie, której dane dotyczą, informacje, których zakres określają odrębne przepisy, w szczególności Ustawa oraz Rozporządzenie, z zachowaniem następujących terminów:

    a) w rozsądnym terminie, nie później jednak niż po upływie jednego miesiąca;

    b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą;

    c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu;

11) w uzasadnionych przypadkach powołuje Inspektora oraz wspiera go w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej;

12) zawiadamia osobę, której dane dotyczą, o naruszeniu ochrony jej danych;

13) zapewnia osobom, których dane dotyczą możliwość kontaktowania się z Inspektorem we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem przysługujących im praw;

14) zapewnia Personelowi stanowiska pracy zgodnie z powierzonymi obowiązkami;

15) podejmuje odpowiednie działania w przypadku wykrycia naruszeń bezpieczeństwa;

16) współpracuje z osobami pełniącymi role odpowiedzialne za bezpieczeństwo danych osobowych;

17) może powierzać wykonanie powyższych obowiązków Inspektorowi;

18) zapewnia by Inspektor był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;

19) wspiera Inspektora w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań, w tym sprzęt komputerowy i wyposażenie biura, oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania

jego wiedzy fachowej poprzez udział w szkoleniach, doskonaleniu zawodowym, dostępie do baz wiedzy prawnej i specjalistycznej literatury;

20) zapewnia, by Inspektor nie otrzymywał instrukcji, poleceń, wytycznych dotyczących wykonywania tych zadań, bądź też nie był poddawany innym formom nacisku w związku z pełnioną funkcją.

2.3. Administrator Systemu Informatycznego

1. Administrator Danych może powołać Administratora Systemu. Gdy Administrator Systemu nie został wyznaczony, jego funkcję sprawuje Administrator Danych, bądź inny podmiot wskazany przez Administratora Danych.
2. Administrator Systemu nadzoruje zabezpieczenie przetwarzanych danych osobowych w systemach informatycznych, zapewnia ciągłość działania systemów informatycznych.
3. Administrator Systemu zarządza systemem informatycznym, w którym przetwarzane są dane osobowe przy wykorzystaniu mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym te dane oraz kontroli dostępu do tych danych.
4. Administrator Systemu sprawuje nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych.
5. Administrator Systemu posługuje się hasłem dostępu do wszystkich stacji roboczych i serwera z pozycji administratora.
6. Administrator przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w szczególności poprzez zarządzanie:
   a) dostępami przez ich nadawanie, odbieranie i zmianę;
   b) kontami użytkowników przez ich zakładanie, blokowanie i usuwanie;
   c) hasłami przez ich zmianę, jak również opracowywanie procedur określających częstotliwość zmiany haseł i ich przestrzeganie.
7. Administrator Systemu wspomaga Administratora Danych oraz Inspektora w opracowaniu i aktualizacji Instrukcji.
8. W przypadku stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje niezwłocznie Inspektora lub Administratora Danych i podejmuje działania mające na celu usunięcie jego skutków.
9. Administrator Systemu wspiera Administratora Danych w szkoleniu Użytkowników w zakresie procedur, instrukcji oraz sprawuje nadzór nad ich przestrzeganiem.
10. Administrator Systemu wspiera Administratora Danych w prowadzeniu szczegółowej dokumentacji naruszeń bezpieczeństwa, incydentów, obniżenia poziomu bezpieczeństwa

bądź innych nieprawidłowości dot. danych osobowych przetwarzanych w systemie informatycznym.

11. Administrator Systemu nadzoruje rozwój, modyfikacje, przeglądy, naprawy, konserwacje, serwisowanie, aktualizacje, tworzenie kopii zapasowych, ich przechowywanie oraz inne czynności wykonywane w systemie informatycznym, a także likwidacje stanowisk komputerowych oraz wszelkich nośników pamięci.

2.4. Inspektor Ochrony Danych

1. Inspektor jest wyznaczany - jeśli dotyczy - przez Administratora Danych na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia niżej wymienionych zadań.
2. Inspektorem może być osoba mająca pełną zdolność do czynności prawnych oraz korzystająca z pełni praw publicznych oraz niekarana za umyślne przestępstwo bądź przestępstwo skarbowe.
3. Inspektor może być członkiem Personelu Administratora lub wykonywać zadania na podstawie umowy o świadczenie usług.
4. Inspektor może wykonywać inne zadania i obowiązki. Administrator Danych zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.
5. Inspektor monitoruje, czy jest właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
6. Inspektor ma obowiązek podnoszenia kwalifikacji własnych z zakresu ochrony danych osobowych poprzez udział w szkoleniach, doskonaleniu zawodowym, korzystanie z baz wiedzy prawnej i specjalistycznej literatury.
7. Inspektor informuje Administratora Danych o przypadkach udzielania mu instrukcji, poleceń, wytycznych dotyczących wykonywania tych zadań bądź też o poddawaniu go innym formom nacisku w związku z pełnioną funkcją.
8. Inspektor nie może zostać odwołany ani ukarany przez Administratora Danych za wypełnianie swoich zadań.
9. Inspektor bezpośrednio podlega Administratorowi Danych.
10. Inspektor jest uprawniony do kontaktowania się z osobami, których dane dotyczą we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy przepisów prawa.
11. Inspektor jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.

12. Inspektor wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
13. Do obowiązków Inspektora należy w szczególności:
    1) informowanie Administratora Danych, Administratora Systemu, Podmiotu Przetwarzającego oraz członków Personelu, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych i doradzanie im w tej sprawie;
    2) monitorowanie przestrzegania przepisów o ochronie danych oraz stały nadzór nad Polityką, Instrukcją, jak również innymi dokumentami w dziedzinie ochrony danych osobowych;
    3) przeprowadzanie audytów, okresowych kontroli i przygotowywanie sprawozdań po ich zakończeniu oraz wdrażanie zmian, w tym podział obowiązków, działania zwiększające świadomość;
    4) przeprowadzanie okresowych szkoleń Personelu przetwarzającego dane osobowe oraz przygotowywanie materiałów szkoleniowych, ze szczególnym uwzględnieniem zmian w zakresie ochrony danych osobowych;
    5) przeprowadzanie szkoleń przed udzieleniem członkowi Personelu upoważnienia do przetwarzania danych osobowych;
    6) prowadzenie ewidencji szkoleń;
    7) prowadzenie Rejestru czynności przetwarzania, jeżeli taki obowiązek zaistnieje na podstawie przepisów prawa albo Inspektor uzna to za stosowne;
    8) prowadzenie Ewidencji zbioru danych, Ewidencji osób upoważnionych do przetwarzania danych osobowych;
    9) weryfikacja wzorów, szablonów, formularzy dokumentów wykorzystywanych przez Administratora Danych;
    10) nadawanie z upoważnienia Administratora Danych uprawnień do przetwarzania danych osobowych;
    11) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
    12) współpraca z Prezesem Urzędu Ochrony Danych Osobowych;
    13) pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
    14) udział w kontrolach prowadzonych przez Prezesa Urzędu Ochrony Danych Osobowych;

15) sprawowanie nadzoru nad wdrożeniem i funkcjonowaniem adekwatnych środków ochrony, w szczególności środków organizacyjnych i technicznych celem zapewnienia bezpieczeństwa przetwarzania danych osobowych;

16) sprawowanie nadzoru nad przeglądami, konserwacjami, uaktualnianiem, zmianą systemów, ze szczególnym uwzględnieniem systemów informatycznych, służących do przetwarzania danych osobowych i w tym zakresie współpracuje z Administratorem Systemu;

17) analiza okoliczności naruszenia bezpieczeństwa danych oraz przygotowanie i wdrożenie zmian zapobiegających wystąpieniu naruszeniom w przyszłości;

18) podejmowanie wraz z Administratorem Danych, Administratorem Systemu stosownych działań w przypadku stwierdzenia naruszenia lub podejrzenia naruszenia przetwarzania danych osobowych.

2.5. Podmiot Przetwarzający

1. Administrator Danych może powierzyć przetwarzanie danych osobowych podmiotowi zewnętrznemu, dającemu wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi przepisów prawa i chroniło prawa osób, których dane dotyczą.
2. Przed powierzeniem przetwarzania danych osobowych Inspektor dokonuje analizy statusu poszczególnych podmiotów w procesie przetwarzania danych osobowych.
3. Podmiot zewnętrzny, o którym mowa wyżej, zobowiązany jest wykorzystywać powierzone mu dane wyłącznie w celach i w zakresie wskazanych w umowie, jak również zachować poufność danych osobowych powierzonych do przetwarzania.
4. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy, która określa co najmniej:
   a) przedmiot i czas trwania przetwarzania;
   b) charakter i cel przetwarzania;
   c) rodzaj danych osobowych oraz kategorie osób, których dane dotyczą;
   d) obowiązki i prawa administratora.
5. Umowa powinna w szczególności określać, że Podmiot Przetwarzający:
   a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora Danych;
   b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;

c) podejmuje wszelkie środki techniczne i organizacyjne zapewniające stopień bezpieczeństwa odpowiadający temu ryzyku;

d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego;

e) pomaga w miarę możliwości Administratorowi Danych poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw;

f) pomaga Administratorowi Danych wywiązać się z obowiązków zapewnienia bezpieczeństwa przetwarzania poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych, zgłoszenia organowi nadzorczemu naruszenia ochrony danych osobowych, zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, konsultacji z organem nadzorczym;

g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora Danych usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;

h) udostępnia Administratorowi Danych wszelkie informacje niezbędne do wykazania spełnienia obowiązków w zakresie powierzenia oraz podpowierzenia przetwarzania danych osobowych oraz umożliwia Administratorowi Danych lub audytorowi upoważnionemu przez Administratora Danych przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

6. Z tytułu czynności wykonywanych w związku z zawarciem umowy powierzenia przetwarzania danych osobowych, Podmiotowi Przetwarzającemu nie przysługuje dodatkowe wynagrodzenie ponad to, które zostało określone w umowie głównej.

7. W związku z obowiązkiem określonym w ust. 5 lit. h) wyżej Podmiot Przetwarzający niezwłocznie informuje Administratora Danych, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie Rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

8. Jeżeli do wykonania w imieniu Administratora Danych konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy te same obowiązki ochrony danych jak w umowie między Administratorem Danych a Podmiotem Przetwarzającym, o których to obowiązkach mowa wyżej, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom Rozporządzenia.

9. Zawarcie umowy podpowierzenia przetwarzania danych osobowych wymaga dla swej ważności uprzedniej szczegółowej lub ogólnej zgody Administratora Danych na piśmie.
10. W przypadku wyrażenia przez Administratora Danych ogólnej pisemnej zgody na podpowierzenie przetwarzania danych, Podmiot Przetwarzający informuje Administratora Danych o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających. Administrator Danych niezwłocznie wyraża zgodę bądź sprzeciw w formie pisemnej.
11. Umowy, o których mowa wyżej mają formę pisemną, w tym formę elektroniczną.
12. W przypadku, gdy umowa główna z danym podmiotem zawiera elementy wskazane wyżej, dla powierzenia danych osobowych nie ma konieczności sporządzania dodatkowo pisemnej umowy o powierzenie przetwarzania danych osobowych.

2.6. Osoby upoważnione do przetwarzania danych osobowych

1. Każda osoba przetwarzająca dane osobowe jest zobowiązania do przestrzegania obowiązujących przepisów prawa, Polityki, Instrukcji, innych dokumentów o charakterze wewnętrznym, a także do utrzymania wysokiego poziomu bezpieczeństwa danych osobowych.
2. Każda osoba składa oświadczenie, że zapoznała się z obowiązującymi przepisami prawa dot. ochrony danych osobowych, Polityką, Instrukcją, innymi dokumentami o charakterze wewnętrznym, a także że zobowiązuje się do utrzymania wysokiego poziomu bezpieczeństwa danych osobowych.
3. Personel mający dostęp do danych osobowych nie może ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
4. W miejscu przetwarzania danych osobowych pracownicy zobowiązani są do stosowania zasady „czystego biurka" oraz „czystego ekranu".
5. Niszczenie nośników zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści.
6. Zabronione jest wynoszenie materiałów, nośników bez względu na formę, zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia.
7. Osoby nieuprawnione nie mogą przebywać w pomieszczeniu, w którym przetwarzane są dane osobowe, z wyjątkiem gdy w pomieszczeniu tym znajduje się osoba upoważniona do przetwarzania danych osobowych albo dane te są w odpowiedni sposób zabezpieczone przed dostępem.

8. Personel zobowiązany jest do stosowania wszelkich dostępnych zabezpieczeń pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe.
9. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każda osoba mająca dostęp do danych.
10. Osoba, która narusza obowiązujące przepisy w zakresie ochrony danych osobowych, postanowienia Polityki, Instrukcji lub innych aktów wewnętrznych ponosi odpowiedzialność przewidzianą w Kodeksie Pracy, ustawie o ochronie danych osobowych lub innych aktach prawnych w zależności od wagi i skutków naruszeń.
11. Upoważnienie do przetwarzania danych osobowych może wydawać Inspektor w imieniu Administratora.
12. Wniosek o wydanie oraz cofnięcie upoważnienie kierowany jest przez Wydział Kadr. Cofnięcie upoważnienia następuje w przypadku ustania stosunku prawnego pomiędzy członkiem Personelu a Administratorem Danych albo w przypadku stwierdzenia ciężkiego naruszenia podstawowych obowiązków dot. ochrony danych osobowych.
13. Ewidencję osób upoważnionych do przetwarzania prowadzi Inspektor.

3. Zasady przetwarzania danych osobowych

3.1. Wprowadzenie

Dane osobowe przetwarzane są zgodnie z następującymi zasadami:

1. legalności;
2. celowości;
3. adekwatności;
4. prawidłowości;
5. retencji danych;
6. integralności;
7. rozliczalności.

Administrator Danych dołoży wszelkich starań, aby wszelkie procesy przetwarzania danych osobowych były zgodne ze wszystkimi zasadami przetwarzania łącznie. Naruszenie którejkolwiek z zasad, prowadzi do przetwarzania danych osobowych niezgodnie z prawem.

3.2. Zasada zgodności z prawem

1. Przetwarzanie jest zgodne z prawem wyłącznie w zakresie, w jakim spełniony jest co najmniej jeden z poniższych warunków:

1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

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 nałożonego przepisem prawa na Administratora Danych;

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 na podstawie przepisów prawa Administratorowi Danych;

6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora Danych lub przez stronę trzecią, 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. Jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani przepisów prawa, aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane należy wziąć pod uwagę między innymi:

   1) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania;

   2) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą a Administratorem Danych;

   3) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa;

   4) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą;

   5) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.

3. Przetwarzanie szczególnych kategorii danych osobowych uważa się za zgodne z prawem, wyłącznie w przypadkach i zakresie, w jakim 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 prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu przetwarzania danych wrażliwych;

2) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora Danych lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;

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;

4) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;

5) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

6) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

7) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;

8) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia;

9) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, na podstawie prawa Unii

lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

3.3. Zasada celowości

1. Zbieranie danych osobowych jest dokonywane wyłącznie dla oznaczonych celów.
2. Zabrania się przetwarzania danych osobowych do celów innych niż cele, w których dane te zostały pierwotnie zebrane.
3. W sytuacji, gdy przetwarzanie danych osobowych będzie odbywało się w nowym celu, nieznanym dla osoby fizycznej, należy o nim poinformować osobę fizyczną i upewnić się, że istnieje do niego podstawa prawna.
4. Dalsze przetwarzanie danych osobowych lub szczególnych kategorii danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych uznawane jest za operacje przetwarzania zgodne z prawem i z pierwotnymi celami, jednak z poszanowaniem zasady adekwatności.

3.4. Zasada adekwatności

1. Dane osobowe zbierane przez Administratora Danych powinny być adekwatne i stosowne do celów, w których są przetwarzane.
2. Inspektor jest informowany o każdej inicjatywie, w ramach której przetwarzane są dane osobowe celem weryfikacji zakresu zbieranych danych.
3. Adekwatność danych powinna być oceniona przed zebraniem danych osobowych.
4. Pozyskiwanie danych, które nie są potrzebne jest zabronione.

3.5. Zasada prawidłowości

1. Dane osobowe przetwarzane przez Administratora Danych muszą być prawidłowe.
2. Administrator Danych aktualizuje przetwarzane dane osobowe, w szczególności na żądanie osoby, której dane dotyczą.

3.6. Zasada retencji danych

1. Dane osobowe są przetwarzane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.
2. W sytuacji, gdy przepisy prawa nie ustanawiają okresu przechowywania danych, przechowywanie następuje z uwzględnieniem praw jednostki oraz funkcji pełnionych przez Administratora Danych.

3. Okresy przechowywania danych osobowych zawarte są w Rejestrze czynności przetwarzania.

3.7. Zasada integralności

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 Danych w fazie planowania jak i w czasie przetwarzania wdraża odpowiednie środki techniczne i organizacyjne zapewniające ochronę danych.

3.8. Zasada rozliczalności

Przetwarzanie danych osobowych odbywa się w sposób udokumentowany, w szczególności pozwalający na wykazanie przestrzegania przepisów prawa dot. ochrony danych osobowych.

4. Opis środków technicznych i organizacyjnych

4.1. Wprowadzenie

Zastosowane środki ochrony powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, zbiorów i kategorii danych osobowych.

Administrator Danych wprowadził środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

4.2. Środki techniczne

1. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
2. Dostęp do urządzeń, na których znajdują się dane osobowe, zabezpieczony jest przy pomocy haseł dostępu.
3. Ochrona sprzętu komputerowego i urządzeń podobnych przed złośliwym oprogramowaniem.
4. Wykonywanie kopii awaryjnych danych ze stosowną częstotliwością.
5. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

4.3. Środki organizacyjne

1. Została opracowana i wdrożona Polityka Bezpieczeństwa oraz Instrukcja, które podlegają okresowej aktualizacji.
2. Do przetwarzania danych zostały dopuszczone wyłącznie osoby, które:

1) wzięły udział w szkoleniu w zakresie ochrony danych osobowych z uwzględnieniem m.in. zagadnień: zagrożenia bezpieczeństwa informacji, skutków naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, stosowanie środków zapewniających bezpieczeństwo informacji;
2) uzyskały upoważnienie do przetwarzania danych i złożyły oświadczenie o zachowaniu tajemnicy.

3. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności członka Personelu bądź w warunkach zapewniających bezpieczeństwo danych.
4. Stanowiska pracy osób przetwarzających dane są usytuowane w taki sposób, że uniemożliwiono bądź ograniczono możliwość wglądu w dane osób nieuprawnionych.
5. Prowadzona jest i aktualizowana inwentaryzacja sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.
6. Kopie zapasowe zbioru danych osobowych przechowywane są, co do zasady, w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.
7. Powierzenie przetwarzania danych osobowych podmiotom zewnętrznym odbywa się na podstawie umowy w formie pisemnej (w tym elektronicznej).
8. Zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez monitorowanie dostępu do informacji, czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem danych.
9. Zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.
10. Ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.
11. Zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.
12. Bezzwłoczne zgłaszanie Administratorowi Danych lub Inspektorowi incydentów naruszenia bezpieczeństwa informacji umożliwiający szybkie podjęcie działań korygujących.
13. Zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
14. Pomieszczenia, w których przetwarzane są dane osobowe objęte są kontrolą dostępu (np. zamki na klucz). Klucze od biurek służbowych, szaf biurowych, drzwi do pomieszczeń są w posiadaniu osobistym pracowników, którzy ponoszą odpowiedzialność za ich zabezpieczenie.

15. Obszary, w których przetwarzane są dane osobowe zabezpieczone są systemem przeciwpożarowym.
16. Zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej szafie niemetalowej lub metalowej bądź biurku.
17. Papierowe nośniki danych osobowych niszczone są w sposób mechaniczny przy użyciu niszczarek dokumentów lub w inny sposób uniemożliwiający ich odtworzenie.

5. Kontrola dostępu

5.1. Wprowadzenie

Celem procedury jest zapewnienie właściwej kontroli dostępu do budynków i pomieszczeń, jak również do systemów informatycznych.

5.2. Opis kontroli dostępu

1. Jakikolwiek dostęp do informacji jest projektowany zgodnie z zasadą: „wszystko jest zabronione, dopóki nie jest wyraźnie dozwolone".
2. Członek Personelu posiada dostęp tylko do takich zasobów, jakie są mu niezbędne do wykonywania obowiązków służbowych i odpowiadający jego zakresowi obowiązków.
3. Dostęp do informacji oraz systemów możliwy jest tylko dla uprawnionych członków Personelu.
4. Sposób uzyskiwania dostępu do systemów informatycznych, zabezpieczenia oraz pozostałe kwestie związane z dostępem reguluje Instrukcja.
5. Administrator Danych wykonuje przeglądy dostępu nie rzadziej niż raz na 12 miesięcy oraz każdorazowo w uzasadnionych przypadkach.
6. Kontrolę dostępu stosuje się m.in. do:
    1) danych osobowych przetwarzanych w systemie informatycznym;
    2) wszystkich informacji dotyczących danych Personelu, w tym danych osobowych Personelu i treści zawieranych umów o pracę oraz innych umów cywilnoprawnych;
    3) wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji;
    4) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych;
    5) rejestru osób dopuszczonych do przetwarzania danych osobowych;
    6) innych dokumentów zawierających dane osobowe.
7. Zakresy określone przez kontrolę dostępu mają zastosowanie do całego Systemu informatycznego w szczególności do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie;
2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
3) personelu i innych osób mających dostęp do informacji podlegających ochronie.

8. Podstawowe założenia kontroli dostępu:
   1) wszelka dokumentacja zawierająca dane osobowe powinna być przechowywana w szafach lub biurkach stanowiskowych zamykanych na klucz, a w wersji elektronicznej na odpowiednim dysku;
   2) obszar przetwarzania i gromadzenia danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych (drzwi zamykane na klucz, hasła dostępu do stacji roboczych, itp.);
   3) przebywanie osób nieupoważnionych bez nadzoru w obszarze przetwarzania danych jest zabronione;
   4) członek Personelu może posiadać dostęp tylko do zasobów, jakie są mu niezbędne do wykonywania obowiązków służbowych – dostęp musi odpowiadać jego zakresowi obowiązków;
   5) dostęp do systemów informatycznych możliwy jest tylko dla uprawnionych Użytkowników, posługujących się unikatowym loginem, dzięki któremu można jednoznacznie zidentyfikować osobę;
   6) do poprawnego uwierzytelnienia, wymagane jest użycie poprawnego loginu oraz hasła, zgodnie z zapisami Instrukcji;
   7) dostęp do poszczególnych informacji ograniczany jest dla poszczególnych grup członków Personelu, dopuszczalne jest także nadawanie szczególnych uprawnień poszczególnym członkom Personelu z zachowaniem zasady, o której mowa w punkcie następnym;
   8) dostęp do informacji w systemach informatycznych powinien być projektowany zgodnie z zasadą: „wszystko jest zabronione, dopóki nie jest wyraźnie dozwolone”;
   9) każdy nowy członek Personelu otrzymuje minimalne uprawnienia dostępu do Systemu informatycznego, niezbędne do rozpoczęcia pracy (m.in. dostęp do systemu operacyjnego, do imiennej poczty e-mail, do sieci informatycznej);
   10) w sytuacjach, gdy w zakresie obowiązków członka Personelu znajduje się przetwarzanie danych osobowych, niezbędne jest upoważnienie do przetwarzania danych osobowych.
9. Nadanie uprawnień nowemu członkowi Personelu możliwe jest po spełnieniu łącznie następujących warunków:

1) zakończeniu procesu rekrutacji i zawarciu umowy o pracę, o staż lub umowy cywilnoprawnej lub umowy o współpracę;

2) przeszkoleniu członka Personelu przez Inspektora oraz złożeniu przez członka Personelu oświadczeń, w których zobowiąże się on do przetwarzania danych osobowych zgodnie z przepisami prawa oraz zapisami niniejszej Polityki oraz innych dokumentów wewnętrznych.

10. Członkowi Personelu należy zapewnić dostęp tylko do tych usług, do których mają określoną autoryzację.
11. Członek Personelu ma umożliwiony dostęp do platformy wewnętrznej, sieci lokalnej, do której podłączone są stacje robocze innych członków Personelu, drukarki sieciowe oraz dyski sieciowe. Dostęp nadawany jest zgodnie z postanowieniami Instrukcji.
12. Każde urządzenie członka Personelu (np. stacja robocza) ma przydzielany unikatowy adres IP.
13. Upoważnienie wygasa w przypadku:

    1) ustania stosunku pracy bądź innego stosunku prawnego łączącego osobę upoważnioną z Administratorem Danych;

    2) zmiany zakresu przetwarzania danych osobowych w związku ze zmianą stanowiska pracy;

    3) ustania obowiązków związanych z przetwarzaniem danych osobowych;

    4) odebrania uprawnienia w związku z umyślnym naruszeniem zasad ochrony danych osobowych.

14. Dokument upoważnienia jest przechowywany w aktach osobowych pracownika bądź osoby niebędącej pracownikiem w rozumieniu Kodeksu pracy.
15. Ewidencja upoważnień do przetwarzania danych osobowych zawiera w szczególności:

    1) imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych;

    2) stanowisko;

    3) zakres upoważnienia do przetwarzania danych osobowych;

    4) identyfikator w przypadku rejestracji osoby upoważnionej w systemie informatycznym wykorzystywanym do przetwarzania danych osobowych (jeśli dotyczy),

    5) data nadania i wygaśnięcia upoważnienia.

16. W przypadku wygaśnięcia upoważnienia do przetwarzania danych osobowych Administrator Danych podejmuje stosowne działania mające na celu wyeliminowanie niebezpieczeństwa naruszenia ochrony danych.
17. Osoba upoważniona przez Administratora Danych informuje Administratora Danych lub Inspektora o następujących zmianach:

1) przyjęciu nowego członka personelu;
2) odejściu członka personelu;
3) rozpoczęciu urlopu macierzyńskiego/wychowawczego oraz informację nt. powrotu z tego urlopu;
4) rozpoczęciu i powrocie z długoterminowego zwolnienia lekarskiego;
5) rozpoczęcie i powrót z dłuższej niż 30 dni kalendarzowych nieobecności;
6) zmianie stanowiska lub komórki organizacyjnej, z którą wiąże się inny zakres uprawnień.

18. W przypadku przetwarzania danych osobowych w sposób rażąco sprzeczny z przyjętymi zasadami i procedurami, można rozwiązać umowę o pracę bez wypowiedzenia z winy członka Personelu. Powyższe ma odpowiednie zastosowanie do pozostałych członków Personelu.
19. Personel obowiązuje polityka czystego ekranu dla środków przetwarzania informacji.
20. Zgodnie z polityką czystego ekranu, każdy członek Personelu jest zobowiązany do:
    1) zabezpieczenia swojego systemu informatycznego przed nieuprawnionym dostępem innych osób poprzez wprowadzenie indywidualnego hasła dostępu;
    2) nieprzechowywania na ekranie głównym Stacji roboczej plików zawierających dane osobowe;
    3) wylogowania oraz zablokowania dostępu do systemu informatycznego po zakończeniu swojej pracy i przed opuszczeniem miejsca pracy.
21. Członek Personelu zapewnia odpowiednią ochronę Stacji roboczej pozostawionej bez opieki. Członek Personelu pozostawiający sprzęt bez opieki (np.: wyjście z pokoju) powinien:
    1) zablokować możliwość korzystania ze Stacji roboczej, np. poprzez włączenie wygaszacza ekranu chronionego hasłem, „uśpienie" Stacji roboczej lub wyłączenie sprzętu;
    2) po zakończonej pracy w systemie informatycznym wylogować się z systemu i wyłączyć Stację roboczą.
22. Przydzielanie haseł do Systemu informatycznego odbywa się zgodnie z Instrukcją. Podczas używania haseł członkowie Personelu powinni postępować zgodnie ze sprawdzonymi praktykami bezpieczeństwa oraz wskazówkami zawartymi w Instrukcji.
23. O ile to konieczne, należy opracować i wdrożyć politykę, plany operacyjne i procedury dla czynności wykonywanych w ramach pracy na odległość.
24. Członkowie Personelu przetwarzający dane osobowe na urządzeniach przenośnych zobligowani są do:

1) stosowania środków ochrony wobec przetwarzanych danych osobowych zlokalizowanych na dyskach urządzeń przenośnych;
2) zachowania szczególnej ostrożności podczas transportu, przechowywania i użytkowania urządzenia przenośnego;
3) stosowania zakazu pozostawiania urządzenia przenośnego w samochodzie, oddawania do przechowalni bagażu, itp.;
4) użytkowania urządzenia w taki sposób, aby zminimalizować ryzyko wglądu w wyświetlane na urządzeniu dane osobowe przez osoby nieuprawnione bez względu na miejsce, w którym korzysta z urządzenia przenośnego;
5) stosowania zakazu udostępniania urządzenia zawierającego dane osobowe osobom nieuprawnionym;
6) niezwłocznego zawiadomienia Administratora Danych lub wyznaczonego podmiotu o ewentualnej kradzieży, zagubieniu, przypadkowej utracie, uszkodzeniu bądź zniszczeniu urządzenia przenośnego.

25. Urządzenia, dyski lub inne elektroniczne nośniki informacji, które zawierają dane osobowe, przeznaczone do:
    a) likwidacji - pozbawia się zapisu tych danych, a w przypadku braku możliwości usunięcia danych uszkadza się w sposób uniemożliwiający ich odczytanie;
    b) naprawy – w zależności od okoliczności pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.
26. Nie tworzy się plików o charakterze baz danych (np. pliku excel) bez uzasadnionych powodów.
27. Plik zawierający dane osobowe powinien być zabezpieczony przed wysłaniem poprzez zaszyfrowanie hasłem. Hasło należy przesłać odbiorcy pliku inną drogą komunikacji.
28. Zabronione jest podłączanie do służbowego sprzętu obcych nośników danych.
29. Członkowie Personelu zobowiązani są do przesyłania elektronicznej korespondencji służbowej wyłącznie za pośrednictwem skrzynki pocztowej Administratora Danych.
30. W przypadku przesyłania korespondencji elektronicznej należy ukrywać listę innych odbiorców poprzez wpisywanie adresu w polu UDW lub BCC.
31. Dostęp do budynków, pomieszczeń i powierzchni zabezpieczonych kluczem i/lub kartami dostępu możliwy jest wyłącznie przez upoważniony Personel, który posiada klucz i/lub kartę dostępu.
32. Każdy członek Personelu jest w ciągłym posiadaniu kluczy i/lub kart dostępu i ponosi pełną odpowiedzialność za ich zabezpieczenie.

33. Każdorazowo przydzielając klucz i/lub kartę dostępu należy odnotować ten fakt w protokole przekazania, podpisanym przez Inspektora lub osobę upoważnioną.
34. W zakresie procedury postępowania z hasłami dostępu stosuje się postanowienia Instrukcji służące do przetwarzania danych osobowych.
35. Dostęp do poszczególnych pomieszczeń zabezpieczony jest kluczem i/lub kartą dostępu.
36. Przed przystąpieniem do pracy należy sprawdzić stan zabezpieczeń, a także przechowywanej dokumentacji i innego wyposażenia.
37. W przypadku stwierdzenia naruszenia zabezpieczeń, każdy członek Personelu jest zobowiązany niezwłocznie zgłosić ten fakt Administratorowi Danych lub Inspektorowi i powstrzymać się od przystąpienia do pracy, do czasu wyrażenia zgody przez Administratora Danych. Fakt naruszenia lub osoba upoważniona odnotowuje w notatce służbowej.
38. W przypadku zgubienia lub zniszczenia klucza i/lub karty dostępu przez osobę uprawnioną, fakt ten należy niezwłocznie zgłosić Administratorowi lub Inspektorowi. Administrator Danych odnotowuje ten fakt w notatce służbowej i niezwłocznie blokuje kartę dostępu, jednocześnie rozpoczynając procedurę wydania nowej karty dostępu. Przed wydaniem klucza Administratora Danych lub osoba upoważniona podejmuje decyzję o wymianie zamka.
39. Na czas nieobecności osoby uprawnionej, wejście do poszczególnych pomieszczeń każdorazowo zamykane jest na klucz lub kodowane kartą dostępu.
40. Po zakończeniu pracy pomieszczenia zamykane są na klucz lub kodowane są kartą dostępu.
41. Zabrania się:
    a) dorabiania kluczy/kart dostępu,
    b) udostępniania kluczy/kart dostępu osobom nieuprawnionym,
    c) pozostawiania otwartych i niezabezpieczonych pomieszczeń, bez nadzoru osoby uprawnionej.
42. Dostęp do szafek i urządzeń biurowych w poszczególnych pomieszczeniach, w których przechowywane są dane osobowe, zabezpieczony jest kluczem.
43. Klucz znajduje się w posiadaniu członka Personelu, którego stanowisko pracy znajduje się w poszczególnych pomieszczeniach.
44. W przypadku opuszczenia stanowiska pracy/zakończenia pracy, dostęp do szafek i urządzeń zostaje zablokowany poprzez ich zamknięcie.
45. Każdy klucz lub karta dostępu musi być opisana i możliwa do identyfikacji.
46. Naruszenie bezpieczeństwa ochrony danych osobowych może nastąpić w wyniku:

a) niewłaściwego działania oraz nieprzestrzegania zasad ochrony danych osobowych przez Personel (zarówno w wyniku działań umyślnych jak i nieumyślnych);

b) niewłaściwego zabezpieczenia pomieszczeń, sprzętu IT, sprzętu elektronicznego, urządzeń zewnętrznych oraz dokumentów;

c) niepożądanego działania osób trzecich odpowiedzialnych za zakłócenie systemu ochrony danych osobowych w związku z nieautoryzowanym dostępem, w szczególności kradzież danych, bądź potencjalne ślady próby kradzieży, zgubienie sprzętu lub nośników danych, utrata zasilania powodująca przerwę w pracy systemów;

d) oddziaływania czynników zewnętrznych (tj. pożar, wilgotność, zalanie, niewłaściwa temperatura otoczenia, itp.).

47. Naruszenie bezpieczeństwa danych osobowych ustala się poprzez:

a) ocenę wyglądu zewnętrznego pomieszczeń oraz stanu urządzeń technicznych;

b) ocenę kompletności i zawartości przetwarzanych zbiorów danych osobowych;

c) identyfikację dostępu do zabezpieczeń oraz dokumentów przez osoby nieautoryzowane;

d) ocenę procesu modyfikacji, zniszczenia i ujawnienia danych osobowych.

48. Zawiadomienie Administratora Danych o naruszeniu bądź wystąpieniu niebezpieczeństwa sporządza się tak, aby zostało złożone w sposób skuteczny i uwzględniało jak najwięcej informacji odnośnie zdarzenia.

49. Zawiadomienie powinno zawierać co najmniej:

a) datę i godzinę wystąpienia zdarzenia/powzięcia informacji o zdarzeniu;

b) imię, nazwisko oraz podpis osoby zawiadamiającej;

c) określenie sytuacji, w której stwierdzono naruszenie bezpieczeństwa ochrony danych osobowych oraz charakteru naruszenia;

d) wskazanie przyczyny wystąpienia naruszenia bezpieczeństwa ochrony danych osobowych;

e) opis sytuacji oraz symptomów wskazujących na naruszenie;

f) opis zabezpieczeń stosowanych w przypadku konkretnego naruszenia;

g) opis działań podjętych w związku z wystąpieniem zdarzenia.

50. Każda osoba zawiadamiająca do momentu przybycia Administratora Danych lub Inspektora, powinna zabezpieczyć miejsce zdarzenia oraz powstrzymać się od jakichkolwiek działań uniemożliwiających identyfikację lub uzyskanie dowodów naruszenia oraz powodujących zatarcie śladów.

51. W ramach polityki czystego biurka, Personel zobowiązany jest do:

    a) niepozostawiania w widocznym i łatwo dostępnym miejscu jakiejkolwiek dokumentacji zawierającej dane osobowe w przypadku każdorazowego opuszczenia swojego stanowiska pracy;

    b) niepozostawiania w miejscu pracy dokumentów zawierających hasła dostępu do Stacji roboczej lub Systemu informatycznego;

    c) niepozostawiania w miejscu pracy pamięci USB zawierających dane bez stosownego zabezpieczenia;

    d) odbioru drukowanych bądź kserowanych dokumentów niezwłocznie po wykonaniu przez urządzenie biurowe zleconego zadania;

    e) usunięcia ze swojego stanowiska pracy wszelkich dokumentów zawierających dane osobowe niezwłocznie po zakończeniu swojej pracy i przed opuszczeniem miejsca pracy. Wówczas, wszelka dokumentacja zawierająca dane osobowe powinna być przechowywana w zamykanej na klucz szafce, do której dostęp posiada wyłącznie członek Personelu oraz inne osoby do tego uprawnione na mocy stosownych zapisów Polityki lub odpowiednich upoważnień;

    f) zniszczenia wszelkiej niepotrzebnej do dalszej pracy dokumentacji zawierającej dane osobowe;

    g) wykorzystywania swojego stanowiska pracy wyłącznie do celów związanych z realizacją obowiązków służbowych.

52. W przypadku stwierdzenia naruszenia bezpieczeństwa ochrony danych osobowych, Administrator Danych podejmuje działania zmierzające do usunięcia powstałego zagrożenia oraz wyjaśnienia okoliczności naruszenia i minimalizacji jego negatywnych konsekwencji w celu zapewnienia bezpiecznego dalszego przetwarzania danych osobowych.

53. Postępowanie wyjaśniające opiera się w szczególności na:

    a) ocenie sytuacji oraz identyfikacji zakresu naruszenia;

    b) ocenie ewentualnych skutków naruszenia;

    c) przesłuchaniu osób zawiadamiających oraz świadków zdarzenia;

    d) zabezpieczeniu ewentualnych dowodów naruszenia;

    e) podjęciu działań mających na celu ustalenie przyczyny/sprawcy naruszenia;

    f) podjęciu ewentualnych działań dyscyplinujących.

54. Administrator Danych podejmuje działania mające na celu ochronę danych osobowych przetwarzanych w formie elektronicznej, w tym:

a) blokuje dostęp do pomieszczeń, sieci oraz urządzeń, które mogą być przyczyną naruszenia i uzyskania dostępu osób nieautoryzowanych;

b) niezwłocznie kończy działalnie aplikacji i programów, które mogą być przyczyną naruszenia i uzyskania dostępu osób nieautoryzowanych;

c) jeżeli przyczyną naruszenia było działanie członka Personelu blokuje dostęp do sieci poprzez wylogowanie użytkownika i zmianę hasła dostępu;

d) podejmuje próbę odtworzenia zagrożonych danych osobowych z utworzonej kopii zapasowej/awaryjnej.

55. Administrator Danych podejmuje działania mające na celu ochronę danych osobowych przetwarzanych w formie dokumentacji papierowej, w tym:

a) blokuje dostęp do pomieszczeń, w których przetwarzane są te dane;

b) zabezpiecza dokumenty oraz ich kopie, do których dostęp mogły uzyskać osoby nieautoryzowane;

c) zabezpiecza dokumenty oraz ich kopie, które zostały częściowo/niewłaściwie zniszczone;

d) zaprzestaje kopiowania dokumentów, które mogą być przyczyną naruszenia i uzyskania dostępu osób nieautoryzowanych;

e) wzywa do opuszczenia pomieszczeń osoby nieautoryzowane lub odpowiedzialne za naruszenie bezpieczeństwa ochrony danych osobowych.

56. Administrator Danych może także podejmować działania polegające na tymczasowej reorganizacji pracy, w tym nakazać jej przerwania oraz żądać dodatkowych wyjaśnień, jeżeli jest to niezbędne do zapewnienia bezpieczeństwa danych osobowych. Odmowa złożenia wyjaśnień stanowi naruszenie obowiązków pracowniczych.

57. Jeżeli naruszenie bezpieczeństwa ochrony danych osobowych związane było z dostępem do systemu informatycznego, Administrator Danych zobowiązany jest niezwłocznie powiadomić Administratora Systemu.

58. Kontynuowanie przetwarzania danych osobowych oraz ponowne podjęcie pracy jest możliwe wyłącznie po uzyskaniu zgody Administratora Danych.

59. Dalsze przetwarzanie danych osobowych lub podjęcie pracy bez zgody, o której mowa wyżej możliwe jest wyłącznie w przypadku konieczności ratowania osób, mienia lub zapobiegania wystąpieniu innego niebezpieczeństwa lub dalszego wycieku danych osobowych.

60. Administrator Danych dokonuje zarejestrowania naruszenia lub zawiadomienia o naruszeniu w rejestrze zawiadomień.

61. W przypadku stwierdzenia naruszenia bezpieczeństwa ochrony danych osobowych Administrator Danych, Inspektor bądź osoba do tego upoważniona bez zbędnej zwłoki zgłasza je Urzędowi, chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

62. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator Danych bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

63. Administrator Danych może zaniechać zawiadomienia o naruszeniu osoby, której dane dotyczą, jeżeli:

    a) Administrator Danych wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

    b) Administrator Danych zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;

    c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

64. W przypadku wystąpienia zdarzeń powodujących naruszenie bezpieczeństwa ochrony danych osobowych Administrator Danych podejmuje postępowanie zabezpieczające w celu wyeliminowania wystąpienia sytuacji naruszenia bezpieczeństwa ochrony danych osobowych w przyszłości.

65. Postępowanie zabezpieczające obejmuje:

    a) podjęcie działań dyscyplinujących, jeżeli przyczyną naruszenia było działanie członka Personelu;

    b) podjęcie działań mających na celu weryfikację i udoskonalenie systemu zabezpieczeń, jeżeli przyczyną naruszenia było niewłaściwe zabezpieczenie pomieszczeń, sprzętu IT, sprzętu elektronicznego, urządzeń zewnętrznych oraz dokumentów;

    c) przeprowadzenie dodatkowego szkolenia dla Personelu, jeżeli przyczyną było niewłaściwe przetwarzane danych osobowych przez osoby upoważnione.

66. Postępowanie zabezpieczające należy przeprowadzić niezwłocznie po wystąpieniu zdarzeń powodujących naruszenie ochrony danych osobowych. Jeżeli postępowanie związane jest z przeprowadzeniem szkolenia, o którym mowa wyżej należy przeprowadzić je w terminie 7 dni od dnia wystąpienia naruszenia.

67. W celu zapewnienia poprawnego funkcjonowania systemu ochrony danych osobowych Administrator Danych może przeprowadzać dodatkowe kontrole, których wynik dokumentuje w notatce służbowej.

68. Nieprzestrzeganie obowiązków określonych w części Kontrola Dostępu stanowi naruszenie obowiązków pracowniczych i może być podstawą pociągnięcia członka Personelu do odpowiedzialności dyscyplinarnej określonej na podstawie przepisów Kodeksu Pracy oraz innej odpowiedzialności określonej przepisami prawa.

6. Obsługa praw jednostek

6.1. Wprowadzenie

1. Administrator Danych zapewnia realizację praw jednostek, których dane przetwarza, wobec wytycznych określonych w Rozporządzeniu, tj.:
   1) prawa do dostępu do danych;
   2) prawa do sprostowania danych;
   3) prawa do usunięcia danych;
   4) prawa do ograniczenia przetwarzania;
   5) prawa do przenoszenia danych;
   6) prawa do sprzeciwu;
   7) prawa do cofnięcia zgody.
2. Administrator Danych w szczególności:
   1) przekazuje osobom wymaganych prawem informacji wobec pozyskiwania danych;
   2) zapewnienie możliwość efektywnego rozpatrzenia żądania osoby, której dane dotyczą, przez wyznaczonego Inspektora Ochrony Danych;
   3) stosuje procedury zapewniające bezpieczeństwo przetwarzanych danych.
3. Administrator Danych pozyskując dane osobowe bezpośrednio od osoby, której dotyczą, wypełnia w trakcie pozyskiwania danych obowiązek informacyjny, o którym mowa wyżej.
4. Obowiązek informacyjny realizowany jest także wtedy, gdy:
   1) dane osobowe zbierane są z innego źródła niż osoba, której dotyczą;
   2) zmieniają się cele przetwarzania danych lub dodaje się nowy cel przetwarzania;
   3) realizuje się żądanie dostępu do danych.

6.2. Inspektor Ochrony Danych

1. Żądania osób fizycznych w zakresie realizacji praw wskazanych wyżej powinny być kierowane do Inspektora (jeśli został powołany) drogą pisemną.
2. Zabrania się członkom Personelu udzielania odpowiedzi w zakresie ochrony danych osobowych.
3. Członkowie Personelu są zobowiązani do udzielania niezwłocznie Inspektorowi wszelkich informacji celem rozpoznania zgłoszenia.
4. Członkowie Personelu są zobowiązani do współpracy z Inspektorem po pozytywnym rozpatrzeniu żądania osoby, której dane dotyczą.
5. Zgłoszenie żądania powinno zawierać:
    1) dane osoby (imię i nazwisko), której zgłoszenie dotyczy oraz osoby zgłaszającej;
    2) opis zgłaszanego żądania wraz ze wskazaniem ewentualnych zastrzeżeń;
    3) pełnomocnictwo, jeśli w imieniu zgłaszającego żądanie działa pełnomocnik.
6. W przypadku zgłoszenia, które jest niepełne, niejasne, Inspektor podejmuje działania celem uzyskania pełnych informacji dot. zgłoszenia.
7. Inspektor wdrożył środki organizacyjne i techniczne zapewniające realizację praw jednostki bez zbędnej zwłoki, tj. nie później niż w terminie jednego miesiąca od otrzymania zgłoszenia żądania.
8. W przypadku wysoce skomplikowanego żądania, tym samym konieczności podjęcia dalece absorbujących czynności przez Inspektora lub także w przypadku znacznej liczby zgłoszonych żądań, Inspektor w terminie jednego miesiąca od otrzymania zgłoszenia żądania, poinformuje zgłaszającego o zakładanym terminie zakończenia czynności oraz wydania decyzji wraz z podaniem przyczyn opóźnienia.
9. Inspektor udzielając odpowiedzi na zgłoszenie informuje zgłaszającego o możliwości wniesienia skargi do Urzędu Ochrony Danych Osobowych oraz skorzystania ze środków ochrony prawnej przed sądem.
10. Inspektor dokumentuje czynności podjęte w związku ze zgłoszeniem.

6.3. Prawo do dostępu do danych

1. Administrator Danych zapewnia realizację prawa dostępu do danych i do informacji o danych na wniosek osoby, której dane dotyczą, poprzez umożliwienie dostępu do danych, przygotowanie kopii danych podlegających przetwarzaniu i przekazanie informacji o:
    1) celu przetwarzania i kategorii przetwarzanych danych;

2) okresie, przez który dane mają być przechowywane, a gdy podanie go nie będzie możliwe, kryteriach ustalania tego okresu;

3) przysługujących podmiotowi danych uprawnieniach do żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania jej danych, wniesienia sprzeciwu wobec przetwarzania, a także wniesienia skargi do organu Urzędu;

4) źródle pozyskania danych osobowych danej osoby jeśli nie zostały zebrane od osoby, której dane dotyczą;

5) podejmowaniu przez Administratora Danych zautomatyzowanych decyzji, w tym m.in. w oparciu o profilowanie, a jeśli tak, to również informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;

6) ujawnieniu (obecnym, bądź przyszłym/planowanym) danych odbiorcom danych, a jeśli tak, to również informacje o tych odbiorcach i o odpowiednich zabezpieczeniach związanych z ich przekazaniem.

6.4. Prawo do sprostowania danych

1. Prawo do sprostowania danych obejmuje:
   1) żądanie poprawienia nieprawidłowych danych;
   2) żądanie uzupełnienia niekompletnych danych;
   3) żądanie aktualizacji danych.
2. Administrator Danych, Inspektor lub inna osoba upoważniona weryfikuje, czy żądanie sprostowania danych nie prowadzi do ujawnienia danych nieprawidłowych lub nie prowadzi do nadmierności zbieranych danych.
3. W przypadku stwierdzenia jednej z powyższej przesłanek Administrator Danych może odmówić spełnienia żądania.
4. Wobec dokonania sprostowania danych Administrator Danych poinformuje o tym odbiorców danych, którym ujawnił przedmiotowe dane osobowe.

6.5. Prawo do usunięcia danych

1. Prawo do usunięcia danych obejmuje:
   1) prawo do żądania usunięcia danych;
   2) prawo do bycia zapomnianym – w przypadku upublicznienia danych przez Administratora Danych;
2. Osoba, której dane dotyczą ma prawo żądać usunięcia danych jeżeli:

1) dane są niekompletne, nieaktualne, nieprawdziwe;

2) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

3) cofnęła ona zgodę, na podstawie której opierało się przetwarzanie i nie ma innej podstawy do tego, aby dane te dalej przetwarzać;

4) dane osobowe były przetwarzane niezgodnie z prawem;

5) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator.

3. Administrator może odmówić spełnienia żądania realizacji prawa do usunięcia danych, w szczególności:

   1) do korzystania z prawa do wolności wypowiedzi i informacji;

   2) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega Administrator Danych, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

   3) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 Rozporządzenia, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1 Rozporządzenia, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub

   4) do ustalenia, dochodzenia lub obrony roszczeń.

4. Wystąpienie chociażby jednej przesłanki określonej wyżej prowadzi do odmowy uwzględnienia żądania.

6.6. Prawo do ograniczenia przetwarzania

1. Osoba fizyczna, której dane dotyczą, ma prawo żądać ograniczenia przetwarzania w następujących przypadkach:

   1) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający Administratorowi sprawdzić prawidłowość tych danych;

   2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;

   3) Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

4) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 Rozporządzenia wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

2. W przypadku uwzględnienia żądania ograniczenia przetwarzania Administrator Danych może je przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

6.7. Prawo do przenoszenia danych

1. Prawo jednostki do przenoszenia danych, które jej dotyczą, obejmuje:
   1) prawo do otrzymania przez nią od Administratora Danych, przedmiotowych danych w powszechnie używanym formacie;
   2) prawo do żądania przesłania danych bezpośrednio pomiędzy Administratorem Danych do innego administratora wskazanego przez osobę, której dane dotyczą, w przypadkach określonych w Rozporządzeniu.
2. Prawo do przenoszenia danych przysługuje jedynie w przypadku, gdy przetwarzanie danych odbywa się na podstawie zgody osoby fizycznej lub umowy oraz w sposób zautomatyzowany.

6.8. Prawo do sprzeciwu

1. Osoba, której dane są przetwarzane, ma prawo w dowolnym momencie i z przyczyn związanych z jej szczególną sytuacją wnieść sprzeciw wobec przetwarzania danych osobowych, wobec przetwarzania danych:
   1) do wykonania zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi Danych;
   2) do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora Danych.
2. Po skutecznym wniesieniu sprzeciwu, Administratorowi Danych nie wolno już przetwarzać ww. danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

6.9. Prawo do cofnięcia zgody

1. W przypadku, gdy podstawą przetwarzania danych osobowych jest zgoda osoby fizycznej, osoba fizyczna ma prawo w dowolnym momencie cofnąć zgodę na przetwarzanie danych osobowych.

2. Cofnięcie zgody nie wpływa na wcześniejszą zgodność z prawem przetwarzania danych.

7. Kontrola organu nadzorczego.

7.1. Wprowadzenie

Urząd Ochrony Danych Osobowych może prowadzić czynności kontrolne wszelkich obszarów oraz sposobów przetwarzania danych. W trakcie postępowania kontrolnego dozwolone jest przeprowadzanie oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych. Urząd Ochrony Danych Osobowych może żądać złożenia wyjaśnień oraz przesłuchiwać osoby w charakterze świadków.

7.2. Postępowanie kontrolne

1. Organem uprawnionym do kontroli ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych, jego zastępca lub upoważnieni pracownicy.
2. Administrator Danych zapewnia dostęp upoważnionych przedstawicieli organu nadzorczego do pomieszczeń, w których przetwarzane są dane osobowe, w szczególności w swojej siedzibie, w godz. 6.00 – 22.00 każdego dnia roboczego.
3. Przedstawiciele Urzędu Ochrony Danych Osobowych uzyskują dostęp do pomieszczeń, w których przetwarzane są dane osobowe po dokonanej przez członka Personelu weryfikacji przedstawionych przez przedstawicieli ww. Urzędu imiennych upoważnień i legitymacji służbowych.
4. Członek personelu:
    1) zabezpiecza oryginały upoważnienia lub sporządza kopię, którą poświadcza za zgodność;
    2) potwierdza sprawdzenie legitymacji służbowych oraz zgodność danych z legitymacji i upoważnienia poprzez podpisanie kopii upoważnienia przy każdej wymienionej z imienia i nazwiska osobie będącej przedstawicielem Urzędu, która zgłosiła się z zamiarem skontrolowania ochrony danych osobowych;
5. Członek Personelu, który został poinformowany o planowanej bądź rozpoczynającej się kontroli Urzędu zobowiązany zawiadomić o tym Administratora Danych.
6. Osobami upoważnionymi do współpracy z Urzędem podczas kontroli są:
    1) Administrator Danych;
    2) Inspektor;
    3) inne osoby wskazane przez Administratora Danych w momencie rozpoczęcia oraz w trakcie przeprowadzanej kontroli.

7. Upoważnieni członkowie personelu są zobowiązani do współpracy z organem nadzorczym poprzez udzielanie ustnych lub pisemnych wyjaśnień, udostępnianie do wglądu dokumentów, udostępnianie w celu wykonania oględzin nośników pamięci i systemów informatycznych.

8. Sprawy kadrowe

8.1. Wprowadzenie

W stosunku pracy podstawę przetwarzania danych osobowych przede wszystkim określa Kodeks pracy, który różnicuje zakres informacji, których Administrator Danych może żądać od kandydata do pracy i od pracownika. Określenie przez Administratora Danych minimalnego zakresu danych osobowych następuje w oparciu o akt wykonawczy w sprawie prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych, w którym zawarte zostały wzory kwestionariuszy osobowych.

8.2. Przetwarzanie danych osobowych

1. Administrator Danych ma prawo żądać od osoby ubiegającej się o pracę następujących informacji:
   1) imię (imiona) i nazwisko;
   2) data urodzenia;
   3) dane kontaktowe wskazane przez taką osobę;
   4) wykształcenie;
   5) kwalifikacje zawodowe;
   6) przebieg dotychczasowego zatrudnienia;

   przy czym dane osobowe, o których mowa w pkt 4-6, gdy jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku.
2. Administrator Danych ma prawo żądać od pracownika podania, niezależnie od danych osobowych, o których mowa wyżej, także:
   1) adres zamieszkania;
   2) numer PESEL, a w przypadku jego braku - rodzaj i numer dokumentu potwierdzającego tożsamość;
   3) innych danych osobowych pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy;

4) wykształcenia i przebiegu dotychczasowego zatrudnienia, jeżeli nie istniała podstawa do ich żądania od osoby ubiegającej się o zatrudnienie;

5) numer rachunku płatniczego, jeżeli pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych.

3. Administrator Danych zamieszcza w ogłoszeniu o pracę stosowną klauzulę informacyjną po uprzednim zatwierdzeniu jej treści przez Inspektora.

4. Administrator Danych żąda podania innych danych osobowych niż określone wyżej, gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

5. Udostępnienie Administratorowi Danych danych osobowych następuje w formie oświadczenia osoby, której dane dotyczą. Pracodawca może żądać udokumentowania danych osobowych w zakresie niezbędnym do ich potwierdzenia.

6. Zgoda osoby ubiegającej się o zatrudnienie lub pracownika może stanowić podstawę przetwarzania przez Administratora Danych innych danych osobowych niż wymienione w ust. 1 i 2 wyżej, z wyjątkiem danych osobowych dotyczących wyroków skazujących i naruszeń prawa. Brak zgody lub jej wycofanie, nie może być podstawą niekorzystnego traktowania osoby ubiegającej się o zatrudnienie lub pracownika, a także nie może powodować wobec nich jakichkolwiek negatywnych konsekwencji, zwłaszcza nie może stanowić przyczyny uzasadniającej odmowę zatrudnienia, wypowiedzenie umowy o pracę lub jej rozwiązanie bez wypowiedzenia przez pracodawcę. Przetwarzanie dotyczy danych osobowych udostępnianych przez osobę ubiegającą się o zatrudnienie lub pracownika na wniosek pracodawcy lub danych osobowych przekazanych pracodawcy z inicjatywy osoby ubiegającej się o zatrudnienie lub pracownika.

7. Zgoda osoby ubiegającej się o zatrudnienie lub pracownika może stanowić podstawę przetwarzania przez pracodawcę Danych osobowych szczególnych kategorii wyłącznie w przypadku, gdy przekazanie tych danych osobowych następuje z inicjatywy osoby ubiegającej się o zatrudnienie lub pracownika.

8. Przetwarzanie danych biometrycznych pracownika jest dopuszczalne także wtedy, gdy podanie takich danych jest niezbędne ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę, lub dostępu do pomieszczeń wymagających szczególnej ochrony.

9. Do przetwarzania Danych osobowych szczególnych kategorii mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania takich danych wydane

przez Administratora Danych. Osoby dopuszczone do przetwarzania takich danych są obowiązane do zachowania ich w tajemnicy.

10. Jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić Administratora Danych na szkodę, Administrator Danych może wprowadzić szczególny nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring). Nagrania obrazu przetwarzane są wyłącznie do celów, dla których zostały zebrane, a przechowywane są przez okres nieprzekraczający 3 miesięcy od dnia nagrania.
11. Jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, Administrator Danych może wprowadzić kontrolę służbowej poczty elektronicznej pracownika (monitoring poczty elektronicznej). Monitoring poczty elektronicznej nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika.

9. Postanowienia końcowe.

1. Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów niniejszego dokumentu Polityki Bezpieczeństwa, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.
2. Do kontroli stanu ochrony danych osobowych uprawnieni są:
    1) Administrator Danych;
    2) Inspektor;
    3) Administrator Systemu;
    4) Pracownicy upoważnieni przez osoby wymienione w pkt 1 – 3.
3. W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy Rozporządzenia, ustawy o ochronie danych osobowych, aktów wykonawczych.
4. We wszelkich sprawach związanych z interpretacją postanowień Polityki Bezpieczeństwa oraz przepisów powszechnie obowiązujących dotyczących ochrony danych osobowych należy zwracać się do Inspektora.