**Polityka bezpieczeństwa danych osobowych w ProcessTeam Sp. z o.o.**

### Postanowienia ogólne

1. Polityka ochrony danych osobowych w ProcessTeam Sp. z o.o. (dalej: „PT”) jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach i procesach przetwarzania danych osobowych przetwarzanych przez PT, w tym zbiorach przetwarzanych w systemie informatycznym.
2. W PT przetwarzane są informacje stanowiące dane osobowe w rozumieniu art. 4 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) z dnia 27 Kwietnia 2016 R. (Dz. Urz. Ue. L Nr 119, Str. 1) – dalej Rozporządzenie RODO.
3. PT przetwarza dane osobowe znajdujące się w administrowanych przez niego zbiorach w określonych celach i w określonym zakresie, jeżeli istnieje ku temu podstawa prawna określona w art. 6 lub 9 RODO lub innych regulacjach.
4. Niniejszy dokument ma na celu realizację założeń ochrony danych osobowych określonych w:
   1. Konstytucja Rzeczypospolitej Polskiej,
   2. Rozporządzenie RODO,
   3. innych przepisach wydanych i przyjętych w celu realizacji ochrony danych osobowych w tym aktach wewnętrznych.
5. PT dąży do realizacji zasad, które wskazują, iż dane osobowe muszą być:
   1. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
   2. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu”);
   3. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
   4. prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
   5. przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 Rozporządzenia RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);
   6. przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).
6. PT przestrzegając zasad wskazanych w ust. 4 wykazuje ich przestrzeganie („rozliczalność”) m.in. poprzez prowadzoną dokumentacją mającą na celu realizację niniejszej Polityki ochrony danych osobowych.
7. **Definicje**
8. PT- ProcessTeam Sp. z o.o.
9. Administrator Danych Osobowych (ADO) – ProcessTeam Sp. z o.o., w imieniu którego działa Prezes.
10. Inspektor Ochrony Danych(IOD) – osoba wyznaczona przez Administratora Danych Osobowych (Prezesa ProcessTeam Sp. z o.o.) do nadzorowania przestrzegania zasad ochrony danych osobowych, oraz przygotowania dokumentów wymaganych przez przepisy ustawy o ochronie danych osobowych w PT.
11. Użytkownik systemu - osoba upoważniona do przetwarzania danych osobowych. Użytkownikiem może być pracownik PT, osoba świadcząca usługi na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w PT.
12. Identyfikator użytkownika - jest to ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
13. Administratorzy Systemu Informatycznego – osoby wyznaczone przez ADO do realizacji zadań z zakresu funkcjonowania Systemu informatycznego oraz stosowania technicznych i organizacyjnych środków ochrony stosowanych w tym Systemie informatycznym
14. Sieć lokalna - połączenie komputerów pracujących w urzędzie w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych.
15. Sieć publiczna - sieć telekomunikacyjna, niebędąca siecią wewnętrzną służąca do świadczenia usług telekomunikacyjnych w rozumieniu ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (tj. Dz. U. 2016, poz.1489, z późn. zm.).
16. Sieć telekomunikacyjna - urządzenia telekomunikacyjne zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci za pomocą przewodów, fal radiowych, bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną w rozumieniu ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne.
17. System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
18. Przetwarzanie danych - rozumie się to w tym dokumencie, jako jakiekolwiek operacje wykonywane nadanych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie. Zabezpieczenie danych w systemie informatycznym - wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
19. Teletransmisja – przesyłanie informacji za pomocą Sieci telekomunikacyjnej.
20. Poufność danych - jest to właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
21. Integralność danych - właściwość zapewniająca, że dane osobowe nie zostały zmienione, lub zniszczone w sposób nieautoryzowany.
22. Rozliczalność - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
23. Aplikacja - program komputerowy wykonujący konkretne zadanie.
24. Wysoki poziom bezpieczeństwa - musi występować wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego, służące do przetwarzania danych osobowych, połączone jest z Siecią publiczną.
25. Komórka organizacyjna - rozumie się przez to dział, zespół lub samodzielne stanowisko pracy.

### Zarządzanie przetwarzaniem i bezpieczeństwem danych osobowych

1. Administratorem danych osobowych przetwarzanych w PT jest PT, reprezentowany przez Prezesa PT.
2. Prezes PT powołuje **Inspektora Ochrony Danych**, który wykonuje zadania wskazane w art. 39 Rozporządzenia RODO do których należy:
   1. informowanie Prezesa PT oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego Rozporządzenia RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
   2. monitorowanie przestrzegania Rozporządzenia RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   3. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
   4. współpraca z organem nadzorczym;
   5. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
      * W ramach wypełniania obowiązków wskazanych w lit. a:
3. informuje o zmianach i nowych interpretacjach w dziedzinie danych osobowych w zakresie dotyczącym administratora danych osobowych;
4. informuje o obowiązkach nałożonych przepisami oraz dokumentami wewnętrznymi na pracowników;
5. udziela odpowiedzi i konsultacji w zakresie stosowania przepisów dotyczących przetwarzania danych osobowych;
   * + W ramach wypełniania obowiązków wskazanych w lit. b:
6. cyklicznie informuje o zaobserwowanych zagrożeniach w dziedzinie ochrony danych osobowych;
7. cyklicznie kieruje zapytania dotyczące przetwarzania danych osobowych;
8. prowadzi audyty planowe według przyjętego harmonogramu;
9. prowadzi audyty doraźne;
10. Inspektor Ochrony Danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
11. Prezes PT zapewnia, by Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
12. Prezes PT wspiera Inspektora Ochrony Danych w wypełnianiu przez niego zadań, o których mowa w art. 39 Rozporządzenia RODO, 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.
13. Prezes PT zapewnia, by Inspektor Ochrony Danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań.
14. Inspektor Ochrony Danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.
15. Inspektor Ochrony Danych może wykonywać inne zadania i obowiązki. Prezes PT zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.
16. Prezes PT powierza Inspektorowi Ochrony Danych:
    1. Monitoring i aktualizacja prowadzonej dokumentacji przetwarzania danych osobowych;
    2. prowadzenie rejestrów czynności danych osobowych i kategorii danych osobowych(o ile jest taka potrzeba) zgodnie z uzyskanymi informacjami;
    3. prowadzenie rejestru osób upoważnionych do przetwarzania danych zgodnie z uzyskanymi informacjami;
    4. opiniowanie umów przetwarzania danych osobowych pod kątem Rozporządzenia RODO;
    5. prowadzenie rejestru incydentów;
17. Inspektor Ochrony Danych podlega bezpośrednio wyłącznie Prezesowi PT.
18. Prezes PT może powołać zastępców Inspektora Ochrony Danych wspierających go w realizacji zadań.
19. **Kierownicy komórek organizacyjnych** (przez które rozumie się także osoby zajmujące samodzielne stanowiska, o ile odpowiadają one samodzielnie za wybrane obszary przetwarzania danych osobowych) są odpowiedzialni za:
    1. zarządzenie zasobem danych osobowych w ramach komórki organizacyjnej;
    2. występowanie z wnioskiem do Administratora Systemu Informatycznego o nadanie, zmianę lub cofnięcie uprawnień pracownikom do określonego zasobu danych osobowych przetwarzanego w systemie informatycznym w tym aplikacjach;
    3. bieżąca kontrola nad realizacją zasad przetwarzania danych osobowych przez podległych pracowników;
    4. zabezpieczenie obszaru przetwarzania danych osobowych;
    5. zgłaszania do Inspektora Ochrony Danych zamiaru podjęcia nowych czynności przetwarzania na danych osobowych w tym w szczególności zamiaru powierzenia przetwarzania danych osobowych podmiotom zewnętrznym;
    6. zgłaszania do Inspektora Ochrony Danych incydentów przetwarzania danych osobowych;
    7. konsultowanie z Inspektorem Ochrony Danych podstawy przetwarzania danych osobowych w tym zasadności dopuszczenia do przetwarzania zbiorów osób i podmiotów trzecich;
    8. realizację procesu udostępniania danych osobowych;
    9. realizację zapisów umów powierzenia przetwarzania danych osobowych;
20. **Pracownik ds. kadrowych** jest odpowiedzialny za:
    1. informowanie Inspektora Ochrony Danych o wszelkich zmianach kadrowych na stanowiskach na których są przetwarzane dane osobowe;
    2. przygotowanie upoważnień do przetwarzania danych osobowych do podpisu przez Inspektora Ochrony Danych lub przekazania mu informacji umożliwiających ich wystawienie,
    3. przechowywanie nadanych upoważnień do przetwarzania danych osobowych oraz oświadczeń o zachowaniu poufności (i innych w aktach osobowych pracowników;
21. **Administrator Systemu Informatycznego** jest odpowiedzialny za zabezpieczenie i prawidłowe funkcjonowanie systemów informatycznych (w tym aplikacji):
    1. prowadzenie aktualnego wykazu systemów informatycznych (w tym aplikacji);
    2. prowadzenie aktualnego wykazu osób wraz z loginami do systemów informatycznych i określonych aplikacji;
    3. fizyczne nadawanie dostępu do systemu (w tym aplikacji) osobom upoważnionym do przetwarzania danych osobowych na wniosek Kierowników komórek organizacyjnych
    4. fizyczne odbieranie lub modyfikację uprawnień do systemów (w tym aplikacji);
    5. nadanie identyfikatorów (login) w systemie (w tym aplikacji);
    6. nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
    7. ustalenia w porozumieniu z Inspektorem Ochrony Danych, zasad ochrony danych w systemie informatycznym oraz akceptowanie wdrażania rozwiązań przygotowywanych w tym celu;
    8. przeciwdziałanie dostępowi osób nieupoważnionych do systemu (w tym aplikacji), w którym przetwarzane są dane osobowe, a także nieautoryzowanych modyfikacji w tym zakresie;
    9. informowanie Inspektora Ochrony Danych o wszelkich incydentach i zdarzeniach w systemie informatycznym mającym wpływ na poufność, integralność i ciągłość przetwarzania danych osobowych;
    10. wykonywanie kopii zapasowych systemów (w tym aplikacji), zabezpieczenie ich przechowywania i okresowe sprawdzenie pod kątem odtwarzalności;
    11. zgłaszania Inspektorowi Ochrony Danych informacji niezbędnych do aktualizacji dokumentów dotyczących przetwarzania danych osobowych;
    12. tworzenie w porozumieniu z Inspektorem Ochrony Danych procedur zarządzania kontami użytkowników, procedur wykonywania kopii zapasowych i innych;
    13. zapewnienie bezpiecznej wymiany danych w sieci wewnętrznej i nadzór nad przesyłaniem danych za pośrednictwem urządzeń teletransmisji;
    14. nadzór nad poprawnym działaniem awaryjnego zasilania urządzeń w szczególności serwerów;
    15. składanie do Prezesa PT propozycji zakupu oprogramowania lub sprzętu w celu podniesienia poziomu bezpieczeństwa systemu;
    16. opiniowanie bezpieczeństwa stosowanych lub planowanych systemów zabezpieczających system informatyczny w porozumieniu Inspektorem Ochrony Danych;
    17. składanie na wniosek Inspektora Ochrony Danych wyjaśnień, raportów, sprawozdań w zakresie obowiązków wskazanych w lit. powyżej.

### Obszar przetwarzania danych osobowych

### Obszar przetwarzania danych osobowych znajduje się w odrębnym dokumencie.

1. **Wykaz oprogramowania służącego do przetwarzania danych osobowych**

Wykaz oprogramowania znajduje się w odrębnym dokumencie prowadzonym przez ASI.

1. **Osoby przetwarzające dane osobowe**

Procedura nadawania upoważnień stanowi załącznik do niniejszego dokumentu.

1. **Obowiązki osób przetwarzających dane osobowe**
2. Obowiązki osób przetwarzających dane osobowe zostały określone w niniejszym dokumencie, procedurach oraz innych przyjętych w jednostce dokumentach.
3. Nieprzestrzeganie wskazanych tam obowiązków stanowi przedmiot analizy Administratora Danych Osobowych w konsultacji z Inspektorem Ochrony Danych. Administrator Danych Osobowych podejmuje decyzję o konsekwencjach mających być wyciągniętych wobec osoby naruszającej obowiązki, o którym mowa w ust. 1.
4. **Umowy powierzenia danych osobowych**
5. W przypadku powierzenia przetwarzania danych osobowych podmiotom trzecim, powierzenie następuje w drodze umowy powierzenia danych osobowych lub innego równorzędnego dokumentu dopuszczonego przez Rozporządzenie RODO.
6. Umowa powierzenia przetwarzania danych lub inny równorzędny dokument powinien zawierać elementy wskazane w Rozporządzeniu RODO.
7. Powierzenie przetwarzania danych osobowych jest konsultowane z Inspektorem Ochrony Danych.
8. Administrator Danych Osobowych ewidencjonuje umowy powierzenia danych osobowych.
9. **Udostępnianie danych osobowych odbiorcom**
   * + 1. Udostępnienie danych osobowych odbiorcą niebędącymi podmiotami przetwarzającymi może nastąpić wyłącznie w przypadku istnienia przesłanki legalizującej udostępnienie danych osobowych.
       2. Udostępnienie danych osobowych jest konsultowane z Inspektorem Ochrony Danych. Komórka organizacyjna (lub osoba zajmująca samodzielne stanowisko) udostępniająca dane ewidencjonuje ich udostępnienie.
10. **Incydenty**
11. Osoby zatrudnione przy przetwarzaniu danych osobowych są zobowiązane powiadomić Inspektora Ochrony Danych o ewentualnych naruszeniach bezpieczeństwa systemu ochrony danych osobowych w każdym zbiorze danych lub systemie.
12. Za zdarzenia naruszające bezpieczeństwo danych osobowych uważa się w szczególności:
13. nieupoważniony dostęp do danych osobowych,
14. ujawnienie bądź utrata danych osobowych,
15. nieupoważniona modyfikacja danych osobowych, kopiowanie lub niszczenie dokumentów zawierających dane osobowe,
16. inne naruszenie postanowień Rozporządzenia RODO.
17. Inspektor ochrony danych osobowych informuje o zdarzeniu Administratora Danych Osobowych, który informuje w przypadkach wskazanych w Rozporządzeniu RODO Urząd Ochrony Danych Osobowych i osoby, których przetwarzanie danych osobowych zostało naruszone.
18. Administrator Danych Osobowych może wydać odrębną szczegółową procedurę postępowania w takich przypadkach.
19. **Gromadzenie danych osobowych**
    * 1. Dane osobowe przetwarzane w PT mogą być uzyskiwane:
20. bezpośrednio od osób, których te dane dotyczą,
21. z innych źródeł, w granicach dozwolonych przepisami prawa.
    * 1. Przetwarzanie danych osobowych może odbywać się wyłącznie w sytuacjach przewidzianych w art. 6 oraz 9 Rozporządzenia RODO oraz stosownych regulacjach wydanych na tej podstawie.
      2. Dane są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
      3. Zbierane dane są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”).
      4. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą lub niszczone, chyba że przepis prawa stanowi inaczej.
      5. W przypadku konieczności udostępnienia dokumentów i danych osobowych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać zmiany tych danych osobowych w sposób zapewniający anonimowość osób, których dane te dotyczą.
      6. W przypadku, gdy dane osoby są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem Rozporządzenia RODO, albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator Danych Osobowych jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.
22. **Obowiązek informacyjny**

### Kierownicy komórek organizacyjnych PT lub osoby zatrudnione na samodzielnych stanowiskach, które zbierają i przetwarzają dane osobowe, są odpowiedzialni udzielić, osobom których dane przetwarzają, wszelkich informacji, o których mowa w art. 13 i 14 Rozporządzenia RODO, oraz z udziałem Inspektora Ochrony Danych prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 w sprawie przetwarzania ich prawach. Obowiązek informacyjny prowadzony jest zgodnie z ustaloną z Inspektorem Ochrony Danych klauzulą informacyjna ich dotyczącą. Klauzula informacyjna zawiera informacje wskazane w art. 12 Rozporządzenia RODO.

1. Administrator Danych Osobowych może wydać odrębną szczegółową procedurę postępowania w takich przypadkach.
2. **Prawa osób, których dotyczą dane osobowe**

Osobom, których dane przetwarza się w zbiorze danych osobowych PT, przysługuje:

* 1. prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych,
  2. prawo do żądania sprostowania (poprawienia) danych,
  3. prawo do żądania usunięcia danych osobowych (tzw. „prawo do bycia zapomnianym”),
  4. prawo do żądania ograniczenia przetwarzania danych osobowych,
  5. prawo do przenoszenia danych do Pani/ Pana lub do innego administratora danych,
  6. prawo do sprzeciwu wobec przetwarzania danych osobowych.

### Inspektor Ochrony Danych opiniuje zasadność żądania i wraz z komórką organizacyjną w której przetwarzane są dane osobowe udziela odpowiedzi.

1. **Czynności przetwarzania i zbiory danych**
   * 1. W PT prowadzi się rejestr czynności przetwarzania danych osobowych i ewentualnie rejestr kategorii przetwarzania danych. Rejestry są aktualizowane przez Inspektora Ochrony Danych na podstawie własnych ustaleń oraz informacji uzyskanych od pracowników. Czynności przetwarzania mogą być grupowane w ramach zbiorów danych osobowych wedle kryterium komórki przetwarzającej dane osobowe lub innego przyjętego w PT takiego jak kategoria osób lub cel przetwarzania danych.
     2. Kierownicy komórek organizacyjnych PT lub osoby zatrudnione na samodzielnych stanowiskach, w których przetwarzane są dane osobowe, są zobowiązani do zgłoszenia Inspektorowi Danych Osobowych informacji na temat:

a) planowanego założenia nowych czynności przetwarzania i zbiorów danych osobowych,

b) wnoszonych zmian do istniejących czynności przetwarzania i zbiorów danych osobowych.

1. **Ocena ryzyka**

### W celu prawidłowego wyznaczenia poziomu ochrony Administrator Danych Osobowych dokonuje okresowej analizy ryzyka, 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. Brana jest ona pod uwagę zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania, a na jej podstawie wdraża się 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.

1. **Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności danych przetwarzanych w systemie**

1. Dostęp do pomieszczeń PT, w których przetwarzane są dane osobowe, podlega kontroli.

2. Kontrola dostępu polegać może w szczególności na ewidencjonowaniu wszystkich przypadków pobierania i zwrotu kluczy do budynków i pomieszczeń. W ewidencji uwzględnia się: imię i nazwisko osoby pobierającej lub zdającej klucz, numer lub inne oznaczenie pomieszczenia oraz godzinę pobrania lub zdania klucza.

3. Klucze do pomieszczeń, w których przetwarzane są dane osobowe wydawane być mogą wyłącznie osobom upoważnionym.

4. PT realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, może wprowadzać inne formy monitorowania dostępu do obszarów przetwarzania danych osobowych.

5. W PT stosowane są następujące dodatkowe środki techniczne i organizacyjne oraz przedsięwzięcia niezbędne do zapewnienia poufności, integralności przetwarzanych danych osobowych:

* 1. środki ochrony fizycznej - urządzenia służące do przetwarzania danych osobowych znajdują się wyłącznie w pomieszczeniach zabezpieczonych zamkami,
  2. zbędne dokumenty papierowe zawierające dane osobowe mogą być niszczone wyłącznie w niszczarkach,
  3. urządzenia stacjonarne na których znajdują się bazy danych osobowych powinny być podłączone do lokalnych awaryjnych zasilaczy UPS, zabezpieczających przed skokami napięcia i zanikiem zasilania,
  4. sieć lokalna podłączona jest do Internetu poprzez router spełniający jednocześnie funkcję sprzętowego, zewnętrznego firewall filtrującego dane przechodzące pomiędzy siecią lokalną i siecią publiczną,
  5. codzienne kopie zapasowe są wykonywane automatycznie poprzez odpowiednie ustawienia w systemach informatycznych,
  6. okresowo są wykonywane kopie zapasowe na nośniki zewnętrzne.

6. W PT stosowane są następujące środki ochrony w ramach narzędzi informatycznych i innych narzędzi programowych oraz środki ochrony w ramach systemu użytkowego:

* 1. identyfikator i hasło dostępu do danych na poziomie aplikacji - dla każdego użytkownika systemu wyznaczony jest odrębny identyfikator, użytkownicy mają dostęp do aplikacji umożliwiający dostęp tylko do tych danych osobowych, do których mają uprawnienia,
  2. komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem, stosowane jest wygaszenie ekranu w przypadku dłuższej nieaktywności użytkownika, stosowana jest blokada hasłem podczas dłuższej nieaktywności użytkownika,
  3. na komputerach stosuje się hasło administracyjne oraz hasło użytkownika;
  4. hasła są konstruowane w następujący sposób:

1. hasło dostępu do stacji roboczej lub oprogramowania powinno składać się z co najmniej z 8 znaków (dużych i małych liter oraz z cyfr lub znaków specjalnych).
2. dokonywać zmiany hasła, w przypadku, gdy nie jest to wymuszone przez system, nie rzadziej niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.
3. hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: imion, nazwisk, inicjałów, dat, numerów rejestracyjnych samochodów, numerów telefonów. Hasło nie może być identyczne z loginem.
4. zobowiązana jest do zachowania hasła w poufności, nawet po utracie przez nie ważności i odpowiada za wszystkie działania wykonane z wykorzystaniem osobistego loginu i hasła.
5. zabronione jest przekazywanie haseł innym osobom oraz zapisywanie haseł w sposób jawny (np. na karteczkach samoprzylepnych, w komputerze); pierwsze hasło nadane przez administratora danych osobowych jest przekazywane użytkownikowi systemu w sposób uniemożliwiający zapoznanie się z nim osób postronnych i niezwłocznie przez niego zmieniane.
6. wszystkie elementy sieci informatycznej są zabezpieczone hasłami, elementy takie jak routery, drukarki z dyskami, stacje robocze w zakresie hasła administracyjnego i podobne są zabezpieczone przez Administratora Systemów Informatycznych znanemu jemu oraz deponowane w kopercie u Administratora Danych Osobowych;
7. Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.
8. W przypadku likwidacji nośników informatycznych zawierających Dane Osobowe lub kopie zapasowe Systemów Informatycznych służących do przetwarzania Danych Osobowych należy przed ich likwidacją usunąć Dane Osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.
9. Nie przechowuje się zbędnych nośników informacji zawierających zbędne Dane Osobowe oraz kopie zapasowe, a także wydruków i innych dokumentów zawierających Dane Osobowe, których przechowywanie nie jest uzasadnione celem ich przetwarzania.
10. Nośniki informacji zawierające Dane Osobowe oraz Kopie Zapasowe, a także wydruki i inne dokumenty zawierające Dane Osobowe przechowywane są w zamykanych szafach w pomieszczeniach stanowiących obszar przetwarzania Danych Osobowych, w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem.
11. Po upływie użyteczności Danych Osobowych, o ile przepis szczególny nie stanowi inaczej, Dane Osobowe są kasowane lub niszczone tak, aby nie było możliwe ich odtworzenie. Dozwolona jest również ich anonimizacja polegająca na pozbawieniu danych umożliwiających identyfikację określonej osoby fizycznej.
12. W przypadku uszkodzenia lub zużycia nośników informacji zwierających Dane Osobowe są one fizycznie niszczone (we własnym zakresie lub przez podmiot profesjonalnie zajmujący się takimi czynnościami) tak, aby nie było możliwe odczytanie danych osobowych. Ze zniszczenia sporządzany jest raport.
13. Do ochrony przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego stosowane jest oprogramowanie antywirusowe. Oprogramowanie obejmuje każdy element systemu informatycznego wymagający ochrony. Konieczność ochrony poszczególnych elementów systemu informatycznego określa Administrator Systemów Informatycznych.
14. Każdy zbiór wczytywany do komputera, podłączane urządzenie, w tym także wiadomość e-mail, musi być przeskanowany programem antywirusowym.
15. Na każdym stanowisku wyposażonym w dostęp do sieci publicznej (Internet) musi być zainstalowanie oprogramowanie antywirusowe oraz program firewall. Niedopuszczalne jest stosowanie dostępu do sieci publicznej (Internet) bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.
16. w przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności Administratora Systemu Informatycznego.
17. przeglądy techniczne sprzętu komputerowego są dokonywane przy każdej czynności w toku codziennych prac jednakże nie rzadziej niż raz w roku.
18. w systemie informatycznym instalowane są zalecane przez producentów oprogramowania poprawki i uaktualnienia. Poprawki i uaktualnienia służą do wyeliminowania błędów w działaniu lub poprawienia wydajności działania.
19. w przypadku powierzenia określonego składnika systemu informatycznego w postaci programu komputerowego dostarczanego przez licencjodawcę programu komputerowego, postanowienia dotyczące poufności oraz przetwarzania danych osobowych będą regulowane na podstawie umowy licencyjnej lub umowy dotyczącej przetwarzania danych osobowych będącej uzupełnieniem umowy licencyjnej.

7. Środki organizacyjne.

* 1. Wyznaczono Inspektora Ochrony Danych.
  2. Tymczasowe wydruki z danymi osobowymi są po ustaleniu ich przydatności niszczone.
  3. Do przetwarzania danych osobowych przy użyciu systemu informatycznego dopuszczane są osoby na podstawie upoważnienia do przetwarzania danych osobowych wydawanego na polecenie Administratora Danych Osobowych.
  4. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane są do zachowania ich w tajemnicy.
  5. Osoby przetwarzające dane osobowe są przed dopuszczeniem ich do tych danych szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych w systemie informatycznym.
  6. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
  7. Ustalono Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.
  8. Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych.

### Procedury zapewniające ochronę danych osobowych

### W PT obowiązują następujące procedury, które stanowią załącznik do niniejszej Polityki:

1. Załącznik Nr 1. Procedura nadawania upoważnień;
2. Załącznik nr 2. Procedura opiniowania zagadnień prawnych związanych z danymi osobowymi;
3. Załącznik nr 3. Procedura reagowania i oceny naruszeń bezpieczeństwa danych osobowych;
4. Załącznik nr 4. Procedura realizowania uprawnień osób, których dane są przetwarzane;
5. Załącznik nr 5. Procedura udzielania informacji podawanej w przypadku pozyskiwania danych;

### Realizacja w/w procedur jest ewidencjonowana w odrębnych dokumentach (listach prowadzonych przez Inspektora Ochrony Danych).

### Postanowienia końcowe

* 1. Inspektor Ochrony Danych zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych,
  2. Wobec osoby, będącej pracownikiem PT, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne,
  3. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Inspektora Ochrony Danych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych wzwiązkuz przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) - (RODO).

### Załączniki

1. Załącznik Nr 1. Procedura nadawania upoważnień;
2. Załącznik nr 2. Procedura opiniowania zagadnień prawnych związanych z danymi osobowymi;
3. Załącznik nr 3. Procedura reagowania i oceny naruszeń bezpieczeństwa danych osobowych;
4. Załącznik nr 4. Procedura realizowania uprawnień osób, których dane są przetwarzane;
5. Załącznik nr 5. Procedura udzielania informacji podawanej w przypadku pozyskiwania danych;
6. Wzór upoważnienia imiennego do przetwarzania danych osobowych.
7. Lista dokumentów przyjętych w jednostce.