Polityka ochrony danych osobowych w STALCO spółka z ograniczoną odpowiedzialnością S.K.A.

Na podstawie art. 24 Rozporządzenia 2016/679, z dniem 25.05.2018 r. wprowadza się Politykę ochrony danych osobowych

Spis treści

1. Postanowienia ogólne

1. Niniejszy dokument zatytułowany “Polityka ochrony danych osobowych” (zwany dalej „Polityką”) ma za zadanie stanowić mapę wymogów, zasad, regulacji ochrony danych osobowych w Podmiocie.
2. Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO - 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.U.UE.L.2016.119.1.
3. Polityka, określająca zasady przetwarzania i ochrony danych w Podmiocie, zawiera w szczególności:

- opis zasad ochrony danych w Podmiocie,
- odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych wymagających doprecyzowania w odrębnych dokumentach).

2. Definicje

Ilekroć w Polityce jest mowa o:

1. Administratorze Danych Osobowych (ADO) – rozumie się przez to STALCO spółka z ograniczoną odpowiedzialnością S.K.A z siedzibą w Skawinie przy ul. Torowej 41, 32-050 Skawina, wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Krakowa - Śródmieścia w Krakowie, Wydział XII Gospodarczy, pod numerem KRS 0000425156, NIP 6792455066, REGON 351398835;
2. Instrukcji – rozumie się przez to Instrukcję określającą sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, która została przyjęta przez ADO jako obowiązujący dokument w Podmiocie;
3. Podmiocie – rozumie się przez to STALCO spółka z ograniczoną odpowiedzialnością S.K.A;
4. 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) Dz.U.UE.L.2016.119.1 z dnia 2016.05.04;
5. danych osobowych – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka

szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

6. danych szczególnych kategorii – rozumie się przez to dane osobowe wymienione w art. 9 ust. 1 RODO, tj. dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby;
7. danych karnych - dane wymienione w art. 10 ust. 1 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa
8. haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi, zapewniający mu dostęp do danych osobowych przetwarzanych w systemie informatycznym,
9. identyfikatorze – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
10. integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
11. integralności systemu – rozumie się przez to właściwość zapewniającą nienaruszalność systemu, niemożność jakiejkolwiek nieautoryzowanej modyfikacji,
12. nośniku danych – rozumie się przez to nośnik służący do zapisu i przechowywania informacji, np. pendrive, płyty, dyski twarde,
13. osobie - rozumie się przez to osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu;
14. odbiorcy danych – 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. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
15. poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
16. powierzeniu przetwarzania danych osobowych – rozumie się przez to zlecenie wykonania czynności przetwarzania danych osobowych przez procesora na rzecz ADO na podstawie stosownego zapisu w umowie, zapewniającego warunki bezpieczeństwa danych osobowych zgodnie z przepisami Ustawy i Rozporządzenia lub na podstawie odrębnej pisemnej umowy powierzenia przetwarzania danych osobowych zawartej zgodnie z art. 28 RODO,
17. podmiocie przetwarzającym – rozumie się przez to osobę lub organizację, której Podmiot powierzył przetwarzanie danych osobowych,
18. personelu – rozumie się przez to osoby świadczące pracę na rzecz ADO na podstawie stosunku pracy, umów cywilnoprawnych (np. umowy o dzieło lub umowy zlecenia), przedsiębiorców wykonujących działalność osobiście i jednoosobowo, osoby odbywające praktyki, stażystów, osoby skierowane do pracy w ramach umów z agencjami pracy

tymczasowej wykonujące prace związane z przetwarzaniem danych osobowych w strukturach ADO;

19. RCPD lub Rejestrze - rozumie się Rejestr Czynności Przetwarzania Danych
20. osobie upoważnionej do przetwarzania danych osobowych – rozumie się przez to członka personelu, któremu ADO nadał na piśmie imienne upoważnienie do przetwarzania danych w Podmiocie,
21. użytkowniku – rozumie się przez to osobę upoważnioną, której ADO nadał identyfikator i przyznał hasło,
22. przetwarzaniu danych – 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. rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
24. systemie informatycznym Administratora Danych Osobowych– rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, zasad przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
25. udostępnianiu danych osobowych – rozumie się przez to przekazywanie, ujawnianie, rozpowszechnianie danych osobowych odbiorcy danych,
26. usuwaniu danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
27. pseudonimizacji - oznacza 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;
28. uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby fizycznej lub podmiotu,
29. zabezpieczeniu systemu informatycznego – rozumie się przez to wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą,
30. zbieraniu danych osobowych – rozumie się przez to pozyskiwanie danych od osoby, której one dotyczą lub z innych źródeł,
31. zbiorze danych osobowych – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,
32. zgodzie osoby, której dane dotyczą – rozumie się przez to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

3. Cel wprowadzenia Polityki, zakres stosowania, zmiany i aktualizacja

1. Administrator Danych Osobowych, przywiązując szczególną wagę do ochrony danych osobowych przetwarzanych w strukturach Podmiocie, deklaruje podejmowanie wszelkich możliwych działań koniecznych do zapobiegania zagrożeniom bezpieczeństwa danych, wynikających z takich zdarzeń, jak:
   a) naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie,
   b) ujawnienie osobom nieupoważnionym zasad ochrony danych stosownych przez ADO,
   c) celowe lub przypadkowe rozproszenie danych w Internecie z ominięciem zabezpieczeń systemu lub wykorzystaniem błędów systemu informatycznego ADO,
   d) nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu informatycznego, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie, działania terrorystyczne,
   e) niewłaściwe parametry środowiska, zakłócające pracę urządzeń komputerowych (nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne),
   f) awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne naruszenia ochrony danych, niewłaściwe działanie procedur serwisowych w tym przyzwolenie na naprawę sprzętu zawierającego dane osobowe poza siedzibą ADO,
   g) ataki z Internetu,
   h) naruszenia zasad określonych w dokumentacji z zakresu ochrony danych osobowych przez osoby upoważnione, związane z nieprzestrzeganiem przez nie zasad ochrony danych, w tym zwłaszcza:
   i) niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy,
   j) ujawnienie osobom nieupoważnionym zasad ochrony danych stosowanych u ADO.
2. ADO opracowuje, zatwierdza i zapewnia wprowadzenie Polityki jako wyrazu woli wdrożenia przepisów prawa dotyczących ochrony danych osobowych oraz w celu zapewnienia ochrony danych osobowych, których jest administratorem przed wszelkiego rodzaju zagrożeniami wewnętrznymi i zewnętrznymi, świadomymi lub nieświadomymi.
3. Niezależnie od Polityki opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
4. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez zachowania osób upoważnionych.
5. Wskazane powyżej zabezpieczenia mają zapewnić poufność, integralność i rozliczalność danych osobowych przetwarzanych przez ADO a także integralność systemu informatycznego, z wykorzystaniem którego to przetwarzanie się odbywa.
6. Jeżeli przepisy jakichkolwiek ustaw przewidują dalej idącą ochronę danych osobowych niż Rozporządzenie, stosuje się przepisy tych ustaw.
7. Zasady określone przez Politykę mają zastosowanie do wszystkich:
   a) danych osobowych przetwarzanych w Podmiocie zarówno w przypadku, gdy jest administratorem danych, jak i w sytuacji, gdy przetwarza dane powierzone na podstawie umów zawartych w trybie art. 28 Rozporządzenia,

b) nośników informacji, np. papierowych, magnetycznych, optycznych itp., na których są lub będą znajdować się dane osobowe,
c) lokalizacji – budynków i pomieszczeń znajdujących się w dyspozycji Podmiocie, w których są lub będą przetwarzane dane osobowe,
d) osób stanowiących personel oraz innych osób mających dostęp do danych osobowych.

4.Ochrona danych osobowych w Podmiocie - ogólne zasady

1. Filary ochrony danych w Podmiocie:
2. Legalność - Administrator dba o ochronę prywatności i przetwarza dane zgodnie z prawem,
3. Bezpieczeństwo - ADO zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie,
4. Prawa jednostki - ADO umożliwia osobom wykonywanie swoich praw i prawa te realizuje,
5. Rozliczalność - ADO dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność
6. Zasady ochrony danych:
7. Dane osobowe są:
    a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość");
    b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami ("ograniczenie celu");
    c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych");
    d) 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");
    e) 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 ("ograniczenie przechowywania");
    f) 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").

5. System ochrony danych.

System ochrony danych w Podmiocie składa się z następujących elementów:

1. Inwentaryzacja danych. ADO dokonuje identyfikacji zasobów danych osobowych w Podmiocie, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystywania danych (inwentaryzacja) w tym:
   a) przypadków przetwarzania danych szczególnych kategorii i danych karnych,
   b) przypadków przetwarzania danych osób, których ADO nie identyfikuje
   c) przypadków przetwarzania danych,
   d) profilowania,
   e) współadministrowania danymi.
2. Rejestr. ADO opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych w Podmiocie (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Podmiocie.
3. Podstawy prawne. ADO zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze w tym:
   a) utrzymuje system zarządzania zgodami na przetwarzanie danych,
   b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy ADO przetwarza dane na podstawie prawnie uzasadnionego interesu ADO.
4. Obsługa praw jednostki. ADO spełnia obowiązki informacyjne względem osób, których dane przetwarza oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
   a) obowiązki informacyjne. ADO przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków;
   b) możliwość wykonania żądań. ADO weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.
   c) obsługa żądań. ADO zapewnia odpowiednia nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO i udokumentowane.
   d) zawiadamianie o naruszeniach. ADO stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem danych.
5. Minimalizacja. ADO posiada zasady i metody zarządzania minimalizacją (privacy by default), a w tym:
   a) zasady zarządzania adekwatnością danych,
   b) zasady reglamentacji i zarządzania dostępem do danych,
   c) zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności.
6. Bezpieczeństwo. ADO zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
   a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii,
   b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie,
   c) dostosowuje środki ochrony danych do ustalonego ryzyka,
   d) posiada system zarządzania bezpieczeństwem informacji,

e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych - zarządza incydentami.

7. Przetwarzający. ADO posiada zasady doboru przetwarzających dane na rzecz Administratora, wymogów co do warunków przetwarzania (umowy powierzenia), zasad weryfikacji wykonywania umów powierzenia.
8. Eksport danych. ADO posiada zasady weryfikacji, czy Podmiot przekazuje dane do państw trzecich (czyli poza UE, Norwegię, Liechtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków tego przekazywania, jeśli ma ono miejsce.
9. Privacy by design. ADO zarządza zmianami wpływającymi na prywatność. W tym celu procedury uruchamiania nowych projektów, inwestycji w Podmiocie uwzględniają konieczność oceny wpływu zmiany na ochronę danych, analizę ryzyka, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

6.Obowiązki Administratora Danych Osobowych

1. ADO realizuje zadania w zakresie ochrony danych osobowych, zmierzające do zapewnienia przestrzegania przepisów Rozporządzenia, w tym w szczególności:
   a) Nadzoruje opracowanie i aktualizację dokumentacji ochrony danych osobowych, w tym Polityki i Instrukcji.
   b) Nadzoruje przestrzeganie zasad określonych w dokumentacji ochrony danych, w tym Polityce i Instrukcji.
   c) Zapewnia adekwatne do zagrożeń i kategorii przetwarzanych danych środki techniczne i organizacyjne zapewniające ochronę danych osobowych w Podmiocie.
   d) Zapewnia zapoznanie osób, którym mają być nadane upoważnienia do przetwarzania danych z przepisami o ochronie danych oraz zasadami ochrony danych przyjętymi w Podmiocie poprzez zorganizowanie dla nich szkoleń, prowadzonych przez osobę posiadającą odpowiednią wiedzę i kompetencje. ADO może prowadzić szkolenia osobiście. Karta szkolenia z zakresu ochrony danych osobowych stanowi Załącznik nr 1 do Polityki.
   e) Podejmuje wszystkie niezbędne działania w celu należytego zabezpieczenia danych osobowych, w tym przed:
   a) udostępnieniem osobom nieupoważnionym,
   b) zabraniem przez osobę nieuprawnioną,
   c) niekontrolowaną zmianą, utratą,
   d) uszkodzeniem lub zniszczeniem.
   f) Zapewnia legalność przetwarzania danych osobowych w Podmiocie, a w szczególności dba, by:
      - na podstawie jednej z przesłanek legalizujących, o których mowa w art. 6 lub 9 Rozporządzenia,
      - zgodnie z obowiązującymi przepisami prawa oraz dobrymi praktykami,
      - zgodnie z zasadami celowości, merytorycznej poprawności, adekwatności oraz ograniczenia czasowego.
   g) Upoważnia do przetwarzania danych osobowych członków personelu Podmiotu w określonym indywidualnie zakresie.
   h) Nadzoruje i dba o zgodne z prawem przekazywanie danych osobowych (udostępnianie i powierzanie).
   i) Zapewnia użytkownikom odpowiednie stanowiska pracy, w tym sprzęt informatyczny, umożliwiające bezpieczne i zgodne z prawem przetwarzanie danych osobowych.
   j) Podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia zasad bezpiecznego przetwarzania danych osobowych.
   k) Przeprowadza regularnie wewnętrzną weryfikację przestrzegania przepisów dotyczących ochrony danych osobowych, w tym dokonuje sprawdzenia.
   l) Zapewnia prawidłową eksploatację systemu informatycznego, zgodnie z celami przetwarzania danych osobowych.
   m) Przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w Instrukcji.

n) Wyrejestrowuje użytkowników.
o) Zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem administracyjnym dostępu do wszystkich stacji roboczych i serwerów z pozycji administratora.
p) Wykonuje oraz sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których przetwarzane są dane osobowe.
q) Wykonuje oraz sprawuje nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego.
r) Szkoli użytkowników w zakresie procedur i instrukcji zapewniających ochronę danych osobowych i weryfikuje poprawność stosowania tych procedur i instrukcji.
s) Wyjaśnia wszystkie zgłoszone nieprawidłowości i incydenty dotyczące przetwarzania danych z wykorzystaniem środków informatycznych.

2. ADO gwarantuje poszanowanie praw osób, których dane dotyczą, a w szczególności prawa do uzyskania informacji o:
   a) administratorze danych,
   b) celu, zakresie, sposobie i podstawie prawnej przetwarzania danych,
   c) terminie do kiedy i jakie dane są przetwarzane,
   d) źródle, z którego dane pochodzą,
   e) sposobie udostępniania danych oraz ich odbiorcach.
   f) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   g) prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
   h) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
   i) prawie wniesienia skargi do organu nadzorczego;
   j) czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
   k) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

3. ADO gwarantuje respektowanie praw osób, których dane dotyczą w zakresie:
   a) żądania uzupełnienia, uaktualnienia, sprostowania, usunięcia, przeniesienia danych, ograniczenia przetwarzania
   b) wniesienia umotywowanego wniosku do zaprzestania przetwarzania danych,
   c) wycofania zgody na przetwarzanie danych osobowych.

4. ADO gwarantuje, że wobec osoby, której dane dotyczą zostanie spełniony obowiązek informacyjny, o którym mowa w art. 13 Rozporządzenia.

7. Zasady nadawania upoważnień do przetwarzania danych

1. Do przetwarzania danych w Podmiocie mogą być dopuszczone wyłącznie osoby przeszkolone w zakresie przetwarzania i ochrony danych zgodnie z Polityką i Instrukcją, którym ADO nadał pisemne upoważnienie do przetwarzania danych osobowych, którego wzór stanowi Załącznik nr 2 do Polityki.
2. Każdy, dopuszczony do przetwarzania danych osobowych pracownik ADO, po otrzymaniu upoważnienia do przetwarzania danych osobowych oraz po odbyciu szkolenia, składa na piśmie oświadczenie o poufności, którego treść kształtowana jest w zależności od zakresu obowiązków danego pracownika i którego wzór stanowią Załącznik nr 3a oraz Załącznik 3b do Polityki.
3. W przypadku, gdy do przetwarzania danych osobowych dopuszczona jest osoba, zatrudniona w Podmiocie na podstawie cywilnoprawnych form zatrudnienia, z osobą taką, po nadaniu jej przez ADO na piśmie odpowiedniego upoważnienia do przetwarzania danych osobowych, zawierana jest umowa o poufności.
4. Upoważnienie, o którym mowa w punkcie 1. musi być aktualne. W przypadku przedłużającej się nieobecności osoby upoważnionej lub zaprzestania wykonywania przez nią części lub wszystkich obowiązków, uzasadniających potrzebę upoważnienia jej do przetwarzania danych osobowych, upoważnienie musi zostać anulowane.
5. Utrata uprawnień do przetwarzania danych osobowych wynikających z upoważnienia do przetwarzania danych osobowych może nastąpić z powodu:
6. rozwiązania stosunku pracy bądź innego stosunku prawnego łączącego osobę upoważnioną z ADO,
7. zmiany stanowiska pracy u ADO, na którym nie ma konieczności posiadania dostępu do zbiorów danych osobowych, a nowy zakres czynności nie wykazuje obowiązków służbowych związanych z przetwarzaniem danych osobowych,
8. umyślnego naruszenia zasad ochrony danych osobowych określonych w Rozporządzeniu, Polityce oraz Instrukcji.
9. W przypadku utraty uprawnień do przetwarzania danych osobowych ADO zobowiązany jest do niezwłocznego anulowania upoważnienia do przetwarzania danych osobowych oraz dokonania zmian w ewidencji osób upoważnionych do przetwarzania danych w odpowiednim zbiorze danych.
10. Ewidencja upoważnień, którą prowadzi ADO znajduje się w Załączniku nr 4 do Polityki.

8.Podstawy przetwarzania

1. Przetwarzanie danych osobowych zwykłych możliwe jest w przypadku spełnienia jednej z przesłanek określonych w art. 6 Rozporządzenia, tj. tylko wtedy, gdy:
    a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
    b) 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;
    c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
    d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
    e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
    f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora 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. Przetwarzanie danych szczególnych kategorii możliwe jest w przypadku spełnienia jednej z przesłanek określonych w art. 9 Rozporządzenia tj. tylko wtedy, gdy:
    a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach;
    b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej;
    c) 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;
    d) 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;
    e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
    f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

g) 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;

h) 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;

i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego;

j) 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.

3. ADO dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
4. ADO wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość, oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności.

9. Gromadzenie i przetwarzanie danych osobowych

Uzyskiwanie danych osobowych

1. Dane osobowe przetwarzane w Podmiocie są uzyskiwane bezpośrednio od osób, których te dane dotyczą, lub z innych źródeł, w granicach dozwolonych przepisami prawa.

Wykorzystanie danych osobowych

1. Zebrane dane osobowe są wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Administrator zachowuje dane osobowe w formie umożliwiającej identyfikację osoby, której dane dotyczą, wyłącznie przez okres czasu konieczny do realizacji celu, dla którego są one przetwarzane, zgodnie z przepisami krajowymi.
2. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

Sposób obsługi praw jednostki i obowiązków informacyjnych

1. ADO dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
2. ADO ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczanie na stronie internetowej informacji lub odwołań (linków) do informacji o prawach osób, sposobie korzystania z nich w Podmiocie, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu z ADO w tym celu, ewentualnym cenniku żądań dodatkowych.
3. ADO dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.
4. ADO wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
5. W celu realizacji praw jednostki, ADO zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez ADO, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.
6. ADO dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

Obowiązek informacyjny

1. W każdym przypadku pobierania danych bezpośrednio od osoby, której dane dotyczą, Administrator danych informuje osobę, której dane dotyczą, zgodnie z Załącznikiem nr 9 do Polityki.
2. W każdym przypadku pobierania danych z innych źródeł niż osoba, której dane dotyczą, Administrator danych informuje osobę, której dane dotyczą, niezwłocznie, jednak nie później niż przy pierwszym kontakcie z osobą, której dane dotyczą, zgodnie z Załącznikiem nr 10 do Polityki.
3. W każdym przypadku odbierania zgody od osoby, której dane dotyczą, korzysta się z klauzul zgody zgodnie z Załącznikiem nr 11 do Polityki.
   ADO informuje osobę o planowanej zmianie celu przetwarzania danych.
   ADO informuje osobę przed uchyleniem ograniczenia przetwarzania.
   ADO informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
4. ADO informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

ADO zawiadamia bez zbędnej zwłoki osobę o naruszeniu danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

10. Żądania osób.

Rejestr realizacji żądań osoby, której dane dotyczą stanowi Załącznik nr 19 do Polityki.

1. Prawo dostępu do danych
   Na żądanie osoby dotyczące dostępu do jej danych Administrator informuje osobę, której dane dotyczą, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Podmiot nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych dla potrzeb opłat za kopie danych.
2. Kopie danych
   Na żądanie Podmiot wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Podmiot wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest na podstawie oszacowanego jednostkowego kosztu obsługi żądania wydania kopii danych.
3. Sprostowanie danych

   Podmiot dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Podmiot ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Podmiot informuje osobę o odbiorcach danych, na żądanie tej osoby.
4. Uzupełnienie danych

   Podmiot uzupełnia i aktualizuje dane na żądanie osoby. Podmiot ma prawo odmówić uzupełnienia danych, jeśli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Podmiot nie musi przetwarzać danych, które są Podmiotowi zbędne). Podmiot może polegać na oświadczeniu osoby co do uzupełnienia danych, chyba że będzie to niewystarczajace w świetle przyjętych przez Podmiot procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
5. Usunięcie danych
   Na żądanie osoby Podmiot usuwa dane, gdy:
   a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
   b) osoba cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
   c) osoba wniosła skuteczny sprzeciw wobec przetwarzania tych danych;
   d) dane osobowe były przetwarzane niezgodnie z prawem;
   e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie;
   f) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku. Podmiot określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17 ust. 3 RODO.

Jeżeli dane podlegające usunięciu zostały upublicznione przez Podmiot, Podmiot podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe o potrzebie usunięcia danych i dostępu do nich. W przypadku usunięcia danych, Podmiot informuje osobę o odbiorcach danych, na żądanie tej osoby.

6. Ograniczenie przetwarzania
   Podmiot dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
   a) osoba, kwestionuje prawidłowość danych osobowych – na okres pozwalający Administratorowi sprawdzić prawidłowość tych danych;
   b) przetwarzanie jest niezgodne z prawem, a osoba, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
   c) Podmiot nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
   d) osoba wniosła sprzeciw wobec przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

   W trakcie ograniczenia przetwarzania Administrator przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej z uwagi na ważne względy interesu publicznego. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.
7. Przenoszenie danych
   Na żądanie osoby, Administrator wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane osobowe jej dotyczące, które dostarczyła ADO, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej w systemach informatycznych Podmiotu. Wniosek o przeniesienie danych stanowi Załącznik nr 20 do Polityki.
8. Sprzeciw w szczególnej sytuacji
   Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Administratora w oparciu o uzasadniony interes Administratora lub o powierzone Administratorowi zadanie w interesie publicznym, Administrator uwzględnił sprzeciw o ile nie zachodzą po stronie Administratora ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
9. Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych
   Jeżeli Podmiot prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Administrator uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

10. Sprzeciw względem marketingu bezpośredniego
    Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Administratora na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), ADO uwzględni sprzeciw i zaprzestanie takiego przetwarzania.
11. Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą
    Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem - w szczególności, gdy informacje są kierowane do dziecka - udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 RODO, oraz prowadzić z nią wszelką komunikację w sprawie przetwarzania. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach - elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.
    Administrator ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy RODO.
    Administrator bez zbędnej zwłoki - a w każdym razie w terminie miesiąca od otrzymania żądania - udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie pkt. 1-11 powyżej. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.
    Jeżeli Administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.
    Informacje podawane osobie, której dane są zbierane oraz komunikacja i działania podejmowane na mocy pkt. 1-11 powyżej są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:
    a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; alb
    b) odmówić podjęcia działań w związku z żądaniem. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

    Jeżeli Administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 15-21 RODO, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.
12. Zgoda na przetwarzanie danych osobowych
    Materiały dotyczące innej niż ustawowa działalności Podmiotu mogą być wysyłane tylko do tych osób, które wcześniej wyraziły zgodę na piśmie na przetwarzanie ich danych osobowych

w tym celu.
Kandydaci do pracy w Podmiocie w procesie rekrutacji są zobowiązani podpisać pisemną zgodę na przetwarzanie ich danych osobowych.
Dokumenty złożone w celu rekrutacji są przechowywane w komórce organizacyjnej, która przetwarza te dane, i są włączane do akt osobowych pracownika.

11. Rejestr Czynności Przetwarzania Danych

1. RCPD stanowi formę dokumentowania czynności przetwarzania, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
2. ADO prowadzi Rejestr, w którym inwentaryzuje i monitoruje sposób w jaki wykorzystuje dane osobowe.
3. Rejestr jest jednym z podstawowych narzędzi umożliwiających Administratorowi rozliczanie większości obowiązków ochrony danych.
4. W Rejestrze dla każdej czynności przetwarzania danych, którą ADO uznał za odrębną dla potrzeb Rejestru, odnotowuje co najmniej: nazwę czynności, cel przetwarzania, opis kategorii osób, podstawę prawną przetwarzania wraz z wyszczególnieniem kategorii uzasadnionego interesu Podmiotu, jeśli jest on podstawą przetwarzania danych, sposób zbierania danych, opis kategorii odbiorców, informację o przekazaniu po EU/EOG, ogólny opis technicznych oraz organizacyjnych środków ochrony danych.
5. Rejestr czynności przetwarzania danych osobowych jest elementem dokumentacji ochrony danych.
6. Rejestr stanowi Załącznik nr 12 do Polityki.
7. Administrator wyznacza Inspektora Ochrony Danych w przypadkach wskazanych w art. 37 RODO, a w przypadku braku jego powołania wyjaśnia ten fakt. Stosowna dokumentacja znajduje się w Załączniku nr 13.

12. Minimalizacja

1. Podmiot dba o minimalizacja przetwarzania danych pod kątem:
    a) adekwatności danych do celów (ilości danych i zakresu przetwarzania)
    b) dostępu do danych,
    c) czasu przechowywania danych.

Minimalizacja zakresu

2. Podmiot zweryfikował zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach RODO.
3. Podmiot dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.
4. Podmiot przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (privacy by design).

Minimalizacja dostępu

5. Podmiot stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).
6. Podmiot stosuje kontrolę dostępu fizycznego.
7. Podmiot dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających.
8. Podmiot dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.

Minimalizacja czasu

9. Podmiot wdraża mechanizmy kontroli cyklu życia danych osobowych w Podmiocie, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.
10. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu, są usuwane z systemów Podmiotu, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Podmiot. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

13. Udostępnianie danych

1. Udostępnianie danych osobowych możliwe jest tylko w wypadku spełnienia jednej z w/w przesłanek przetwarzania danych osobowych.
2. Udostępnianie danych osobowych może nastąpić tylko po przedłożeniu wniosku, którego wzór stanowi Załącznik nr 5 do Polityki, o przekazanie lub udostępnienie informacji.
3. ADO prowadzi rejestr udostępnień danych osobowych w celu zapewnienia kontroli procesu udostępnień. Wzór rejestru stanowi Załącznik nr 6 do Polityki.
4. Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.
5. Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
6. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na wniosek następuje w terminie 30 dni od daty jego otrzymania.
7. Odmowa udostępnienia danych osobowych następuje wówczas, gdy spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

14. Powierzanie przetwarzania danych osobowych

1. ADO może powierzyć przetwarzanie danych osobowych innemu podmiotowi zewnętrznemu w drodze umowy zawartej na piśmie, w tym w formie elektronicznej, której wzór stanowi Załącznik nr 7 do Polityki.
2. Szczegółowy wykaz zbiorów danych osobowych oraz podmiotów, którym dane osobowe są powierzane do przetwarzania znajduje się w Załączniku nr 8 do Polityki.
3. Przekazanie zbiorów podmiotowi zewnętrznemu w celu ich przetwarzania nie powoduje zmiany właściwego ADO.
4. Jeżeli przetwarzanie ma być dokonywane w imieniu ADO, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
5. Podmiot przetwarzający nie może skorzystać z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym Administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.
6. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych osobowych obowiązany jest wykorzystywać powierzone mu dane wyłącznie w celach i w zakresie, które zostały wskazane w zawartej z nim umowie, jak również zachować poufność danych osobowych powierzonych mu do przetwarzania.
7. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych obowiązany jest między innymi do:
    a) stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
    b) opracowania i wdrożenia dokumentacji dotyczącej przetwarzania i ochrony danych osobowych,
    c) zapewnienia, aby do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez ADO,
    d) prowadzenia ewidencji osób upoważnionych do przetwarzania danych,
    e) zobowiązania osób, które zostały upoważnione do przetwarzania danych osobowych do zachowania w tajemnicy tych danych oraz sposobów i zabezpieczania.
    f) zapewnienia kontroli nad tym jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane,
    g) poinformowania ADO o sytuacji podpowierzenia oraz wskazania w umowie nazwy podmiotu wraz z danymi teleadresowymi, któremu zostaną podpowierzone dane osobowe.

15. Bezpieczeństwo

1. Podmiot zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Podmiot.
   Analizy ryzyka i adekwatności środków bezpieczeństwa
2. Podmiot przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:
3. Podmiot zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
4. Podmiot kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
5. Podmiot przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Podmiot analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
6. Podmiot ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Podmiot ustala przydatność i stosuje takie środki i podejście jak:
   a) pseudonimizacja,
   b) szyfrowanie danych osobowych,
   c) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnieniapoufności, integralności, dostępności i odporności systemów i usług przetwarzania,
   d) środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

   Oceny skutków dla ochrony danych
7. Podmiot dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.
8. Podmiot stosuje metodykę oceny skutków przyjętą w Podmiocie.
   Środki bezpieczeństwa
9. Podmiot stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.
10. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w Podmiocie i są bliżej opisane w procedurach przyjętych przez Podmiot dla tych obszarów.
    Zgłaszanie naruszeń
11. Podmiot stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

16. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Zabezpieczenia organizacyjne:
   a) została opracowana i wdrożona polityka ochrony,
   b) została opracowana i wdrożona instrukcja zarządzania systemem informatycznym,
   c) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez ADO,
   d) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych,
   e) członkowie personelu oraz inne osoby przetwarzające dane osobowe zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,
   f) członkowie personelu oraz inne osoby przetwarzające dane osobowe obowiązane zostały do zachowania ich w tajemnicy,
   g) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
   h) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych,
   i) stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe,
   j) przeprowadza się regularne przeglądy Polityki oraz Instrukcji,
   k) przekazywanie danych osobowych do podmiotów trzecich (udostępnianie i powierzanie) jest nadzorowane oraz odbywa się na zasadach zgodnych z przepisami prawa.
2. Zabezpieczenia ochrony fizycznej danych osobowych opisane są w Załączniku 14 do Polityki.
3. Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej stosowana są do fizycznych elementów systemu, ich połączeń oraz systemów operacyjnych. Szczegółowy opis zabezpieczeń zawarty jest w Instrukcji.
4. Zabezpieczenia narzędzi programowych i baz danych (techniczne i programowe) stosuje się dla procedur, aplikacji, programów i innych narzędzi programowych przetwarzających dane osobowe. Szczegółowy opis zabezpieczeń zawarty jest w Instrukcji.

17. Procedura analizy ryzyka i plan postępowania z ryzykiem

1. Analizę ryzyka dla zasobów biorących udział w procesach przeprowadza Administrator danych z wykorzystaniem Załącznika nr 15 do Polityki.
2. Analiza ryzyka jest przeprowadzana nie rzadziej niż raz w roku i stanowi podstawę do aktualizacji sposobu postępowania z ryzykiem.
3. Na podstawie wyników przeprowadzonej analizy ryzyka Administrator danych wdraża sposoby postępowania z ryzykiem.
4. Każdorazowo Administrator danych wybiera sposób postępowania z ryzykiem i określa, które ryzyka i w jakiej kolejności będą rozpatrywane jako pierwsze.

18. Eksport danych

1. Podmiot rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy (EOG w 2017 = Unia Europejska, Islandia, Lichtenstein i Norwegia).
2. Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych (shadow IT), Podmiot okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.

19. Projektowanie prywatności

1. Podmiot zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.
2. W tym celu zasady prowadzenia projektów i inwestycji przez Podmiot odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowania bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

20. Procedura DPIA (Data Protection Impact Assessment)

1. ADO dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych tam, gdzie zgodnie z analizą ryzyka, ryzyko naruszenia praw i wolności jest wysoki.
2. DPIA jest przeprowadzana przy każdorazowej istotnej zmianie procesu przetwarzania danych osobowych, np. zmiana dostawcy usług, zmiana sposobu przetwarzania danych, wymiana zasobów biorących udział w procesie.
3. DPIA jest przeprowadzana wraz z analizą ryzyka nie rzadziej niż raz w roku w stosunku do procesów, które w wyniku poprzednio przeprowadzonego DPIA wykazały wysokie ryzyko dla praw i wolności osób, których dane dotyczą.
   Środki bezpieczeństwa
4. ADO stosuje środki bezpieczeństwa ustalone w ramach analizy ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.
5. Środki bezpieczeństwa danych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w Podmiocie.

21. Procedura postępowania w przypadku naruszenia bezpieczeństwa danych osobowych

1. Naruszeniem ochrony danych osobowych jest naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, a w szczególności:
   a) nieautoryzowany dostęp do danych,
   b) utrata nośników,
   c) nieautoryzowane modyfikacje lub zniszczenie danych,
   d) udostępnianie danych nieautoryzowanym podmiotom,
   e) nielegalne ujawnianie danych,
   f) pozyskiwanie danych z nielegalnych źródeł.
2. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy członek personelu jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie ADO lub bezpośredniego przełożonego, a następnie stosować się do podjętych przez nich decyzji.
3. Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:
   a) opis symptomów naruszenia ochrony danych osobowych,
   b) określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych,
   c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę tego naruszenia,
   d) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.
4. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   b) niewłaściwe zabezpieczenie sprzętu IT lub oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   c) nieprzestrzeganie zasad ochrony danych osobowych przez personel.
5. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),
   c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
6. W przypadku stwierdzenia wystąpienia zagrożenia lub incydentu ADO prowadzi postępowanie wyjaśniające, w toku, którego ustala przyczynę zaistniałego zagrożenia lub incydentu, wskazuje jakie są jego potencjalne skutki oraz jakie działania należy podjąć w celu naprawy tego stanu.
7. ADO ustala również osoby odpowiedzialne za naruszenie oraz zabezpiecza dowody w danej sprawie i dokumentuje swoje ustalenia.

8. ADO jest także odpowiedzialny za analizę incydentów bezpieczeństwa lub zagrożeń ochrony danych osobowych w celu ustalenia, czy istnieje konieczność podjęcia działań korygujących lub zapobiegawczych. Jeśli ADO taką potrzebę stwierdza, określa źródło powstania incydentu lub zagrożenia, zakres działań korygujących lub zapobiegawczych, termin realizacji oraz osobę odpowiedzialną.
9. ADO jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych.
10. W przypadku naruszenia ochrony danych osobowych, ADO bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
11. Zgłoszenie, o którym mowa w pkt. 10, musi co najmniej:
    a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie
    b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
    c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
    d) opisywać środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
12. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie i bez zbędnej zwłoki.
13. Wszystkie powyższe czynności są przez ADO rejestrowane. ADO po opanowaniu sytuacji nadzwyczajnej opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości; wzór raportu końcowego stanowi Załącznik nr 16 do Polityki.
14. Rejestr naruszeń stanowi Załącznik nr 17 do Polityki.
15. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
16. Zawiadomienie, o którym mowa w ust. 15, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w 15.
17. Zawiadomienie, o którym mowa w ust. 15, nie jest wymagane, w następujących przypadkach:
    a) Administrator 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 zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w pkt. a);

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.

18. Jeżeli Administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 17.
19. Schemat postępowania w przypadku naruszenia ochrony danych osobowych stanowi Załącznik nr 21 do Polityki.
20. Lista kontrolna -jak postąpić w przypadku naruszenia ochrony danych stanowi Załącznik nr 22 do Polityki.

22. Przeglądy Polityki i audyty systemu

1. Polityka powinna być poddawana przeglądowi/sprawdzeniu przynajmniej raz na rok pod kątem ich aktualności oraz zgodności deklarowanego w nich stanu z prawem. W razie istotnych zmian dotyczących przetwarzania danych osobowych ADO może zarządzić przegląd Polityki stosownie do potrzeb.
2. Do kontroli stanu ochrony danych osobowych w Podmiocie upoważnieni są:
   a) ADO,
   b) osoby wyznaczone przez ADO.
3. ADO analizuje, czy Polityka i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:
   a) zmian w budowie systemu informatycznego,
   b) zmian organizacyjnych ADO, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
   c) zmian w obowiązującym prawie.
4. Raz do roku kontroli podlegają wszystkie systemy informatyczne przetwarzające dane osobowe oraz zabezpieczenia fizyczne i bezpieczeństwo osobowe.
5. ADO przygotowuje plan kontroli uwzględniając zakres oraz potrzeby fizyczne, czasowe i osobowe.
6. Kontroli podlega sprzęt, system teleinformatyczny, realizacja zabezpieczeń oraz przestrzeganie Polityki.
7. ADO może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych.
8. Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole.
9. ADO może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot. Wzór sprawozdania stanowi Załącznik nr 18 do Polityki.

23. Postanowienia końcowe

1. Niniejsza Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.
2. Użytkownik zobowiązany jest złożyć oświadczenie o tym, iż został zapoznany z przepisami Rozporządzenia oraz instrukcjami obowiązującymi u ADO, a także o zobowiązaniu się do ich przestrzegania.
3. Oświadczenie potwierdzające zaznajomienie użytkownika z przepisami prawa dotyczącymi ochrony danych osobowych oraz instrukcjami obowiązującymi u ADO, a także o zobowiązaniu się do ich przestrzegania, przechowywane jest w aktach osobowych pracownika.
4. Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
5. Wszyscy upoważnieni zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.
6. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane stanowić mogą podstawę do pociągnięcia danej osoby do odpowiedzialności, adekwatnie do łączącego ją z ADO stosunku prawnego
7. W sprawach nieuregulowanych w Instrukcji mają zastosowanie przepisy Rozporządzenia oraz innych aktów, w tym wykonawczych.

Lista załączników do Polityki

1. Zał. nr 1 do Polityki-Karta szkolenia z zakresu ochrony danych osobowych
2. Zał. nr 2 do Polityki-Upoważnienie do przetwarzania danych
3. Zał. nr 3a do Polityki-Oświadczenie o poufności-personel
4. Zał. nr 3b do Polityki- Oświadczenie o poufności-personel techniczny, sprzątający
5. Zał. nr 4 do Polityki- Ewidencja upoważnień
6. Zał. nr 5 do Polityki-wniosek o udostępnienie danych
7. Zał. nr 6 do Polityki-Rejestr udostępnień
8. Zał. nr 7 do Polityki-wzór umowy powierzenia przetwarzania danych osobowych
9. Zał. nr 8 do Polityki-Rejestr powierzeń
10. Zał. nr 9 do Polityki-wzór klauzuli informacyjnej 1
11. Zał. nr 10 do Polityki-wzór klauzuli informacyjnej 2
12. Zał. nr 11 do Polityki-wzór klauzuli zgody na przetwarzanie danych
13. Zał. nr 12 do Polityki-Rejestr czynności przetwarzania
14. Zał. nr 13 do Polityki- Lista kontrolna - wyznaczenie inspektora ochrony danych
15. Zał. nr 14 do Polityki-Zasady ochrony pomieszczeń
16. Zał. nr 15 do Polityki-Analiza ryzyka
17. Zał. nr 16 do Polityki-wzór raportu z naruszenia ochrony danych
18. Zał. nr 17 do Polityki-rejestr naruszeń ochrony danych osobowych
19. Zał. nr 18 do Polityki-Sprawozdanie ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ich ochronie
20. Zał. nr 19 do polityki-Rejestr realizacji żądań podmiotu danych
21. Zał. nr 20 do Polityki-Wniosek o przeniesienie danych
22. Zał. nr 21 do Polityki- Schemat postępowania w przypadku naruszenia ochrony danych osobowych
23. Zał. nr 22 do Polityki- Lista kontrolna -jak postąpić w przypadku naruszenia ochrony danych