DO UŻYTKU WEWNĘTRZNEGO

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH MOSTOSTAL SIEDLCE

Polityka Bezpieczeństwa Danych Osobowych w Mostostal Siedlce 1
§ 1 Postanowienia ogólne 2
§ 2 Słownik pojęć 3
§ 3 Główne elementy systemu ochrony danych osobowych ADO 7
§ 4 Dane osobowe przetwarzane przez ADO 8
§ 5 Upoważnienie do przetwarzania danych osobowych 10
§ 6 Przetwarzanie danych osobowych przez ADO 12
§ 7 Sposób wykonania obowiązków informacyjnych 14
§ 8 Prawa osób, których dane dotyczą 14
§ 9 Udostępnianie danych osobowych innym podmiotom 18
§ 10 Powierzanie przetwarzania danych osobowych 18
§ 11 Przekazanie danych osobowych do państwa trzeciego 19
§ 12 Przetwarzanie danych osobowych poza miejscem przetwarzania 19
§ 13 Przetwarzanie danych w systemie informatycznym 19
§ 14 Sposób przepływu danych pomiędzy systemami informatycznymi 20
§ 15 Przetwarzanie danych osobowych znajdujących się na nośnikach papierowych 21
§ 16 Usuwanie danych osobowych 21
§ 17 Uruchamianie nowych projektów 22
§ 18 Zabezpieczenie danych osobowych 22
§ 19 Postępowanie w przypadku naruszenia ochrony danych osobowych 26
§ 20 Odpowiedzialność za naruszenie 26
§ 21 Szkolenia z zakresu ochrony danych osobowych 27
§ 22 Analiza ryzyka 27
§ 23 Przeglądy Polityki bezpieczeństwa danych osobowych 30
§ 23 Wykaz dokumentów związanych 30
Załączniki 31

§ 1

POSTANOWIENIA OGÓLNE

I. Podstawy prawne, cele Polityki Bezpieczeństwa Danych Osobowych i jej wdrożenie, zakres zastosowania

1. Polityka Bezpieczeństwa Danych Osobowych („**Polityka Bezpieczeństwa DO**" lub „**Polityka**") stanowi wykonanie obowiązków wynikających z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
2. Polityka została opracowana w celu:
   a) określenia zasad przetwarzania danych osobowych w Mostostal Siedlce spółka z ograniczoną odpowiedzialnością sp. k. z siedzibą w Siedlcach;
   b) wskazania stosowanych środków technicznych i organizacyjnych zapewniających bezpieczne przetwarzanie danych osobowych;
   c) wdrożenia procedur oraz reguł postępowania, które należy stosować żeby właściwie wykonywać obowiązki administratora danych osobowych, w szczególności zapewnienia, aby dane osobowe były przetwarzane zgodnie z zasadami wynikającymi z obowiązujących przepisów;
   d) budowania wśród pracowników i współpracowników wiedzy dotyczącej ochrony danych osobowych.
3. Odpowiedzialność za wdrożenie Polityki i jej utrzymanie spoczywa na Mostostal Siedlce spółka z ograniczoną odpowiedzialnością sp. k. z siedzibą w Siedlcach .
4. Za stosowanie Polityki Bezpieczeństwa DO w codziennej działalności operacyjnej odpowiedzialni są także pracownicy i współpracownicy Mostostal Siedlce spółka z ograniczoną odpowiedzialnością sp. k. z siedzibą w Siedlcach.
5. W przypadku, w którym dochodzi do przekazania danych osobowych podmiotom trzecim, należy zapewnić zgodność postępowania tych podmiotów z Polityką.
6. Polityka ma zastosowanie w stosunku do wszystkich pracowników i współpracowników Mostostal Siedlce spółka z ograniczoną odpowiedzialnością sp. k. z siedzibą w Siedlcach. Polityka ma również zastosowanie do osób trzecich, mających na zlecenie Mostostal Siedlce spółka z ograniczoną odpowiedzialnością sp. k. z siedzibą w Siedlcach dostęp do danych osobowych.
7. Polityka ma zastosowanie do wszystkich danych osobowych przetwarzanych przez Mostostal Siedlce spółka z ograniczoną odpowiedzialnością sp. k. z siedzibą w Siedlcach niezależnie od formy ich przetwarzania (elektronicznej lub papierowej).
8. Polityka ma zastosowanie do procesów danych osobowych administrowanych przez Polimex Mostostal S.A. z siedzibą w Warszawie a użytkowanych przez Mostostal Siedlce spółka z ograniczoną odpowiedzialnością spółka komandytowa, jak również zbiorów danych osobowych będących własnością stron trzecich, o ile dane osobowe wchodzące w ich skład zostały przekazane Mostostal Siedlce spółka z ograniczoną

odpowiedzialnością sp. k. z siedzibą w Siedlcach na podstawie umowy powierzenia lub równoważnego instrumentu prawnego i mają charakter poufny.

9. Polityka jest dokumentem nadrzędnym dla wszystkich pozostałych dokumentów dotyczących ochrony danych osobowych.
10. Polityka jest dokumentem podrzędnym w stosunku do obowiązujących Mostostal Siedlce spółka z ograniczoną odpowiedzialnością sp. k. z siedzibą w Siedlcach przepisów prawa, w szczególności Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 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) i musi zostać do nich dostosowana w przypadku stwierdzenia jej niezgodności z tymi przepisami, w szczególności w przypadku zmiany obowiązujących przepisów.
11. Polityka jak i cała dokumentacja ochrony danych osobowych powinna być aktualizowana przez Mostostal Siedlce spółka z ograniczoną odpowiedzialnością sp. k. z siedzibą w Siedlcach w celu zapewnienia jej zgodności z wytycznymi właściwych organów nadzoru, w tym w szczególności Prezesa Urzędu Ochrony Danych Osobowych jak i Europejskiej Rady Ochrony Danych.
12. Polityka oraz tworzona na jej podstawie dokumentacja ochrony danych osobowych mają charakter wewnętrzny, co oznacza, że nie mogą być one udostępniane jakimkolwiek podmiotom trzecim bez pisemnej zgody Mostostal Siedlce spółka z ograniczoną odpowiedzialnością sp. k. z siedzibą w Siedlcach.

§ 2

SŁOWNIK POJĘĆ

Pojęcia występujące w Polityce Bezpieczeństwa DO mają następujące znaczenie:

RODO	oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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)
PxM lub **Polimex**	oznacza Polimex Mostostal S.A. z siedzibą w Warszawie, al. Jana Pawła II 12, 00-124 Warszawa, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS: 22460, NIP: 8210014509, REGON: 710252031, kapitał zakładowy: 473.237.604,00 złotych wpłacony w całości
Spółka, Mostostal Siedlce lub MS	oznacza Mostostal Siedlce spółka z ograniczoną odpowiedzialnością sp. k.

Administrator Danych Osobowych lub **ADO**	oznacza MS jako administratora danych osobowych w rozumieniu art. 4 pkt 7) RODO, jak również osoby sprawujące faktyczny zarząd ADO
ustawa o ochronie danych osobowych	oznacza ustawę z 10.05.2018 o ochronie danych osobowych
PUODO	oznacza Prezesa Urzędu Ochrony Danych Osobowych
EROD	oznacza Europejską Radę Ochrony Danych
IOD	oznacza osobę wyznaczoną w Spółce do nadzoru nad przestrzeganiem zasad ochrony danych osobowych w Spółce
Koordynator ochrony danych osobowych (KODO)	oznacza osobę wyznaczoną przez ADO lub osobę wyznaczoną przez Dyrektora Spółki/inną osobę na polecenie ADO w uzgodnieniu z IOD w celu sprawowania nadzoru nad przestrzeganiem zasad ochrony danych osobowych w danej lokalizacji i zobowiązaną do współpracy z IOD, ADO i Administratorem Systemów Informatycznych w tym zakresie. ADO za pośrednictwem IOD prowadzi rejestr KODO
Administrator Systemów Informatycznych (ASI)	oznacza osobę wyznaczoną przez Dyrektora Biura Informatyki PxM w celu administrowania, stosowania zabezpieczeń oraz sprawowania nadzoru nad zabezpieczeniem systemów informatycznych, w których przetwarzane są dane osobowe
Pracownik lub **Pracownicy**	oznacza cały personel Spółki/Spółek zatrudniony w ramach stosunku pracy jak i na podstawie umów cywilnoprawnych
Zbiór	oznacza jakikolwiek zbiór danych osobowych w rozumieniu art. 4 pkt 6 RODO
Incydent	oznacza zdarzenie, którego skutki mogą zagrozić integralności, poufności, legalności przetwarzania lub bezpieczeństwu danych osobowych
dane osobowe	oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej

dane wrażliwe lub **dane szczególnej kategorii**	oznaczają dane osobowe szczególnych kategorii wymienione w art. 9 oraz 10 RODO, tj. dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej, dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym
przetwarzanie danych osobowych	oznacza 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
powierzenie przetwarzania danych osobowych	oznacza zlecenie przez ADO innemu podmiotowi wykonywania czynności związanych z przetwarzaniem danych osobowych
profilowanie	oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się
pseudonimizacja	oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji
usuwanie danych osobowych lub anonimizacja	oznacza niszczenie danych osobowych lub ich anonimizację
nośnik	oznacza materiały, na których przechowywane są dane osobowe takie jak w szczególności serwery własne lub podwykonawców, zawierające macierze dyskowe, dyski twarde, dyskietki, płyty CD, taśmy, pamięć flash, smarthphony, ale również kartki papieru, zdjęcia

utrwalanie danych osobowych	oznacza zapisanie danych osobowych na jakimkolwiek nośniku w tym skopiowanie lub przegranie zbiorów informacji
miejsce przetwarzania danych osobowych	oznacza budynki, pomieszczenia lub części pomieszczeń, a także lokalizacje w których są przetwarzane dane osobowe w formie papierowej i/lub elektronicznej określone w Załączniku nr 1 do Polityki
osoba upoważniona do przetwarzania danych osobowych	oznacza osobę, której ADO nadał pisemne upoważnienie do przetwarzania danych osobowych, i która została zobowiązana do zachowania w tajemnicy danych osobowych oraz sposobów ich przetwarzania
odbiorca danych osobowych	oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią
System informatyczny (SI)	oznacza zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych
Sieć publiczna	oznacza sieć telekomunikacyjną wykorzystywaną do świadczenia publicznie dostępnych usług telekomunikacyjnych
dostawca/podwykonawca	oznacza podmiot trzeci, od którego ADO nabywa towary lub usługi, niebędący pracownikiem ADO, który może przetwarzać dane osobowe w związku z wykonaniem umowy z ADO
RCPD	oznacza rejestr czynności przetwarzania danych
Aktywa	oznaczają kontrolowane przez ADO zasoby majątkowe o wiarygodnie określonej wartości, uzyskane w wyniku zdarzeń, które spowodują wpływ do ADO korzyści ekonomicznych
Identyfikowanie ryzyka	oznacza szereg czynności polegających na określeniu sytuacji, które mogą się wydarzyć powodując straty/naruszenie
Kontekst	oznacza informacje związane z działalnością ADO, m.in. przepisy dotyczące ochrony danych, środowiska technologicznego, społecznego, finansowego i innego ADO
Akceptacja ryzyka	oznacza określenie dopuszczalności danego ryzyka definiowane przez wartość progową przy przedziałach ryzyka

Naruszenie ochrony danych	oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przechowywanych, przesyłanych lub w inny sposób przetwarzanych
Ocena ryzyka	oznacza czynności polegające na porównaniu wyników uzyskanych podczas analizy ryzyka z kryteriami oceny ryzyka określonymi na etapie ustanawiania kontekstu działania ADO
Szacowanie ryzyka	oznacza całościowy proces identyfikacji ryzyka, analizy ryzyka oraz oceny ryzyka przy uwzględnieniu treści dotyczących Szacowania ryzyka zawartych w § 22
Zabezpieczenie	oznacza środek, którego celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia.

§ 3

GŁÓWNE ELEMENTY SYSTEMU OCHRONY DANYCH OSOBOWYCH ADO

1. Na System ochrony danych osobowych ADO składają się:

   a) identyfikacja zasobów

   - ADO dokonuje identyfikacji zasobów danych osobowych, kategorii danych osobowych, sposobów ich wykorzystywania, w tym przypadków przetwarzania danych wrażliwych, przypadków przetwarzania danych osobowych dzieci i profilowania,

   b) rejestry

   - ADO prowadzi rejestr czynności przetwarzania danych osobowych, który jest podstawowym kompendium wiedzy o procesach przetwarzania danych osobowych zachodzących u ADO, w jaki sposób i kto je przetwarza. ADO prowadzi rejestr naruszeń, w którym dokumentowane są Incydenty dotyczące danych osobowych, ewidencję upoważnień, rejestr żądań podmiotów danych,

   c) realizacja praw i wolności osób, których dane dotyczą

   - ADO spełnia obowiązki informacyjne względem osób, których dane osobowe przetwarza, oraz zapewnia realizację ich praw i wolności, rozpatrując otrzymane w tym zakresie żądania, w tym w szczególności: **(i)** ADO przekazuje osobom, których dane dotyczą wymagane informacje, zarówno przy zbieraniu danych osobowych jak i w innych sytuacjach; **(ii)** ADO weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich podwykonawców; **(iii)** ADO zapewnia odpowiednie zasoby i procedury, aby żądania osób, których dane dotyczą były realizowane w terminach i w sposób wymagany przez RODO; **(iv)** ADO stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych osobowych,

d) monitorowanie

- ADO dokonuje regularnych sprawdzeń systemu ochrony danych osobowych przyjętego w Spółce, w tym poprzez audyt/weryfikację środków technicznych i organizacyjnych,

e) *privacy by design*

- ADO uwzględnia kwestie ochrony danych osobowych już w fazie projektowania nowych rozwiązań, i procesów,

f) bezpieczeństwo i zasada *privacy by default*

- ADO domyślnie zapewnia odpowiedni poziom ochrony danych osobowych, w szczególności poprzez przeprowadzanie analizy ryzyka dla czynności przetwarzania, przeprowadzanie oceny skutków dla ochrony Danych Osobowych (DPIA) tam, gdzie ryzyko naruszenia praw i wolności osób zostało wskazane jako wysokie, czy zarządzania Incydentami,

g) budowanie wiedzy

- ADO zwiększa świadomość swojego personelu szkoląc Pracowników z zakresu ochrony Danych Osobowych, w tym z zasad wprowadzonych Polityką,

h) weryfikacja podwykonawcy/dostawcy

- ADO weryfikuje dostawców przetwarzających dane osobowe w imieniu i na rzecz ADO w zakresie spełniania przez nich wymogów bezpiecznego i zgodnego z prawem przetwarzania danych osobowych. ADO zawiera stosowne umowy powierzenia przetwarzania danych osobowych. Aspekty te reguluje szczegółowo Polityka dotycząca umów zawieranych przez Spółkę, w tym umów powierzenia przetwarzania danych osobowych stanowiąca Załącznik nr 2 do Polityki,

i) eksport danych

- ADO w zakresie w jakim zastosowanie będzie miało przekazywanie danych osobowych do państw trzecich, tj. poza EOG (Europejski Obszar Gospodarczy) dba o zapewnienie odpowiedniego poziomu ochrony, w tym w szczególności poprzez zawieranie stosownych klauzul umownych zatwierdzonych przez Komisję Europejską.

2. W zakresie pkt. 1. powyżej, uprawnionym do reprezentowania i prowadzenia spraw jest ADO, który:

a) wykonuje ustawowe obowiązki z zakresu bezpieczeństwa danych osobowych samodzielnie przy współpracy z IOD lub za pośrednictwem KODO, czy ASI, bądź innych osób, których zlecił realizację zadań z pkt. 1.

§ 4

DANE OSOBOWE PRZETWARZANE PRZEZ ADO

I. Rejestr czynności przetwarzania

1. RCPD z chwilą jego utworzenia przez ADO jest podstawowym źródłem wiedzy o przetwarzanych w Spółce danych osobowych. Ponadto stanowi formę dokumentowania czynności przetwarzania danych osobowych,

pełni rolę mapy przetwarzania i jest jednym z kluczowych elementów umożliwiających realizację zasady rozliczalności. Wzór RCPD stanowi Załącznik nr 9 do Polityki. RCPD jest utrzymywany za ADO przez Zastępcę IOD przy współpracy z KODO i ASI.

2. W RCPD, dla każdej czynności przetwarzania, wskazuje się co najmniej:
   a) jaka jest podstawa prawna przetwarzania, wraz z wyszczególnieniem kategorii, uzasadnionego interesu ADO, jeśli podstawą jest uzasadniony prawnie interes,
   b) w jakich celach dane są przetwarzane,
   c) opis kategorii osób, których dotyczy przetwarzanie,
   d) jakie czynności składają się na przetwarzanie,
   e) opis kategorii odbiorców danych osobowych,
   f) czy dochodzi do transferu danych osobowych,
   g) czy dochodzi do powierzenia przetwarzania danych osobowych.
3. RCPD może zawierać także informacje dodatkowe, gdyż jako podstawowe źródło wiedzy o aktualnym na dany dzień przetwarzaniu danych osobowych w Spółce, jest uzupełniany o dane prawem niewymagane, ale istotne z perspektywy zasady rozliczalności.

II. Identyfikacja Zbiorów

1. ADO przy współpracy z IOD, Zastępcą IOD lub za pośrednictwem KODO, czy ASI dokonuje ciągłej identyfikacji i inwentaryzacji Zbiorów danych osobowych.
2. Raz w roku kalendarzowym, w trakcie przeprowadzania audytu przetwarzania danych osobowych w Działalności, ADO za pośrednictwem IOD, przy jego współpracy z KODO i ASI weryfikuje jakie kategorie danych są w Spółce przetwarzane, w ramach jakich czynności i procesów przetwarzania, w tym w szczególności, czy dochodzi do przetwarzania danych osobowych dotychczas niezidentyfikowanych i niewpisanych do RCPD.

III. Aktualizacja Zbiorów i czynności przetwarzania

1. Pracownik Spółki, który zauważy potrzebę uwzględnienia nowego Zbioru danych osobowych lub czynności przetwarzania danych osobowych, innych niż te, które znajdują się w RCPD, zobowiązany jest zgłosić ten fakt swojemu bezpośredniemu przełożonemu. Przełożony następnie informuje o tym IOD lub Zastępcę IOD.
2. Pracownik Spółki informuje Zastępcę IOD o zamiarze zbierania nowej kategorii danych osobowych przed rozpoczęciem nowych czynności przetwarzania danych osobowych lub pozyskaniem ich z innego źródła aniżeli bezpośrednio od osoby, której dotyczą.
3. Decyzję o uwzględnieniu nowego Zbioru lub czynności i wpisaniu ich do RCPD podejmuje IOD lub Zastępca IOD, który w razie konieczności informuje o tym ADO.

4. Informując o potrzebie uwzględnienia nowego Zbioru danych osobowych lub czynności przetwarzania, Pracownik zobowiązany jest przedstawić wszelkie informacje na temat tworzonego Zbioru, o które poprosi Zastępca IOD/ADO a w szczególności informacje na temat: kategorii osób, których dane osobowe będą przetwarzane w nowym Zbiorze, kategorii danych osobowych oraz celu ich przetwarzania.

IV. Aktualizacja RCPD

1. Aktualizacje RCPD przeprowadza na bieżąco ADO za pośrednictwem Zastępcy IOD na podstawie informacji uzyskiwanych bezpośrednio od Pracowników, na podstawie własnych obserwacji lub z innych wiarygodnych źródeł.

§ 5

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

I. Udzielanie upoważnień

1. Do przetwarzania danych osobowych mogą być dopuszczeni wyłącznie Pracownicy posiadający upoważnienie do przetwarzania danych osobowych nadane przez ADO.
2. W przypadku konieczności udzielenia przez ADO upoważnienia do przetwarzania danych osobowych osobie innej niż Pracownik ADO, postanowienia niniejszego Rozdziału stosuje się odpowiednio.
3. Upoważnienia mogą być nadawane przez osobę wyznaczoną do tego przez ADO (Dział Kadr i Płac). Wzory upoważnień do przetwarzania danych stanowią Załącznik nr 3 do Polityki.
4. Upoważnienie do przetwarzania danych osobowych nadawane jest w momencie zatrudnienia Pracownika (najpóźniej z chwilą wpływu do Działu Kadr I Płac wniosku przełożonego Pracownika o nadanie upoważnienia).
5. Upoważnienia nadawane są Pracownikom, którzy spełnią wymagania określone w pkt. II. poniżej i na wniosek. Wzór wniosku o nadanie upoważnienia do przetwarzania danych osobowych stanowi Załącznik nr 4 do Polityki.
6. Kopie udzielonych upoważnień oraz kopie podpisanych przez Pracowników oświadczeń o zachowaniu poufności przechowywane są przez ADO. ADO za pośrednictwem działu Kadr i Płac prowadzi ewidencję udzielonych upoważnień według wzoru stanowiącego Załącznik nr 5 do Polityki.
7. Dział Kadr i Płac ADO odpowiada za bieżące informowanie o wszelkich zmianach w zatrudnieniu Pracowników.
8. Zabronione jest przetwarzanie danych osobowych przez osobę, która nie posiada upoważnienia do przetwarzania danych osobowych.
9. Pracownik, któremu nadano upoważnienie do przetwarzania danych osobowych, może przetwarzać dane osobowe wyłącznie w zakresie i w sposób wynikający z powierzonych mu zadań.
10. Jeśli upoważnienie dotyczy przetwarzania danych osobowych przez Pracownika także w Systemie Informatycznym, przełożony Pracownika na podstawie ustaleń z ASI/Biurem Informatyki, występuje do Działu Kadr i Płac w celu nadania Pracownikowi upoważnienia, uwzględniając dostępy i uprawnienia informatyczne.

11. Upoważnienia do przetwarzania danych osobowych, o których mowa w niniejszym punkcie, są archiwizowane w aktach osobowych poszczególnych Pracowników.
12. KODO lub bezpośredni przełożony Pracownika jest zobowiązany do przesyłania do Działu Kadr i Płac informacji o każdej zmianie osób upoważnionych do przetwarzania danych osobowych (na podstawie informacji uzyskanych od kierowników komórek organizacyjnych i ASI), w terminie do 15. dnia miesiąca następującego po miesiącu, w którym wystąpiła zamiana.

II. Wymagania w zakresie dopuszczenia Pracownika do przetwarzania danych osobowych

1. Każdy Pracownik, który ma być dopuszczony przez ADO do przetwarzania danych osobowych, przed uzyskaniem upoważnienia do ich przetwarzania powinien:
   a) zapoznać się z Polityką;
   b) złożyć oświadczenie o zachowaniu poufności danych osobowych oraz sposobów ich zabezpieczenia stosowanych w Spółce, zgodnie z wzorem stanowiącym Załącznik nr 6 do Polityki.
2. Każdy Pracownik przed otrzymaniem upoważnienia do przetwarzania danych osobowych, a jeśli nie będzie to możliwe, po otrzymaniu upoważnienia do przetwarzania danych osobowych powinien odbyć co najmniej podstawowe szkolenie z zakresu prawa ochrony danych osobowych. Szkolenie powinno nastąpić najpóźniej w ciągu 2 miesięcy od daty udzielenia upoważnienia do przetwarzania danych osobowych.

§ 6

PRZETWARZANIE DANYCH OSOBOWYCH PRZEZ ADO

I. Czynności przetwarzania danych osobowych i podstawy prawne

1. Przez przetwarzanie danych osobowych rozumie się wykonywanie jakichkolwiek operacji na danych osobowych w Spółce, czy to w sposób zautomatyzowany w Systemie informatycznym czy w sposób niezautomatyzowany, w tym 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.
2. Przetwarzanie danych osobowych możliwe jest wyłącznie w oparciu o jedną z podstaw prawnych wskazanych w art. 6 ust. 1 lit. a) - f) RODO, co oznacza, że przetwarzanie tych danych jest dopuszczalne tylko wtedy:
   a) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub w większej liczbie określonych celów,
   b) przetwarzanie danych osobowych jest niezbędne do wykonania umowy, gdy osoba, której dane dotyczą jest jej stroną, lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
   c) przetwarzanie danych osobowych jest niezbędne do wypełnienia obowiązku prawnego ciążącego na ADO,
   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 ADO,

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO 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.

3. Przetwarzanie danych wrażliwych jest dopuszczalne wyłącznie w przypadkach wskazanych w art. 9 ust. 2 RODO, w szczególności, jeżeli osoba, której dane dotyczą, wyrazi na to wyraźną zgodę w jednym lub kilku konkretnych celach. Przetwarzanie danych dotyczących wyroków skazujących i naruszeń prawa dopuszczalne jest tylko na zasadach wskazanych w art. 10. RODO.

4. Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel ADO) Spółka dookreśla podstawę w czytelny sposób, gdy jest to potrzebne. Np. dla zgody wskazując na jej zakres, gdy podstawą jest wykonanie obowiązku – w miarę możliwości wskazując na konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując na kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń.

5. ADO za pośrednictwem IOD wdraża metody zarządzania zgodami na przetwarzanie danych osobowych umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej danych osobowych w konkretnym celu, oraz rejestrację odmowy zgody, cofnięcia zgody i innych czynności gwarantujących możliwość wykonywania praw i wolności osoby, której dane dotyczą.

6. Pracownik, który został upoważniony do przetwarzania danych osobowych powinien znać podstawy prawne, na jakich Spółka dokonuje konkretnych czynności przetwarzania.

II. Zbieranie danych osobowych

1. ADO zbiera dane osobowe wyłącznie wtedy, gdy ich przetwarzanie jest dopuszczalne zgodnie z RODO lub innymi obowiązującymi przepisami prawa.

2. Zbieranie danych osobowych dokonywane jest dla oznaczonych przez ADO przy współpracy z IOD lub Zastępcą IOD, skonkretyzowanych, zgodnych z prawem celów.

3. Rozpoczęcie zbierania danych osobowych powinno być zaopiniowane przez IOD lub Zastępcę IOD.

4. Zbierając dane osobowe, Spółka zobowiązana jest wykonać obowiązek informacyjny wobec osób, których dane dotyczą zgodnie z art. 13 RODO (w przypadku, gdy dane osobowe są zbierane od tych osób) lub zgodnie z art. 14 RODO (w przypadku, gdy dane osobowe są zbierane z innych źródeł niż osoby, których dane dotyczą). Wzory przykładowych klauzul informacyjnych stanowią Załącznik nr 7 do Polityki – są one jedynie poglądowe, a każda klauzula informacyjna powinna zostać dostosowana na potrzeby procesu przetwarzania danych osobowych w Spółce.

§ 7

SPOSÓB WYKONANIA OBOWIĄZKÓW INFORMACYJNYCH

1. ADO współpracując z IOD i Zastępcą IOD dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane osobowe przetwarza.
2. ADO za pośrednictwem IOD lub Zastępcy IOD ułatwia osobom korzystanie z ich praw poprzez podjęcie różnych działań w zależności od przypadku, w tym: np. zamieszczenie na stronie internetowej ADO komunikatów lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w Spółce.
3. ADO za pośrednictwem IOD lub Zastępcy IOD dba o dotrzymywanie prawnych terminów realizacji obowiązku informacyjnego względem osób, których dane dotyczą.
4. ADO za pośrednictwem IOD lub Zastępcy IOD informuje osobę o planowanej zmianie celu przetwarzania danych.

§ 8

PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

I. **Prawa osób, których dane dotyczą**

1. Realizując prawa osób, których dane dotyczą, ADO przy współpracy z IOD i Zastępcą IOD wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste itp.), Spółka może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu. W każdym przypadku osoba, której dane osobowe dotyczą jest uprawniona do uzyskania od Spółki potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

   a) celach przetwarzania,

   b) o kategoriach odnośnych danych osobowych,

   c) o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,

   d) w miarę możliwości o planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu,

   e) o prawie do żądania od ADO sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania,

   f) o prawie wniesienia skargi do organu nadzorczego,

   g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o źródle danych,

h) o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. Spółka zobowiązana jest do udzielenia informacji, o której mowa w ust. 1 powyżej, bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania.

3. **Dostęp do danych**:

- na żądanie osoby dotyczące dostępu do jej danych, ADO (w każdym razie za pośrednictwem IOD lub Zastępcy IOD) informuje osobę, 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 ADO nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

4. **Kopie danych osobowych**:

- Na żądanie ADO za pośrednictwem IOD lub Zastępcy IOD i w konsultacji z właściwymi komórkami organizacyjnymi danej Spółki wydaje osobie kopię danych osobowych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.

5. **Sprostowanie danych osobowych**:

- ADO za pośrednictwem IOD lub Zastępcy IOD i w konsultacji z właściwymi komórkami organizacyjnymi danej Spółki dokonuje sprostowania nieprawidłowych danych osobowych na żądanie osoby, której dane osobowe dotyczą. ADO ma prawo odmówić sprostowania danych osobowych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości tych danych, których sprostowania się domaga. W przypadku sprostowania danych osobowych ADO informuje osobę o odbiorcach danych, na żądanie tej osoby.

6. **Usunięcie danych osobowych**. Na żądanie, ADO za pośrednictwem IOD i w konsultacji z właściwymi komórkami organizacyjnymi danej Spółki usuwa dane osobowe, gdy:

- nie są one niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
- zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
- osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych osobowych,
- dane osobowe były przetwarzane niezgodnie z prawem,
- konieczność usunięcia wynika z obowiązku prawnego.

ADO przy współpracy z IOD określa sposób obsługi prawa do usunięcia danych osobowych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych osobowych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.

Jeżeli dane osobowe podlegające usunięciu zostały upublicznione przez ADO, Spółka 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 ADO za pośrednictwem IOD lub Zastępcy IOD informuje osobę o odbiorcach danych, na żądanie tej osoby.

7. **Ograniczenie przetwarzania.** ADO ogranicza przetwarzanie danych osobowych na żądanie osoby, gdy:
   - osoba kwestionuje prawidłowość danych osobowych – na okres pozwalający sprawdzić ich prawidłowość,
   - przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
   - ADO nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
   - osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie ADO zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

   W trakcie ograniczenia przetwarzania ADO przechowuje dane osobowe, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. ADO informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych osobowych ADO informuje osobę o odbiorcach danych, na żądanie tej osoby.

8. **Przenoszenie danych osobowych**:
   - na żądanie osoby ADO wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Działalności, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w Systemach Informatycznych ADO.

9. **Sprzeciw w szczególnej sytuacji**:
   - jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych osobowych, a dane przetwarzane są przez ADO w oparciu o uzasadniony interes ADO lub o powierzone ADO zadanie w interesie publicznym, ADO uwzględni sprzeciw, o ile nie zachodzą po stronie ADO ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów,

praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

10. **Sprzeciw względem marketingu bezpośredniego / profilowania**:
    - jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych osobowych przez ADO na potrzeby marketingu bezpośredniego jak również profilowania, ADO uwzględni sprzeciw i zaprzestanie takiego przetwarzania.
11. Wnioski osób, których danych dotyczą o udzielenie informacji o danych przetwarzanych przez Spółkę, są załatwiane przez komórki organizacyjne Spółki odpowiedzialne za przetwarzanie tych danych **w porozumieniu z IOD (lub Zastępcą IOD)** procedującym wniosek.

II. **Procedura**

Dokumentem regulującym postępowanie w zgłoszenia przez osobę, której dane dotyczą żądania realizacji jej praw i wolności jest Instrukcja postępowania w sprawie realizacji żądań podmiotów danych stanowiąca Załącznik nr 8 do Polityki.

§ 9

UDOSTĘPNIANIE DANYCH OSOBOWYCH INNYM PODMIOTOM

1. Wnioski dotyczące udostępnienia danych osobowych podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa, wpływające do Spółki należy niezwłocznie przekazywać do IOD (lub Zastępcy IOD), który, we współpracy z właściwymi komórkami organizacyjnymi Spółki, przygotowuje odpowiedź w przedmiotowej sprawie. W razie wątpliwości, decyzję w sprawie zgody na udostępnienie danych osobowych lub o odmowie udostępnienia podejmuje ADO.
2. Informacje zawierające dane osobowe powinny być przekazane uprawnionym podmiotom listem poleconym (za potwierdzeniem odbioru) lub innym bezpiecznym sposobem (np. w formie zaszyfrowanej), zaakceptowanym przez ADO.
3. Każdorazowe udostępnienie danych osobowych, zarówno w wersji tradycyjnej (papierowej) jak i informatycznej (elektronicznej) podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa podlega wpisowi do rejestru prowadzonego przez IOD (Zastępcę IOD).
4. Dane nie mogą być udostępnianie drogą telefoniczną oraz w innych sposób, który uniemożliwia ustalenie tożsamości osoby uzyskującej dostęp do danych.

§ 10

POWIERZANIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Spółka może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie na podstawie pisemnej umowy zawartej pomiędzy Spółką, a tym podmiotem.
2. Spółka może przetwarzać dane osobowe na zlecenie innego administratora danych wyłącznie na podstawie pisemnej umowy zawartej pomiędzy Spółką, a tym podmiotem i na podstawie uprzedniej weryfikacji podmiotu, któremu Spółka zamierza powierzyć dane do przetwarzania, po pozytywnym zakończeniu tej weryfikacji Polityka dotycząca umów, w tym umów powierzenia przetwarzania danych osobowych przez ADO stanowi Załącznik nr 2 do Polityki. Ocena negatywna zostaje przedstawiona ADO, który powinien wykluczyć podmiot trzeci jako niegwarantujący prawidłowego poziomu ochrony danych osobowych.
3. Powierzenie przetwarzania danych osobowych następuje poprzez zawarcie przez ADO na piśmie umowy powierzenia przetwarzania danych osobowych z podmiotem, któremu zleca się czynności związane z ich przetwarzaniem. Wzór umowy powierzenia przetwarzania stanowi Załącznik nr 10 do Polityki.

4. Podmiot, któremu ADO zamierza powierzyć przetwarzanie Danych Osobowych, zobowiązany jest przed rozpoczęciem ich przetwarzania podjąć środki zabezpieczające dane osobowe oraz spełnić wszelkie wymagania wskazane umową.
5. Dalsze powierzenie przetwarzania danych osobowych przez podmiot, któremu ADO powierzył przetwarzanie danych osobowych, zawsze wymaga uprzedniej pisemnej zgody ADO.
6. Podmioty, z którymi ADO zawarł umowy powierzenia przetwarzanie danych osobowych, podlegają ujawnieniu w RCPD prowadzonym przez ADO.

§ 11

PRZEKAZANIE DANYCH OSOBOWYCH DO PAŃSTWA TRZECIEGO

1. Kierownik komórki organizacyjnej jest zobowiązany do przekazania do IOD każdej umowy, której zawarcie lub realizacja wiąże się z przekazaniem danych osobowych do państwa trzeciego, w rozumieniu art. 30 RODO, w celu weryfikacji poziomu ochrony danych osobowych zapewnianego przez państwo trzecie.
2. W przypadku, gdy przekazanie danych do państwa trzeciego warunkowane jest wyrażeniem zgody przez PUODO lub zatwierdzeniem innych instrumentów zapewniających odpowiednie gwarancje praw i wolności osób IOD występuje ze stosownym wnioskiem do PUODO.

§ 12

PRZETWARZANIE DANYCH OSOBOWYCH POZA MIEJSCEM PRZETWARZANIA

1. Przetwarzanie danych osobowych poza miejscem ich przetwarzania odbywa się za zgodą kierownika komórki organizacyjnej, w której jest zatrudniona osoba wykonująca tę czynność.
2. Pracownik przetwarzający dane osobowe w postaci papierowej lub na komputerze przenośnym poza miejscem przetwarzania danych osobowych, zobowiązany jest do ich ochrony przed dostępem osób nieupoważnionych, zagubieniem, uszkodzeniem lub częściowym zniszczeniem.
3. Zasady ochrony komputerów przenośnych, na których przetwarzane są dane osobowe oraz zasady zdalnego dostępu do systemu informatycznego Spółki określa „Polityka Bezpieczeństwa IT Polimex Mostostal S.A." (pkt 2.2, pkt 2.5 oraz pkt 2.10 rozdział „Zasady pracy w systemach informatycznych").

§ 13

PRZETWARZANIE DANYCH W SYSTEMIE INFORMATYCZNYM

1. Dane osobowe mogą być przetwarzane wyłącznie w zasobach Systemu informatycznego Spółki, spełniających wymogi Rozporządzenia. Dane osobowe przetwarzane w Systemie informatycznym muszą być okresowo archiwizowane na nośnikach poprzez tworzenie ich kopii zapasowych. Tworzenie kopii zapasowych danych osobowych powinno odbywać się według opracowanych wcześniej przez ASI procedur.
2. Kopie zapasowe Zbiorów danych osobowych przechowywane są w lokalizacjach lub pomieszczeniach innych od pomieszczeń, w których przechowywane są Zbiory danych osobowych eksploatowanych na bieżąco.

3. Transport nośników informacji zawierających kopie zapasowe danych osobowych może odbywać się wyłącznie w bezpieczny sposób, według opracowanych wcześniej procedur.
4. Wszystkie elektroniczne nośniki informacji muszą charakteryzować się odpowiednią trwałością zapisu proporcjonalną do planowanego okresu przechowywania danych osobowych.
5. Wszystkie elektroniczne nośniki informacji powinny być testowane pod kątem możliwości odtworzenia zapisanych na nich danych osobowych.
6. Nośniki Informacji przeznaczone do wycofania z eksploatacji muszą uprzednio zostać pozbawione danych osobowych, w sposób trwały i nieodwracalny.
7. Do przechowywania nośników stosuje się odpowiednio postanowienia dotyczące zasad przetwarzania danych osobowych w formie papierowej.
8. Zasady zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych określa Instrukcja Zarządzania Systemami Informatycznymi przetwarzającymi dane osobowe w Spółkach Grupy PxM stanowiąca Załącznik nr 11 do Polityki Bezpieczeństwa DO.

§ 14

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY SYSTEMAMI INFORMATYCZNYMI

1. Opis sposobu przepływu danych osobowych pomiędzy poszczególnymi systemami sporządza ASI we współpracy z kierownikami komórek organizacyjnych, w których przetwarzane są dane osobowe w Systemach Informatycznych, według wzoru stanowiącego Załącznik nr 12 do Polityki.
2. Kierownicy komórek organizacyjnych zobowiązani są do informowania ASI o każdej zmianie sposobu przepływu danych osobowych (modyfikacja systemu, rozbudowa systemu, zmiana struktury danych).
3. ASI zobowiązany jest do aktualizacji opisu sposobu przepływu danych osobowych pomiędzy poszczególnymi systemami co 6 miesięcy. W przypadku wdrożenia nowych systemów, ASI dokonuje aktualizacji stosownie do potrzeb.
4. Opis sposobu przepływu danych osobowych powinien w szczególności zawierać następujące informacje:
   a) przepływ danych osobowych pomiędzy poszczególnymi modułami danego Systemu Informatycznego (SI),
   b) rodzaj przepływu (jednokierunkowy czy dwukierunkowy, tj. tylko odczyt lub odczyt i zapis),
   c) sposób realizacji przepływu (automatyczny, na skutek działających algorytmów/ instrukcji lub manualny, import/eksport danych).
5. W przypadku wymiany danych osobowych pomiędzy więcej niż 2 Zbiorami danych, dla każdej pary Zbiorów należy sporządzić jeden rekord w tabeli.

§ 15

PRZETWARZANIE DANYCH OSOBOWYCH ZNAJDUJĄCYCH SIĘ NA NOŚNIKACH PAPIEROWYCH

1. Przetwarzanie Danych Osobowych w formie papierowej odbywa się zgodnie ze zwyczajowo przyjętymi zasadami.
2. Zasady przechowywania, sposób archiwizowania i likwidacji dokumentów papierowych zawierających dane osobowe określa Instrukcja kancelaryjna i archiwalna Spółki. Dane osobowe w formie papierowej należy przechowywać w wyznaczonych do tego celu pomieszczeniach zabezpieczonych przed dostępem osób nieuprawnionych.
3. Przekazywanie dokumentów papierowych z danymi osobowymi do Archiwum Spółki odbywa się zgodnie z Instrukcją kancelaryjną i archiwalną Spółki.
4. Dokumenty zawierające dane osobowe zamykane są w sposób utrudniający dostęp do ich zawartości.
5. Dokumenty zawierające dane wrażliwe przechowywane są w szafach zamykanych na klucz.
6. Zabronione jest pozostawianie dokumentów papierowych zawierających dane osobowe w miejscach umożliwiających ich wykorzystanie przez osoby nieuprawnione.
7. Pracownicy zobowiązani są do przestrzegania „zasady czystego biurka" oraz „czystego ekranu" szczegółowo określonych w Załączniku nr 13 do Polityki, co w szczególności oznacza, że nie są oni uprawnieni do opuszczania stanowisk pracy po zakończeniu dnia pracy bez uprzedniego usunięcia dokumentów w formie papierowej zawierających dane osobowe z miejsc widocznych w pomieszczeniu oraz ich zabezpieczenia przed nieuprawnionym dostępem osób nieuprawnionych.
8. Przechowywanie dokumentacji zawierającej dane osobowe w archiwach zewnętrznych, prowadzonych przez uprawnione do prowadzenia tej działalności podmioty trzecie, może odbywać się wyłącznie na podstawie stosownej umowy zawartej przez ADO oraz towarzyszącej jej umowy powierzenia przetwarzania danych osobowych.

§ 16

USUWANIE DANYCH OSOBOWYCH

1. Dane osobowe są przechowywane nie dłużej, niż wymaga tego cel, dla którego są przetwarzane, chyba że przepisy prawa zezwalają lub nakazują przechowywanie ich przez dłuższy czas.
2. Odpowiedzialność za usunięcie danych osobowych oraz niszczenie nośników i ponoszą Pracownicy, którzy powinni wykonywać te czynności w ramach swoich obowiązków służbowych. Usunięcie danych osobowych przetwarzanych w Systemie Informatycznym oraz niszczenie nośników odbywa się pod nadzorem ASI.
3. W razie uzasadnionej potrzeby (np. na żądanie kontrahenta ADO w przypadku Zbiorów powierzonych), z czynności usunięcia danych osobowych, a także z czynności zniszczenia nośników sporządza się protokół.

4. Na podstawie umowy powierzenia przetwarzania danych osobowych, dane osobowe oraz nośniki mogą być usuwane i niszczone przez podmiot, któremu powierzono do przetwarzania dane osobowe, w sposób uniemożliwiający zapoznanie się z danymi przez osoby nieupoważnione.

§ 17

URUCHAMIANIE NOWYCH PROJEKTÓW

1. W przypadku planowania nowych projektów czy wdrożenia nowych rozwiązań, Pracownik i będący inicjatorem lub managerem projektu albo ADO, w braku wskazanego wcześniej Pracownika, przedstawi ADO i IOD podstawowe założenia celem dokonania przez ADO/IOD oceny wpływu zmiany na ochronę danych osobowych już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.
2. IOD przedstawia ADO swoją rekomendację w zakresie wpływu na ochronę danych osobowych.

§ 18

ZABEZPIECZENIE DANYCH OSOBOWYCH

I. Środki techniczne

1. ADO stosuje środki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem RODO oraz innych przepisów prawa, oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. W tym celu ADO za pośrednictwem ASI i przy ogólnej współpracy Biura Informatyki (właściwymi służbami informatycznymi) ustala przydatność i stosuje takie środki i podejście jak m.in.: pseudonimizacja, szyfrowanie danych osobowych, inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności Systemu IT i usług przetwarzania, środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie Incydentu.
2. ADO za pośrednictwem ASI przeprowadza okresową analizę ryzyka i na tej podstawie przygotowuje plan działań w zakresie zastosowania środków technicznych i organizacyjnych, celem zapewnienia właściwej ochrony przetwarzanych danych osobowych lub jej polepszenia.
3. ADO za pośrednictwem ASI przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:
   a) ADO za pośrednictwem ASI zapewnia odpowiedni stan wiedzy ASI o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych,
   b) ADO za pośrednictwem ASI kategoryzuje dane osobowe oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają,

c) ADO za pośrednictwem ASI 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.

II. Reguły ochrony obszaru przetwarzania danych

1. Dane osobowe mogą być przetwarzane wyłącznie w miejscu przetwarzania danych osobowych, na który składają się pomieszczenia, w których ADO prowadzi swoją działalność.
2. Pomieszczenia, w których przetwarzane są dane osobowe w siedzibie ADO zabezpieczone są drzwiami zwykłymi lub wzmacnianymi i przeciwpożarowymi, zamykanymi na klucz lub wyposażonymi w system kontroli dostępu.
3. Pomieszczenia, w których przetwarzane są dane osobowe podczas nieobecności zajmujących je Pracowników powinny być zamykane w sposób ograniczający możliwość dostępu do nich osobom nieupoważnionym.
4. Osoby wyznaczone przez ADO (Dział Administracji) sporządzają i na bieżąco aktualizują listę Pracowników upoważnionych do dysponowania kluczami do pomieszczeń biurowych, w których przetwarzane są dane osobowe.
5. Osoby nieuprawnione do przetwarzania danych osobowych mogą przebywać wewnątrz obszaru przetwarzania danych osobowych wyłącznie w obecności osoby upoważnionej przez ADO do przetwarzania tych danych.
6. Pomieszczenia biurowe, w których przetwarzane są dane osobowe zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego lub wolnostojącej gaśnicy.
7. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
8. Drukarki wykorzystywane w procesie przetwarzania danych osobowych powinny być, w miarę możliwości, usytuowane z dala od ciągów komunikacyjnych, z których mogłyby korzystać osoby nieuprawnione.
9. Dane osobowe mogą być przetwarzane poza wskazanymi miejscami przetwarzania danych osobowych przez Pracowników przy użyciu służbowych przenośnych urządzeń z uwzględnieniem zasad bezpieczeństwa.

III. Podstawowe reguły przesyłania danych osobowych przez sieć

1. Ruch sieciowy powinien zostać poddany stałemu monitoringowi przez ASI.
2. Konfiguracja sieci powinna być udokumentowana, a dokumentacja konfiguracji sieci na bieżąco aktualizowana przez ASI.
3. Należy okresowo przeprowadzać przeglądy, w celu sprawdzenia, czy nie zostały wprowadzone nieautoryzowane zmiany w konfiguracji sieci.
4. Należy zapewnić wymaganą przepustowość sieci. Obciążenie linii komunikacyjnych i węzłów sieci powinno być systematycznie monitorowane.

5. Dostęp do usług sieciowych, takich jak: przesyłanie danych, praca interakcyjna, poczta elektroniczna itp. musi być realizowany w sposób kontrolowany przez ASI.
6. Dostęp do zdalnych funkcji diagnostycznych zaimplementowanych w węzłach sieci komputerowej powinien znajdować się pod ścisłą kontrolą ASI.
7. Dane wykorzystywane do uwierzytelnienia użytkowników w Systemie IT (login, hasło) nie mogą być przesyłane pocztą elektroniczną. Odstąpić od tej zasady można wyłącznie przy użyciu zgodnej z obowiązującym prawem i zaakceptowanej przez ADO metody zabezpieczenia danych osobowych (np. stosownej kryptografii), lub za odrębną pisemną zgodą ADO.
8. Pracownicy ADO nie mogą używać do celów służbowych innych skrzynek poczty elektronicznej niż przydzielone im indywidualnie przez ASI.
9. Przekazywanie lub otrzymywanie danych osobowych lub oprogramowania do/z firmy zewnętrznej powinno odbywać się na podstawie umowy precyzującej warunki zapewniające bezpieczeństwo przekazania danych osobowych. Zawarte w umowie zobowiązania dotyczące bezpieczeństwa danych osobowych powinny zależeć od poziomu sklasyfikowania przekazywanych/otrzymywanych danych pod kątem ich wrażliwości, jak również uwzględniać wyniki przeprowadzanej analizy ryzyka, jeżeli była ona przeprowadzona.

IV. Ochrona przed oprogramowaniem inwazyjnym

1. ADO za pośrednictwem ASI i przy współpracy z Biurem Informatyki PxM (właściwymi służbami informatycznymi) stosuje i na bieżąco aktualizuje oprogramowanie zabezpieczające przed oprogramowaniem inwazyjnym oraz innymi formami nieuprawnionego dostępu do Systemu Informatycznego.
2. Wykrycie wirusa lub innej formy ingerencji w System Informatyczny przez użytkownika powinno zostać natychmiastowo zgłoszone do ASI oraz ADO.
3. Wszystkie komputery służbowe ADO podlegają okresowej kontroli aktualności oprogramowania antywirusowego, w terminach określonych przez ASI.
4. Zabrania się używania w Spółce jakiegokolwiek oprogramowania, które uprzednio nie zostało sprawdzone i zaakceptowane przez ASI.

V. Szyfrowanie

1. Dane wykorzystywane do uwierzytelnienia użytkowników w Systemie Informatycznym (login, hasło) mogą być przesyłane przez Sieć publiczną wyłącznie pod warunkiem ich zaszyfrowania.
2. ASI w porozumieniu z ADO może podjąć decyzję o szyfrowaniu również innych kategorii danych, kluczowych w działalności ADO. **Natomiast, przesyłanie (w każdej sytuacji na zewnątrz) danych osobowych, z których ujawnieniem wiąże się ryzyko naruszenia praw i wolności osób, których te dane dotyczą, przez sieć powinno odbywać się przy pomocy zabezpieczeń hasłem. Hasło powinno być przekazane odbiorcy wiadomości inną drogą (np. za pośrednictwem SMS). W tym celu ADO tworzy katalog danych osobowych, których przesyłanie wymaga szyfrowania (dane przesyłane za pośrednictwem wiadomości e-mail zabezpieczone są hasłem, które**

przesyłane jest na numer telefonu komórkowego odbiorcy wiadomości): dane dotyczące skazań i innych naruszeń prawa (dane z Krajowego Rejestru Karnego), w tym mandaty, dane dotyczące przynależności do związków zawodowych działających w Spółce, dane dotyczące stanu zdrowia, dane dotyczące wynagrodzeń pracowników, numery PESEL.

3. Szyfrowanie informacji powinno odbywać się wyłącznie przy wykorzystaniu algorytmów, programów i narzędzi szyfrujących zgodnych z obowiązującymi wymogami prawa.
4. Dostęp do kluczy szyfrujących jest kontrolowany i ograniczony wyłącznie do osób uprawnionych do ich używania w związku z wykonywanymi zadaniami służbowymi.
5. Klucze szyfrujące generowane są w taki sposób, aby nie było możliwe powtórzenie procesu generacji przez osobę nieuprawnioną.
6. Klucze szyfrujące są okresowo zmieniane. Częstotliwość zmiany kluczy szyfrujących powinna być uzależniona od wrażliwości szyfrowanych danych.
7. Dyski twarde komputerów i innych urządzeń mobilnych (jeśli metoda zostanie wprowadzona) powinny być szyfrowane przy użyciu metody wybranej przez ASI.

VI. Zasady zarządzania kontrolą dostępów

1. Dla Systemów IT ustalone zostają zasady kontroli nad przyznawaniem praw dostępu do zasobów w nich przetwarzanych.
2. Biuro Informatyki PxM (właściwa komórka ds. informatyki) prowadzi rejestr przydzielonych uprawnień w Systemach Informatycznych i uprawnień nadanych Pracownikom ADO, w tym w poszczególnych aplikacjach wykorzystywanych w Spółce.
3. Dla Systemu Informatycznego o prawie dostępu do informacji decyduje przełożony Pracownika, dyr. Biura Informatyki. W zakresie danych stricte HR'owych Dyrektor Biura Informatyki PxM informuje Biuro Dział Kadr i Płac o zakresie dostępu danego Pracownika do SI w celu odzwierciedlenia tego w nadawanym upoważnieniu do przetwarzania danych osobowych.
4. Zakres przyznanych praw dostępu powinien być determinowany rzeczywistymi potrzebami służbowymi Pracownika, któremu te prawa są nadawane, i zakresem jego obowiązków służbowych.
5. Zmiany zakresu obowiązków Pracownika, mające wpływ na zakres przetwarzanych przez niego danych osobowych powinny mieć natychmiastowe odzwierciedlenie w przyznanych mu prawach do SI.
6. W przypadku odebrania użytkownikowi upoważnienia do przetwarzania danych osobowych, ASI blokuje dostęp tego użytkownika w SI lub kontaktuje się z administratorem aplikacji, po uzyskaniu informacji od ADO/Działu Kadr i Płac.
7. Prawa nadane użytkownikom powinny być cyklicznie weryfikowane przez ASI.

VII. Kontrola dostępu

1. Dostęp do Systemu informatycznego ADO możliwy jest wyłącznie po podaniu przez użytkownika właściwego identyfikatora i hasła.
2. Każdemu Pracownikowi/użytkownikowi przydzielany jest unikalny identyfikator.
3. Hasła ustalane przez Pracowników:
   a) muszą zawierać co najmniej 8, ale nie więcej niż 30 znaków;
   b) są kombinacją znaków alfanumerycznych;
   c) składają się z liter, cyfr, znaków interpunkcyjnych, symboli matematycznych i innych symboli konwencjonalnych;
   d) muszą zawierać znaki z co najmniej trzech z poniższych czterech kategorii:
      - wielkie litery języków europejskich (od A do Z);
      - małe litery języków europejskich (od a do z);
      - podstawowe 10 cyfr (od 0 do 9);
      - znaki niealfanumeryczne: ~ ! @ # $ % ^ & * ( ) _ + - = { } | \ : " ; ' < > ?, . /.
4. Hasła są zmieniane co 30 dni. ASI monitoruje zmianę haseł przez użytkowników i wysyła w tym celu stosowne przypomnienia.
5. System Informatyczny umożliwia zalogowanie wyłącznie uprawnionym użytkownikom.
6. Użytkownicy nie posiadają dostępu do narzędzi administracyjnych SI.

§ 19

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Dokumentem regulującym postępowanie w przypadku naruszenia ochrony danych osobowych w Spółce jest Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych, stanowiąca Załącznik nr 14 do Polityki.
2. ADO za pośrednictwem IOD prowadzi stosowny rejestr naruszeń ochrony danych osobowych w Spółce.

§ 20

ODPOWIEDZIALNOŚĆ ZA NARUSZENIE

1. Wszyscy Pracownicy Spółki zobowiązani są bezwzględnie przestrzegać zasad ochrony danych osobowych wynikających z niniejszej Polityki.
2. W stosunku do Pracowników świadczących pracę na rzecz danej Spółki, którzy naruszą określone w niniejszej Polityce procedury i postanowienia obowiązujące w zakresie ochrony danych osobowych, mogą zostać zastosowane konsekwencje przewidziane w umowie stanowiącej podstawę stosunku prawnego ze Spółką za istotne naruszenie jej postanowień jak również konsekwencje dyscyplinarne. W szczególności Spółka może rozwiązać umowę z Pracownikiem w trybie natychmiastowym oraz dochodzić stosownego odszkodowania, co nie wyłącza innych uprawnień Spółki wynikających z przepisów prawa.

§ 21

SZKOLENIA Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

1. W celu zapewnienia właściwego poziomu ochrony danych osobowych w Spółce, Dział Administracji Spółki opracowuje plan szkoleń według następujących zasad:
   a) szkolenie z zakresu ochrony danych osobowych powinna odbyć każda osoba rozpoczynająca pracę w Spółce w ramach *onboardingu* i co do zasady przed upoważnieniem do przetwarzania danych osobowych;
   b) szkolenia osób upoważnionych do przetwarzania danych osobowych powinny być przeprowadzane w przypadku każdej zmiany zasad, procedur lub przepisów prawa w zakresie ochrony danych osobowych w Spółce a niezależnie od ww. zmian nie rzadziej niż raz do roku;
   c) w trakcie szkolenia osoby upoważnione do przetwarzania danych osobowych powinny uzyskać wiedzę dotyczącą: przepisów prawnych i procedur dotyczących ochrony danych osobowych obowiązujących w Spółce, w tym sporządzania i przechowywania kopii, niszczenia wydruków i zapisów na nośnikach, ochrony danych osobowych przed osobami postronnymi, odpowiedzialności za naruszenie obowiązków z zakresu ochrony danych osobowych.
2. Szkolenia będą prowadzone przez kompetentne jednostki szkoleniowe lub IOD (Zastępcę IOD).

§ 22

ANALIZA RYZYKA

1. ADO narażony jest na wpływ zewnętrznych oraz wewnętrznych czynników, które mogą spowodować Naruszenie ochrony danych. Jednym z zadań ADO jest wdrożenie odpowiednich Zabezpieczeń. Służą do tego Analiza ryzyka oraz Ocena skutków ryzyka dla ochrony danych, które są częścią ciągłego procesu udoskonalania systemu zarządzania bezpieczeństwem informacji.
2. Decydując o doborze środków technicznych i organizacyjnych ADO uwzględnia czynniki jak: **(i)** stan wiedzy technicznej; **(ii)** koszt wdrażania wymaganych zabezpieczeń; **(iii)** charakter, zakres, kontekst i cele przetwarzania; **(iv)** ryzyko naruszenia praw i wolności podmiotów danych.
3. Środkiem pomocnym w zapewnieniu bezpieczeństwa przetwarzania jest upoważnienie przez ADO każdej osoby przetwarzającej u niego dane osobowe i zatrudnionej u ADO. Ponadto zaznajomienie osób, o których mowa w zdaniu poprzednim z zasadami ochrony danych funkcjonującymi u ADO oraz zobowiązanie ich do zachowania tajemnicy w związku z przetwarzanymi danymi.

I. **Opis procedury zarządzania ryzykiem**

1. Opis procedury zarządzania ryzykiem w GK PxM znajduje się w dokumencie Procedura Zarządzania Ryzykiem w Grupie Kapitałowej Polimex Mostostal, który jest dokumentem powiązanym z niniejszą Polityką. Postanowienia zawarte w tej procedurze stosuje się w adekwatnym zakresie do Analizy ryzyka

przeprowadzanej na potrzeby wdrożenia przez ADO odpowiednich Zabezpieczeń służących ochronie danych osobowych, z uwzględnieniem poniższych treści.

2. Obowiązują następujące zasady przetwarzania danych, zawarte w sześciu punktach: **(i)** zasada zgodności z prawem, rzetelności i przejrzystości; **(ii)** ograniczenia celu; **(iii)** minimalizacji danych; **(iv)** prawidłowości; **(v)** ograniczenia przechowywania; **(vi)** integralności i poufności. ADO musi być w stanie wykazać przestrzeganie ww. zasad.

3. Bezpieczeństwo danych musi być odpowiednie do ryzyka naruszenia praw i wolności osób, których dane dotyczą. W konsekwencji, **poziom bezpieczeństwa powinien być dostosowany do tego, jaką szkodę lub krzywdę może wyrządzić osobom naruszenie bezpieczeństwa ich danych**. Realizacja zasady odpowiedniego bezpieczeństwa ma ścisły związek z szacowaniem ryzyka przetwarzania danych. **W zależności od rodzaju posiadanych danych, sposobu ich przetwarzania czy wielkości podmiotu będącego administratorem danych konieczne jest zastosowanie odpowiednich środków bezpieczeństwa minimalizujących ryzyko utraty kontroli nad przetwarzaniem danych**.

4. Zasady odpowiedniości bezpieczeństwa oraz zasada rozliczalności polegają na tym, że **jeśli nie zostanie przeprowadzona analiza ryzyka i klasyfikacja ryzyka naruszenia ochrony danych, a w jej ramach, ryzyka i konsekwencji naruszenia praw i wolności osób, nie będzie można wykazać, że zastosowane zostały odpowiednie środki bezpieczeństwa. Należy więc ocenić ryzyko, żeby zastosować odpowiednie do niego środki**. ADO powinien kłaść nacisk na kwestie bezpieczeństwa, uwzględniając zagrożenia pochodzące zarówno z zewnątrz jak i wewnątrz podmiotu. Kluczowa jest analiza oraz podnoszenie poziomu zabezpieczeń. Zastosowanie przez ADO systemów zapobiegających ryzykom wycieków danych, których ujawnienie może narazić podmiot na odpowiedzialność administracyjną, cywilną, karną czy innego rodzaju straty jest konieczne w aspekcie ochrony danych i informacji. Zasada bezpieczeństwa musi być zgodna z zasadą legalności i minimalizacji danych.

5. Niezależnie od zasady rozliczalności, ADO musi być w stanie wykazać przestrzeganie pozostałych zasad, w tym legalności. Jeżeli przetwarzanie odbywa się na podstawie zgody[1] ADO musi być w stanie wykazać, ze osoba, której dane dotyczą wyraziła zgodę na przetwarzanie jej danych osobowych. ADO musi zatem pamiętać o utrwaleniu faktu uzyskania zgody na przetwarzanie w celu wykazania w szczególności przed organem nadzorczym, że otrzymał tę zgodę. Zgoda osoby, której dane dotyczą musi mieć charakter **uprzedni** w stosunku do przetwarzania jej danych przez ADO.

6. Zarządzanie ryzykiem opiera się na wdrożeniu schematu postępowania zwanego cyklem Deminga. Jest to proces polegający na ciągłej poprawie danego zagadnienia, by osiągnąć jak najwyższy poziom realizacji. Cykl Deminga charakteryzuje się czterema etapami: **(i)** zaplanuj; **(ii)** wykonaj; **(iii)** sprawdź; **(iv)** popraw. Jeżeli po wykonaniu ostatniego etapu nie udało się osiągnąć wyznaczonego poziomu realizacji – całą procedurę należy ponowić. Dopiero w razie odniesienia oczekiwanych rezultatów, cała procedurę można uznać jako standard

[1] *obecny art. 7 RODO.*

i jedynie monitorować prawidłowość jej działania. Dla zagadnienia ochrony danych przyjęto schemat wykorzystujący pojęcia niezbędne przy Analizie ryzyka.

Kontekst	wyznaczenie zagrożonych elementów ADO, które mają pośredni i bezpośredni wpływ na ochronę danych osobowych
Szacowanie ryzyka	określenie występujących u ADO zagrożeń, skutków ich wystąpienia oraz prawdopodobieństwa czy dane zagrożenie może nastąpić
Postępowanie z ryzykiem	wybór jednej ze ścieżek postępowania
Sprawdzenie	zweryfikowanie czy po zmianach dla danego kontekstu występuje jeszcze zagrożenie przetwarzania danych osobowych.

7. Dla sporządzenia Analizy ryzyka obejmującej wszystkie możliwe zagrożenia oraz konteksty przetwarzań danych osobowych wykorzystuje się metodę szacowania opisaną w Procedurze Zarządzania Ryzykiem w Grupie Kapitałowej Polimex Mostostal.
8. Oszacowaną wartość ryzyka danego zagrożenia przyporządkowuje się odpowiedniemu poziomowi ryzyka według tabeli zawartej w Procedurze Zarządzania Ryzykiem w Grupie Kapitałowej Polimex Mostostal (pkt. 5.6.). Metoda pozwala oszacować ryzyko dla każdego zagrożenia, uwzględniając poziom skutków i prawdopodobieństwa dając jednocześnie możliwość określenia czy dane ryzyko jest akceptowalne.

II. Kontekst zagrożenia

1. Ustalenie Kontekstu jest podstawą dla prawidłowego sporządzenia Analizy ryzyka, która jest wyjściową do Oceny skutków ryzyka dla ochrony danych. Należy określić możliwe zagrożenia, które mogą mieć negatywny wpływ na uwarunkowania związane z działaniem podmiotu a zwłaszcza dotyczące posiadanych danych w wersji papierowej, sprzętu, oprogramowania, pomieszczeń oraz nośników danych.
2. Na wymienione wyżej Aktywa wpływają różne czynniki zagrożeń, zarówno wewnętrzne jak i zewnętrzne dlatego też istotne jest sporządzenie ich listy. Identyfikacja zasobów i zagrożeń powinna być przeprowadzona na odpowiednim poziomie szczegółowości, co zapewni prawidłowe oszacowanie poszczególnych ryzyk i poziomów akceptacji. Zagrożenia można podzielić na kilka grup: **(i)** organizacyjne; **(ii)** techniczne; **(iii)** personalne; **(iv)** fizyczne.
3. Po przeprowadzeniu analizy ryzyka u ADO należy krótko opisać wnioski z niej wynikające, a dotyczące ryzyka wystąpienia naruszeń w zakresie ochrony danych osobowych uwzględniając, czy ADO dołożył starań, aby poziom ochrony danych osobowych był jak najniższy, a także czy występujące ryzyka cechują się akceptowalnym (lub nie) poziomem ryzyka. Każdorazowym zaleceniem wynikającym z przeprowadzonej analizy ryzyka powinna być sukcesywna kontrola przez ADO, czy stopień ryzyka pojawienia się naruszenia nie zwiększy się w przyszłości.

4. W razie wystąpienia zbyt dużego ryzyka cząstkowego (dotyczącego jednego zagrożenia) należy dołożyć starań, aby je zminimalizować. RODO[2] wskazuje działania i środki, które mogą być wdrożone w celu minimalizacji ryzyka jak np.: **(i)** pseudonimizacja danych; **(ii)** szyfrowanie danych; **(iii)** zdolność do szybkiego przywrócenia dostępności danych i dostępu do nich w razie incydentu fizycznego, technicznego; **(iv)** regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania (są to przykłady możliwych działań, ponieważ konkretne rozwiązania zależą od ADO i są wynikiem przeprowadzonej Analizy ryzyka).

§ 23

PRZEGLĄDY POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. ADO zobowiązany jest do zapewnienia zgodności Polityki Bezpieczeństwa Danych Osobowych i pozostałych dokumentów z zakresu ochrony danych osobowych, o których mowa w Polityce, z:
   a) Systemem Informatycznym Spółki,
   b) strukturą organizacyjną Spółki,
   c) przepisami prawa dotyczącymi ochrony danych osobowych.
2. W celu wypełnienia zobowiązań, o których mowa w ust. 1., ADO za pośrednictwem IOD co najmniej raz w roku dokonuje przeglądu „Polityki Bezpieczeństwa DO".
3. W przypadku istotnej zmiany przepisów prawnych, struktury organizacyjnej Spółki, budowy Systemu Informatycznego albo zakresu przetwarzania danych osobowych w Spółce, IOD zobowiązany jest do przeprowadzenia przeglądu „Polityki Bezpieczeństwa DO" przed upływem terminu, o którym mowa w ust. 2.

§ 23

WYKAZ DOKUMENTÓW ZWIĄZANYCH

Dokumentami związanymi z **Polityką Bezpieczeństwa Danych Osobowych** są:

1) Polityka Bezpieczeństwa dla Spółek Grupy Kapitałowej Polimex Mostostal;
2) Polityka Bezpieczeństwa IT w Polimex Mostostal S.A.;
3) Instrukcja zarządzania Systemami Informatycznymi przetwarzającymi dane osobowe w Spółkach Grupy Kapitałowej Polimex Mostostal;
4) Instrukcja kancelaryjna i archiwalna Spółki;
5) Instrukcje bezpieczeństwa poszczególnych obiektów;
6) Procedura Zarządzania Ryzykiem w Grupie Kapitałowej Polimex Mostostal.

[2] *obecny Art. 32 ust. 1 RODO.*

ZAŁĄCZNIKI

1. Wzór ewidencji miejsc przetwarzania danych osobowych
2. Polityka dotycząca umów zawieranych przez Spółkę, w tym umów powierzenia przetwarzania danych osobowych
3. Wzór upoważnienia do przetwarzania danych osobowych i dalszego upoważnienia
4. Wzór wniosku o nadanie upoważnienia do przetwarzania danych osobowych
5. Wzór ewidencji udzielonych upoważnień do przetwarzania danych osobowych
6. Wzór oświadczenia o zachowaniu poufności i zapoznaniu się z Polityką
7. Wzory przykładowych klauzul informacyjnych
8. Instrukcja postępowania w sprawie realizacji żądań podmiotów danych
9. Wzór Rejestru Czynności Przetwarzania Danych Osobowych
10. Wzór umowy powierzenia przetwarzania danych osobowych
11. Instrukcja Zarządzania Systemami Informatycznymi przetwarzającymi dane osobowe w Spółkach Grupy PxM
12. Opis sposobu przepływu danych pomiędzy Systemami Informatycznymi
13. Polityka „czystego biurka" i „czystego ekranu"
14. Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych
15. Schemat dotyczący przepływu informacji z zakresu przetwarzania danych osobowych w MS (A) i w Spółkach z GK PxM, w których wyznaczono IOD (B).

PREZES ZARZĄDU
Tomasz Klapunowicz

Dział Administracji
Kierownik Działu
Sławomir Marchel