Wydanie I

Polityka ochrony danych osobowych

Spis treści

I. PRZEDMIOT / CEL

Niniejsza Polityka Ochrony Danych Osobowych dotyczy wszystkich Spółek wchodzących w skład Grupy Kapitałowej ROBYG (każda z nich rozumiana dalej jako „Spółka") i powstała w oparciu o analizę charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia. Jej podstawowym celem jest uregulowanie wszystkich obszarów, które odnoszą się do procesów przetwarzania danych oraz przyjętych w Spółce środków technicznych i organizacyjnych.

II. ODPOWIEDZIALNOŚĆ

a. Nadzór nad aktualnością niniejszego dokumentu sprawuje Inspektor Ochrony Danych.
b. Każdorazowa zmiana bądź aktualizacja niniejszej polityki wymaga konsultacji z powołanym w Grupie ROBYG inspektorem ochrony danych (IOD).

III. ZAWARTOŚĆ

Rozdział 1. Słowniczek

§ 1.

Przez użyte w Polityce Ochrony Danych Osobowych (PODO) terminy należy rozumieć:

1) **administrator danych** – Spółka, czyli osoba prawna która samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
2) **audyt** – systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu;
3) **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;
4) **działy** – jednostki organizacyjne Spółki;
5) **dostępność** – właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;

6) **kierownik działu** – osoba sprawująca bezpośredni nadzór (merytoryczny i służbowy) w dziale;
7) **Spółka** – podmiot wchodzący w skład Grupy Kapitałowej ROBYG
8) **incydent bezpieczeństwa** – każde wykryte naruszenie albo wykryta próba naruszenia bezpieczeństwa danych osobowych będąca naruszeniem obowiązujących przepisów wewnętrznych Spółki lub powszechnie obowiązujących przepisów prawa; źródłem incydentu bezpieczeństwa może być zarówno przypadkowe, jak i celowe działanie albo jego zaniechanie przez pracowników / współpracowników lub osoby, przy pomocy których Spółka wykonuje swoje czynności;
9) **inspektor ochrony danych (IOD)** – osoba wyznaczona do realizacji zadań wskazanych w art. 39 RODO;
10) **integralność** – właściwość polegającą na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;
11) **naruszenie ochrony danych osobowych** - oznacza 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;
12) **ocena ryzyka** – proces mający na celu oszacowanie wagi ryzyka rozumianej jako funkcja prawdopodobieństwa wystąpienia skutku i krytyczności jego następstw dla praw lub wolności osób fizycznych, których dane osobowe przetwarza Spółka;
13) **organ nadzorczy** – Prezes Urzędu Ochrony Danych Osobowych (PUODO);
14) **podatność systemu teleinformatycznego** - właściwość systemu teleinformatycznego, która może być wykorzystana przez co najmniej jedno zagrożenie;
15) **podmiot przetwarzający (procesor)** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
16) **polityka ochrony danych osobowych (PODO)** – niniejszy dokument, przez który należy rozumieć zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania;
17) **postępowanie z ryzykiem** - proces modyfikowania ryzyka; postępowanie z ryzykiem może uwzględniać np. unikanie ryzyka poprzez decyzję o nierozpoczynaniu lub niekontynuowaniu działań powodujących ryzyko, usunięcie źródła ryzyka, zachowanie ryzyka na podstawie świadomej decyzji.
18) **poufność** – właściwość zapewniająca, że dane osobowe nie są udostępniane lub wyjawiane nieupoważnionym osobom fizycznym;
19) **pracownicy i współpracownicy Działu IT** – osoby nadzorujące pracę systemu teleinformatycznego oraz wykonujące czynności wymagające specjalnych uprawnień lub osoby nadzorujące wykonywanie tych czynności przez pomiot (podmioty) zewnętrzny na podstawie umowy (umów) zawartej ze Spółką;

20) **proces przetwarzania danych** – seria powiązanych ze sobą działań lub zadań, które rozwiązują określony problem lub prowadzą do osiągnięcia określonego efektu przy wykorzystaniu danych osobowych;
21) **profilowanie** - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
22) **przetwarzanie** - 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;
23) **RODO** - 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
24) **rozliczalność** – właściwość zasobu informatycznego oznaczająca, że wykonane na nim działania mogą być jednoznacznie przypisane wykonującej je osobie lub systemowi informatycznemu;
25) **ryzyko** – prawdopodobieństwo tego, że zagrożenie wykorzysta podatność powodując skutek;
26) **system teleinformatyczny** - zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego w rozumieniu ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne;
27) **system ochrony danych osobowych (SODO)** – polityka ochrony danych osobowych, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez Spółkę dążące do ochrony danych osobowych, które przetwarza;
28) **użytkownik** – pracownik lub współpracownik Spółki oraz inne osoby, przy pomocy których Spółka wykonuje swoje czynności, posiadające uprawnienia do pracy w systemie teleinformatycznym zgodnie z zakresem obowiązków służbowych i nadanymi uprawnieniami;
29) **właściciel biznesowy** - osoba odpowiedzialna za działanie i ciągłe ulepszanie danego procesu przetwarzania danych;
30) **zagrożenie** – stan faktyczny, który może spowodować naruszenie bezpieczeństwa danych osobowych;
31) **zagrożenie systemu teleinformatycznego** - potencjalna przyczyna niepożądanego zdarzenia, która może wywołać szkodę w systemie teleinformatycznym;

32) **zasada wiedzy koniecznej** – dostęp pracowników i współpracowników Spółki lub osób, przy pomocy których Spółka wykonuje swoje czynności na danych osobowych, ograniczony wyłącznie do tych danych, które są im niezbędne do wykonania powierzonych zadań;

Rozdział 2. Podstawy prawne

§ 2.

Niniejsza Polityka Ochrony Danych Osobowych opiera się na:.

1) Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (w dalszej części jako RODO);
2) Ustawie o ochronie danych osobowych (UODO);
3) Ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (w dalszej części jako UŚUDE);
4) Ustawie z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (w dalszej części jako PT);
5) PN-ISO/IEC 27001:2013;
6) PN-ISO/IEC 27005:2014;
7) Wytyczne Grupy Roboczej Art. 29 Ds. Ochrony Danych Osobowych tj. w szczególności:
   a) Wytyczne dotyczące inspektorów ochrony danych (‘DPO’) z dnia 13 grudnia 2016 r.;
   b) Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko”, do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017 r.;
   c) Wytyczne dotyczące prawa do przenoszenia danych z dnia 13 grudnia 2016 r.;
   d) Wytyczne dotyczące ustalenia wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego z dnia 13 grudnia 2016 r.

Rozdział 3. Deklaracja stosowania

§ 3.

1) Zarząd Spółki przyjmującej niniejszą PODO w Grupie ROBYG, świadomy odpowiedzialności za zapewnienie bezpieczeństwa danych osobowych, deklaruje gotowość budowy kompleksowego systemu ochrony danych osobowych (SODO) oraz wsparcie wszelkich działań mających na celu ochronę danych osobowych przetwarzanych przez Spółki z Grupy ROBYG.
2) Zarząd Spółki, podjął decyzję o powołaniu inspektora ochrony danych (IOD) dla Grupy ROBYG. Szczegółowy zakres zadań i statut IOD zostały określone w procedurze „Zadania i statut Inspektora Ochrony Danych” stanowiącej **załącznik nr 1** do PODO.

3) Zarząd Spółki zobowiązuje kierowników działów do:
   a) zapewnienia właściwych warunków organizacyjno-technicznych przetwarzania danych osobowych w podległych działach;
   b) zapewnienia bieżącego nadzoru nad przestrzeganiem obowiązujących w Spółce polityk i procedur mających na celu zapewnienie ochrony danych osobowych;
4) Zarząd Spółki zobowiązuje Kierownika Działu IT do:
   a) informowania Zarządu Spółki o potrzebach w zakresie niezbędnych środków technicznych, które zapewniać będą bezpieczeństwo danych osobowych;
   b) wdrożenia niezbędnych środków technicznych i organizacyjnych mających na celu zabezpieczenie infrastruktury IT oraz systemów teleinformatycznych służących do przetwarzania danych osobowych;
   c) informowania Inspektora Ochrony Danych o planowanych do wdrożenia środkach zabezpieczeń, rezygnacji z przyjętych środków zabezpieczeń lub ich zastąpienia, a także konsultowania wszelkich wątpliwości dotyczących tych środków z Inspektorem Ochrony Danych;
   d) dbania o zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów teleinformatycznych i usług przetwarzania;
   e) dbania o zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego mającego związek z systemami teleinformatycznymi i infrastrukturą IT służącymi do przetwarzania danych osobowych;
   f) regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych w ramach systemów teleinformatycznych i infrastruktury IT.
5) W celu uszczegółowienia zasad wskazanych w PODO Zarząd Spółki może wyznaczyć osobę bądź osoby odpowiedzialne za opracowanie dokumentacji ochrony danych osobowych obejmującej szczegółowe polityki, instrukcje i procedury wynikające z PODO oraz do wdrożenia i utrzymania właściwego poziomu bezpieczeństwa danych osobowych wynikającego z tych uregulowań.

Rozdział 4. Cel i zakres PODO

§ 4.

1) Celem PODO jest stworzenie podstaw organizacyjnych dla wdrożenia SODO w Spółce.
2) PODO odnosi się do wszelkich danych osobowych znajdujących się w posiadaniu Spółki niezależnie od tego w jaki sposób te dane są przetwarzane.
3) Zasady ustanowione w PODO powinny być stosowane przez wszystkie osoby zatrudnione w Spółce / współpracujące z Spółką.

Rozdział 5. Czynniki zewnętrzne i wewnętrzne istotne dla celu działania Spółki

§ 5.

1) Czynniki zewnętrzne mające wpływ na działalność Spółki (kontekst zewnętrzny) w zakresie dotyczącym bezpieczeństwa danych osobowych:
   a) powszechnie obowiązujące przepisy prawa w zakresie ochrony danych osobowych;
   b) pozycja rynkowa Spółki;
   c) funkcjonowanie Spółki w ramach międzynarodowej grupy kapitałowej i wiążące się z tym oczekiwania właściciela;
   d) współpraca z innymi podmiotami i partnerami biznesowymi;
   e) oczekiwania klientów.
2) Czynniki wewnętrzne mające wpływ na działalność Spółki (kontekst wewnętrzny) w zakresie dotyczącym bezpieczeństwa danych osobowych:
   a) wewnętrzne regulacje i procedury obowiązujące w Spółce;
   b) struktura organizacyjna Spółki,
   c) zobowiązania i uprawnienia Spółki wynikające z zawartych umów i porozumień,
   d) cele opisane w niniejszej PODO.

Rozdział 6. Role i odpowiedzialność za bezpieczeństwo danych osobowych

§ 6.

Szczególna rola i odpowiedzialność za bezpieczeństwo danych osobowych spoczywa na:

a) Zarządzie Spółki;
b) Kierownikach poszczególnych działów;
c) Kierowniku Działu IT oraz pracownikach i współpracownikach Działu IT;
d) Inspektorze ochrony danych (IOD)

§ 7.

1) Zarząd Spółki sprawuje nadzór nad bezpieczeństwem danych osobowych, w szczególności odpowiada za odpowiednią strukturę organizacyjną i podział zadań zapewniający bezpieczeństwo danych i systemów teleinformatycznych
2) Do kompetencji Zarządu Spółki należy:
   a) prawna odpowiedzialność za funkcjonowanie Spółki, w tym również za przestrzeganie wymagań związanych z zabezpieczeniem danych osobowych i systemów teleinformatycznych;

b) zatwierdzanie i publikowanie dokumentów i procedur związanych z ochroną danych osobowych dotyczących wszystkich pracowników i współpracowników Spółki;
c) zapewnienie wsparcia organizacyjno-finansowego przy wdrażaniu mechanizmów zabezpieczenia danych osobowych i systemów teleinformatycznych;
d) zapewnienie odpowiednich pomieszczeń (stosownie zabezpieczonych i wyposażonych) do procesu przetwarzania i przechowywania danych osobowych;
e) uwzględnianie kryterium wiarygodności zatrudnianych pracowników i współpracowników przy rekrutacji na stanowiska związane z dostępem do krytycznych danych osobowych lub z administracją krytycznych komponentów systemów teleinformatycznych;
f) zaznajomienie pracowników i współpracowników z prawnymi oraz pracowniczymi konsekwencjami naruszenia bezpieczeństwa danych osobowych (za pośrednictwem IOD);
g) zapewnienie pracownikom i współpracownikom szkoleń w zakresie poszerzania wiedzy i świadomości związanej z bezpieczeństwem danych osobowych oraz stosowanymi rozwiązaniami używanymi w celu utrzymania bądź zapewnienia odpowiedniego poziomu zabezpieczeń stosowanych w procesach przetwarzania i gromadzenia danych (co do zasady szkolenia w powyższym zakresie prowadzi IOD);
h) wyznaczenie i powołanie IOD;
i) przestrzeganie innych zasad określonych w dokumencie stanowiącym **załącznik nr 2** do PODO.

§ 8.

Do zadań kierowników, w tym w szczególności właścicieli biznesowych dla poszczególnych procesów przetwarzania danych należy:

a) nadzór nad przestrzeganiem zasad i procedur składających się na PODO w pracy kierowanego działu;
b) promowanie i wymaganie postaw zgodnych z zasadami bezpieczeństwa danych osobowych przyjętymi w Spółce, w tym reakcja na wszelkie wykryte nieprawidłowości,
c) przekazywanie, bezpośrednio po wykryciu naruszenia ochrony danych osobowych, stosownej informacji o takim naruszeniu łącznie do Kierownika Działu IT oraz IOD (uwaga – w przypadkach szczególnych Spółka ma obowiązek zgłosić naruszenie do Prezesa Urzędu Ochrony Danych Osobowych i ma na to 72 godziny liczone od wykrycia naruszenia, stąd reakcja kierownika musi być niezwłoczna); informacja taka powinna zawierać:
   - opis charakteru 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;
   - opis możliwe konsekwencje naruszenia ochrony danych osobowych, na tyle na ile jest to możliwe.

d) identyfikowanie podatności i zagrożeń dla nadzorowanych procesów przetwarzania danych i przekazywanie w tym zakresie informacji do Kierownika Działu IT oraz IOD;
e) uczestniczenie w procesie oceny i postępowania z ryzykiem, które odnosi się do nadzorowanych przez danego kierownika procesów przetwarzania danych;
f) współpraca z innymi podmiotami i osobami odpowiedzialnymi za bezpieczeństwo danych osobowych w Spółce;
g) przestrzeganie innych zasad określonych w dokumencie stanowiącym **załącznik nr 2** do PODO.

§ 9.

Do zadań Kierownika Działu IT oraz pracowników i współpracowników Działu IT, oprócz tych, które zostały wprost wskazane w PODO albo jej załącznikach, należą:

a) dbanie o poprawne i efektywne działanie administrowanych systemów teleinformatycznych;
b) opiniowanie zgłoszeń w zakresie potrzeb dotyczących rozwoju systemów teleinformatycznych;
c) uczestniczenie w identyfikacji i ocenie ryzyka związanego ze środowiskiem teleinformatycznym;
d) uczestniczenie w procesie oceny i postępowania z ryzykiem;
e) wdrażanie odpowiednich środków organizacyjnych i technicznych odpowiadających zidentyfikowanym w trakcie oceny ryzyka zagrożeniom;
f) świadczenie wsparcie technicznego dla użytkowników systemów teleinformatycznych;
g) wykonywanie i/lub nadzorowanie procedury backupu danych osobowych (sporządzania kopii awaryjnych);
h) reagowanie i podejmowanie stosownych działań w odniesieniu do wykrytych incydentów naruszenia ochrony danych osobowych;
i) na wniosek kierownika danego działu nadawanie użytkownikom prawa dostępu do systemów teleinformatycznych;
j) uczestniczenie w przygotowaniu propozycji zakresu testów, dokonywanie instalacji i uczestniczenie w testowaniu nowych wersji oprogramowania w środowisku testowym;
k) sporządzanie zapotrzebowania na oprogramowanie, sprzęt i usługi związane z technicznymi aspektami ochrony systemu teleinformatycznego;
l) dokonywanie i/lub nadzorowanie bezpiecznej eliminacji wycofanych z użytku systemów i komponentów infrastruktury teleinformatycznej;
m) odpowiedzialność za ciągłość działania systemów i infrastruktury teleinformatycznej oraz łączy teleinformatycznych;

n) dbanie o właściwe wyposażenie lokalizacji zapasowych (o ile występują), a także odpowiednie zabezpieczenie zasobów awaryjnych;
o) monitorowanie dostępności systemów teleinformatycznych;
p) odpowiedzialność za odtworzenie danych osobowych z kopii awaryjnych;
q) sprawowanie nadzoru nad działaniem zewnętrznych dostawców usług w zakresie jakości i przestrzegania standardów bezpieczeństwa danych osobowych w zakresie czynności technicznych realizowanych w związku z wykonaniem umów;
r) przestrzeganie innych zasad określonych w dokumencie stanowiącym **załącznik nr 2** do PODO.

§ 10.

Do zadań użytkowników, oprócz tych, które zostały wprost wskazane w PODO albo jej załącznikach, należą:

a) przestrzeganie zasad określonych w PODO i wskazanych w niej załącznikach;
b) zapewnienie poufności w stosunku do wszystkich danych osobowych przetwarzanych w Spółce;
c) zabronione jest rozpowszechnianie danych osobowych podlegających ochronie
d) obowiązek zachowania poufności danych osobowych w Spółce w zakresie związanym z wykonywaniem przez pracowników i współpracowników zadań dla Spółki nie wygasa po ustaniu stosunku pracy/współpracy;
e) przestrzeganie innych zasad określonych w dokumencie stanowiącym **załącznik nr 2** do PODO.

Rozdział 7. Procedury i zasady ochrony danych osobowych

§ 11.

Szczegółowa procedura zgłaszania naruszeń stanowi **załącznik nr 3** do PODO.

§ 12.

Szczegółowa procedura projektowania nowych procesów stanowi **załącznik nr 4** do PODO.

§ 13.

Szczegółowa procedura ochrony danych osobowych w relacjach z dostawcami stanowi **załącznik nr 5** do PODO.

§ 14.

Szczegółowa procedura nadawania upoważnień stanowi **załącznik nr 6** do PODO.

§ 15.

Zasady korzystania z przydzielonego sprzętu stanowią **załącznik nr 7** do PODO.

§ 16.

Zasady pracy z pocztą elektroniczną stanowią **załącznik nr 8** do PODO.

§ 17.

Zasady zabezpieczenia danych na stanowisku pracy stanowią **załącznik nr 9** do PODO.

§ 18.

Szczegółowa procedura dokonywania przeglądów praw dostępu stanowi **załącznik nr 10** do PODO.

§ 19.

Zasady korzystania z systemów IT stanowią **załącznik nr 11** do PODO.

§ 20.

Szczegółowa procedura zarządzania danymi służącymi do uwierzytelniania stanowi **załącznik nr 12** do PODO.

§ 21.

Szczegółowa procedura obsługi wniosków podmiotów danych stanowi **załącznik nr 13** do PODO.

Rozdział 8. Szkolenia i edukacja

§ 22.

1) Pracownicy i współpracownicy Spółki w zakresie odpowiednim do swoich zadań i obowiązków są zobowiązani znać treść niniejszej PODO oraz wskazanych w niej załączników.
2) Pracownicy i współpracownicy Spółki powinni zostać poinformowani o zakresie odpowiedzialności i obowiązków wynikających z niniejszej PODO wraz z konsekwencjami prawnymi i dyscyplinarnymi w przypadku jej naruszenia.
3) Wszyscy pracownicy i współpracownicy zobligowani są do uczestnictwa w szkoleniach dotyczących ochrony danych osobowych.

§ 23.

Szkolenia w zakresie ochrony danych osobowych przeprowadza się cyklicznie, lub w razie potrzeby na wniosek Kierownika Działu HR.

Rozdział 9. Audyt

§ 24.

1) PODO powinna być poddawana regularnym audytom.
2) Do przeprowadzania audytu upoważnieni są, każdy we właściwym zakresie (odpowiadającym realizowanym zadaniom służbowym):
   a) osoby zatrudnione na stanowisku audytora wewnętrznego;
   b) IOD;
   c) Kierownik Działu IT i/lub upoważnieni przez niego pracownicy i współpracownicy Działu IT;

d) podmioty zewnętrzne za zgodą Zarządu Spółki.

3) Przeprowadzenie audytu wymaga sporządzenia jego planu, w którym określa się m.in. cel, kryteria, zakres podmiotowy i przedmiotowy.
4) Wyniki audytu przedstawia się kierownikowi działu objętego czynnościami audytowymi oraz Zarządowi Spółki.

Rozdział 10. Przegląd i aktualizacja PODO

§ 25.

1) Przegląd PODO powinien być dokonywany co najmniej raz do roku z zastrzeżeniem postanowień ust. 2.
2) W przypadku wystąpienia znaczących zmian powinien być przeprowadzany przegląd doraźny, którego celem będzie weryfikacja zasad i ewentualne dostosowanie PODO do zmian środowiska organizacyjnego, warunków biznesowych, środowiska technicznego, a także w zakresie zachowania zgodności z przepisami powszechnie obowiązującego prawa.
3) Aktualizacji PODO dokonuje IOD.
4) Wszelkie zmiany w niniejszej Polityce wymagają akceptacji IOD.