POLITYKA OCHRONY DANYCH OSOBOWYCH W LOOKSOFT SP. Z O.O.

21.05.2018 R.

Wersja 1.0

Spis treści

I. **POSTANOWIENIA OGÓLNE** ... 3
Przedmiot Polityki ... 3
Słowniczek ... 4
II. **FUNDAMENTY I ZASADY OCHRONY DANYCH OSOBOWYCH** ... 6
Fundamenty systemu ochrony danych osobowych ... 7
Zasady ochrony danych osobowych ... 7
III. **PODMIOTY TWORZĄCE SYSTEM OCHRONY DANYCH OSOBOWYCH** ... 8
Współadministrator danych osobowych ... 8
Inspektor Ochrony Danych ... 8
Osoby upoważnione ... 10
Podmioty przetwarzające ... 11
Administrator Danych Osobowych jako podmiot przetwarzający ... 11
Odbiorcy danych osobowych ... 12
IV. **PRZETWARZANIE DANYCH OSOBOWYCH** ... 12
Zarządzanie ryzykiem ... 12
Ocena skutków dla ochrony danych osobowych ... 13
Uprzednie konsultacje z Prezesem Urzędu Ochrony Danych Osobowych ... 13
Privacy by design i privacy by default ... 13
Inwentaryzacja ... 13
Rejestr czynności przetwarzania danych osobowych ... 14
Identyfikacja i weryfikacja podstaw prawnych przetwarzania danych osobowych ... 14
Przetwarzanie danych osobowych na podstawie zgody ... 15
Profilowanie i zautomatyzowane podejmowanie decyzji ... 15
Minimalizacja ... 16
Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych ... 16
V. **UPRAWNIENIA OSÓB FIZYCZNYCH** ... 16
Obowiązki informacyjne ... 17
Rodzaje uprawnień osób fizycznych ... 18
Realizacja uprawnień osób fizycznych ... 18
Pobieranie opłat za wykonywanie uprawnień ... 18
VI. B**EZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH** ... 19
Obowiązek zapewnienia bezpieczeństwa przetwarzania danych osobowych ... 19
Systemy informatyczne ... 19
Zasady bezpieczeństwa ... 20
Wykrywanie i klasyfikowanie naruszeń ochrony danych osobowych ... 20
Zawiadamianie o naruszeniu ochrony danych osobowych ... 20
VII. **KONTROLA I DOSKONALENIE SYSTEMU OCHRONY DANYCH OSOBOWYCH** ... 21
Audyt wewnętrzny ... 21
Kontrola przetwarzania danych osobowych ... 21
Przegląd Polityki i załączników ... 21
Szkolenia ... 22
VIII. **WYKAZ ZAŁĄCZNIKÓW** ... 22
Wykaz załączników ... 22
IX. **POSTANOWIENIA KOŃCOWE** ... 23
Postanowienia końcowe ... 24

I. POSTANOWIENIA OGÓLNE

§ 1.
Przedmiot Polityki

1. **Looksoft Spółka z ograniczoną odpowiedzialnością.** jest Administratorem Danych Osobowych w rozumieniu art. 4 pkt 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE L z dnia 4 maja 2016 r.).
2. W celu zapewnienia przetwarzania danych osobowych przez Administratora Danych Osobowych zgodnie z obowiązującym prawem, a w szczególności zapewnienia najwyższej ochrony przetwarzanych danych osobowych, Administrator Danych Osobowych przyjmuje niniejszą Politykę.
3. Niniejsza Polityka jest zgodna z:
   a) rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE L z dnia 4 maja 2016 r. — dalej: RODO);
   b) ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych— dalej: u.o.d.o.);
   c) ustawą z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t. j. Dz. U. 2017 poz. 1219, z późn. zm. — dalej: u.ś.u.d.e.);
   d) ustawą z dnia 26 czerwca 1974 r. — Kodeks pracy (t. j. Dz. U. 2018 poz. 108, z późn. zm. — dalej: k.p.);

4. Polityka stanowi część składową systemu ochrony danych osobowych obowiązującego u Administratora Danych Osobowych, określając w szczególności:
   a) zasady przetwarzania danych osobowych u Administratora Danych Osobowych;
   b) zasady zapewniania ochrony przetwarzanych danych osobowych;
   c) procedury stosowane u Administratora Danych Osobowych;
   d) wzorce dokumentów i formularzy stosowanych przez Administratora Danych Osobowych;
   e) wzorce klauzul informacyjnych;
   f) wzorce klauzul zgody.
5. Niniejsza Polityka jest środkiem prawnym przewidzianym w art. 24 ust. 2 RODO.

§ 2.
Słowniczek

Na potrzeby niniejszej Polityki przyjmuje się następujące definicje użytych pojęć:

	Pojęcie	Definicja
a) a)	**Administrator Danych Osobowych**	**LookSoft Sp. z o.o.** z siedzibą w Warszawie przy ulicy Grochowskiej 14E, 04-217 Warszawa, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m. st. Warszawy, XIII Wydział Gospodarczy KRS pod numerem KRS: 0000276822, kapitał zakładowy 50 000,00 PLN, NIP 1132662715 , REGON 140930064.
b) b)	**Administrator Systemów Informatycznych**	osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za funkcjonowanie i bezpieczeństwo systemów informatycznych
c)	**Dane niezidentyfikowane**	Dane osobowe, których Administrator Danych Osobowych nie identyfikuje w odniesieniu do konkretnych podmiotów danych (np. zapis z monitoringu, korespondencja e-mailowa zawierająca dane osób trzecich)
d) c)	**Dane osobowe**	wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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
e) d)	**Dane dzieci**	dane osobowe osób fizycznych poniżej 16. roku życia
f) e)	**Dane karne**	dane osobowe dotyczące wyroków skazujących i czynów zabronionych lub powiązanych środków bezpieczeństwa
g) f)	**Dane szczególne**	dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych; dane genetyczne; dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej; dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby fizycznej
h) g)	**Dane zwykłe**	dane osobowe, które nie są danymi szczególnymi
i) h)	**Dostępność**	zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, kiedy jest to potrzebne
j) j)	**Incydent**	zdarzenie mogące wpłynąć na bezpieczeństwo danych osobowych w zakresie dostępności, integralności, poufności lub odporności systemów i usług przetwarzania. Incydent może prowadzić do naruszenia ochrony danych osobowych, ale nie musi
k) k)	**Inspektor Ochrony Danych (IOD)**	osoba wyznaczona przez Administratora Danych Osobowych do wypełniania zadań przewidzianych w art. 39 ust. 1 RODO
l) m)	**Integralność**	zapewnienie dokładności i kompletności informacji oraz metod przetwarzania
m) n)	**Naruszenie ochrony danych osobowych**	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
n) o)	**Odbiorca danych osobowych**	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną (osobą) trzecią. Nie uznaje się za odbiorców organów publicznych, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego
o) p)	**Odporność**	zdolność systemów informatycznych do prawidłowego funkcjonowania mimo dużego obciążenia
p) q)	**Osoba upoważniona**	osoba upoważniona przez Administratora Danych Osobowych do przetwarzania danych osobowych w określonym przez niego zakresie
q) r)	**Państwo trzecie**	państwo nienależące do Unii Europejskiej oraz Europejskiego Obszaru Gospodarczego
r) s)	**Podmiot danych**	osoba fizyczna, której dane osobowe dotyczą
s) t)	**Podmiot przetwarzający**	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych Osobowych
t) u)	**Polityka**	niniejsza „Polityka ochrony danych osobowych w LookSoft**”**
u) v)	**Poufność**	zapewnienie, że dane osobowe są dostępne jedynie dla osób upoważnionych
v) w)	**Profilowanie**	dowolna forma 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
w) x)	**Przetwarzanie danych osobowych**	operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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
x) y)	**Pseudonimizacja**	przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej
y) z)	**Rozliczalność**	wykazanie przez Administratora Danych Osobowych, że przestrzega przepisów dotyczących ochrony danych osobowych w prowadzonych procesach przetwarzania danych osobowych

z) za)	**Strona (osoba) trzecia**	osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż: – osoba, której dane dotyczą; – Administrator Danych Osobowych i współadministrator danych osobowych; – podmiot przetwarzający; – osoba upoważniona
aa) zb	**System informatyczny**	zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych
bb) zc)	**System ochrony danych osobowych**	całokształt środków technicznych, organizacyjnych i prawnych wraz z niezbędną dokumentacją, wdrożonych przez Administratora Danych Osobowych, służących zapewnieniu, że przetwarzanie danych osobowych będzie odbywało się zgodnie z przepisami z zakresu ochrony danych osobowych
cc) zd	**Współadministrator danych osobowych**	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który wspólnie z Administratorem Danych Osobowych decyduje o celach i sposobach przetwarzania danych osobowych
dd) ze)	**Zagrożenie**	potencjalna możliwość wystąpienia incydentu
ee) zf)	**Zbiór danych osobowych**	uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie
ff) zg)	**Zgoda**	dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych

II. FUNDAMENTY I ZASADY OCHRONY DANYCH OSOBOWYCH

§ 3.
Fundamenty systemu ochrony danych osobowych

Administrator Danych Osobowych tworzy system ochrony danych osobowych w swojej organizacji, budując go na następujących fundamentach:

a) **podejście oparte na ryzyku** — Administrator Danych Osobowych jest zobowiązany zidentyfikować ryzyka towarzyszące przetwarzaniu danych osobowych oraz ustalić ich wpływ na operacje związane z danymi osobowymi, a w szczególności na prawa i wolności osób fizycznych;

b) **poszanowanie praw osób fizycznych** — Administrator Danych Osobowych, jak również wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych, są zobowiązani ułatwić osobom fizycznym realizację ich praw związanych z ochroną danych osobowych;

c) **legalność** — Administrator Danych Osobowych, jak również wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych, są zobowiązani

przeprowadzać jakiekolwiek operacje związane z danymi osobowymi przy zachowaniu pełnej zgodności z obowiązującym prawem;

d) **bezpieczeństwo** — Administrator Danych Osobowych jest zobowiązany zapewnić bezpieczeństwo przetwarzania danych osobowych, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze;

e) **rozliczalność** — Administrator Danych Osobowych, jak również wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych, są zobowiązani dokumentować sposób spełnienia obowiązków wynikających z przepisów z zakresu ochrony danych osobowych.

§ 4.

Zasady ochrony danych osobowych

Administrator Danych Osobowych przetwarza dane osobowe w oparciu o następujące zasady:

a) **zasada zgodności z prawem, rzetelności i przejrzystości** — dane osobowe są przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;

b) **zasada ograniczenia celu** — dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;

c) **zasada minimalizacji danych** — dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;

d) **zasada prawidłowości** — dane osobowe są prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;

e) **zasada czasowości** — dane osobowe są przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;

f) **zasada integralności i poufności** — dane osobowe są przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

III. PODMIOTY TWORZĄCE SYSTEM OCHRONY DANYCH OSOBOWYCH

§ 5.

Współadministrator danych osobowych

1. Administrator Danych Osobowych może wspólnie ustalać cele i sposoby przetwarzania danych osobowych ze współadministratorem danych osobowych — jeżeli taka konieczność wynika z przedsięwzięć realizowanych przez Administratora Danych Osobowych.
2. Administrator Danych Osobowych jest zobowiązany zawrzeć ze współadministratorem danych osobowych umowę o współadministrowanie danymi osobowymi, której wzór stanowi Załącznik nr 1.
3. W umowie o współadministrowanie danymi osobowymi należy określić w szczególności:
   a) zakresy odpowiedzialności Administratora Danych Osobowych i współadministratora danych osobowych;
   b) sposób realizowania obowiązków wynikających z przepisów z zakresu ochrony danych osobowych;
   c) sposób spełnienia obowiązków informacyjnych z art. 13 RODO i art. 14 RODO;
   d) punkt kontaktowy — jeżeli jest to wskazane;
   e) relacje pomiędzy Administratorem Danych Osobowych i współadministratorem danych osobowych a podmiotami danych;
   f) sposób przekazania podmiotom danych treści uzgodnień pomiędzy Administratorem Danych Osobowych a współadministratorem danych osobowych.

§ 6.

Inspektor Ochrony Danych

1. W przypadkach wskazanych w art. 37 ust. 1 RODO lub w prawie polskim Administrator Danych Osobowych jest zobowiązany wyznaczyć Inspektora Ochrony Danych.
2. W przypadkach innych niż wskazane w ust. 1, Administrator Danych Osobowych może podjąć decyzję o dobrowolnym wyznaczeniu Inspektora Ochrony Danych.
3. Administrator Danych Osobowych zawiadamia Prezesa Urzędu Ochrony Danych Osobowych w terminie 14 dni o:
   a) wyznaczeniu Inspektora Ochrony Danych, podając jego dane kontaktowe;
   b) zmianie Inspektora Ochrony Danych, podając jego dane kontaktowe;
   c) rezygnacji z wyznaczania Inspektora Ochrony Danych, jeżeli wcześniej był wyznaczony.
4. Administrator Danych Osobowych może zatrudnić Inspektora Ochrony Danych na podstawie umowy o pracę lub na podstawie cywilnoprawnej umowy o świadczenie usług.
5. Z uwagi na konflikt interesów Inspektorem Ochrony Danych nie może być osoba zatrudniona na stanowisku, które decyduje o celach przetwarzania danych osobowych.
6. Inspektor Ochrony Danych ma za zadanie:
   a) informować Administratora Danych Osobowych oraz osoby przez niego zatrudnione, które przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy prawa;

b) doradzać w sprawie przestrzegania przepisów z zakresu ochrony danych osobowych;
c) monitorować przestrzeganie przepisów z zakresu ochrony danych osobowych, niniejszej Polityki oraz innych dokumentów Administratora Danych Osobowych;
d) monitorować podział obowiązków;
e) podejmować działania zwiększające świadomość w zakresie ochrony danych osobowych;
f) przeprowadzać szkolenia osób zatrudnionych w zakresie ochrony danych osobowych;
g) prowadzić audyty;
h) udzielać na żądanie Administratora Danych Osobowych zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitorować jej wykonanie zgodnie z art. 35 RODO;
i) współpracować z Prezesem Urzędu Ochrony Danych Osobowych;
j) pełnić funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzić konsultacje we wszelkich innych sprawach.

7. Administrator Danych Osobowych jest zobowiązany zapewnić, by Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
8. Administrator Danych Osobowych jest zobowiązany wspierać Inspektora Ochrony Danych w wypełnianiu przez niego zadań, o których mowa w ust. 7, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
9. Administrator Danych Osobowych:
   a) nie może wydawać Inspektorowi Ochrony Danych żadnych instrukcji;
   b) nie może karać Inspektora Ochrony Danych za wykonywanie przez niego obowiązków;
   c) nie może odwołać Inspektora Ochrony Danych za wykonywanie przez niego obowiązków.
10. Inspektor Ochrony Danych podlega bezpośrednio Administratorowi Danych Osobowych lub najwyższemu kierownictwu Administratorów Danych Osobowych.

§ 7.
Osoby upoważnione

1. Przetwarzania danych osobowych w ramach struktury Administratora Danych Osobowych mogą dokonywać wyłącznie osoby upoważnione przez Administratora Danych Osobowych.
2. Administrator Danych Osobowych zapewnia, aby żadna z osób upoważnionych nie miała dostępu do większej ilości danych osobowych i procesów przetwarzania danych osobowych niż jest to konieczne do prawidłowego wypełniania obowiązków i zadań.
3. Procedura nadawania, zmiany i odbierania upoważnień stanowi Załącznik nr 2.

4. Osoba upoważniona do przetwarzania danych osobowych przed przystąpieniem do czynności ma obowiązek:
   a) zapoznać się z dokumentami z zakresu ochrony danych osobowych, w szczególności z niniejszą Polityką — w zakresie ustalonym przez Administratora Danych Osobowych;
   b) odbyć szkolenie z zakresu ochrony danych osobowych;
   c) złożyć oświadczenie na piśmie o zapoznaniu się z dokumentami z zakresu ochrony danych osobowych oraz o odbyciu szkolenia z zakresu ochrony danych osobowych;
   d) złożyć oświadczenie na piśmie o przestrzeganiu zasad ochrony danych osobowych oraz ustalonych procedur.
5. Wzory oświadczeń, o których mowa w ust. 4, stanowią Załącznik nr 3.
6. Oświadczenia, o których mowa w ust. 4, są dołączane do umowy zawartej z osobą upoważnioną lub do akt osobowych osoby upoważnionej.
7. Administrator Danych Osobowych zapewnia osobom upoważnionym dostęp do dokumentów z zakresu ochrony danych, z wyjątkiem tych dokumentów, które nie powinny być dostępne dla wszystkich osób upoważnionych.
8. Obowiązki określone w ust. 4 nie dotyczą osób, które są dopuszczane do przetwarzania danych osobowych incydentalnie (np. w celu naprawy sprzętu). W takiej sytuacji należy wskazać w treści zawartej umowy obowiązek przestrzegania ochrony danych osobowych oraz przekazać najważniejsze informacje na temat ochrony danych osobowych. W zależności od sytuacji z takimi osobami można zawrzeć również umowę powierzenia.
9. Administrator Danych Osobowych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.
10. Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych stanowi Załącznik nr 4.

§ 8.

Podmioty przetwarzające

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych podmiotowi przetwarzającemu w zależności od własnych potrzeb.
2. Administrator Danych Osobowych jest zobowiązany powierzać przetwarzanie danych osobowych tylko takim podmiotom przetwarzającym, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Zakazane jest korzystanie z usług podmiotów przetwarzających, które takich gwarancji nie dają.
3. Wzór umowy powierzenia przetwarzania danych osobowych stanowi Załącznik nr 5.
4. W przypadku korzystania przez podmiot przetwarzający z usług innego podmiotu przetwarzającego, który nie daje analogicznych gwarancji, o jakich mowa w ust. 2, Administrator Danych Osobowych jest zobowiązany wnieść sprzeciw, a w innych przypadkach — może wnieść sprzeciw, jeżeli istnieją ku niemu podstawy.

5. Wzór sprzeciwu stanowi załącznik do umowy powierzenia przetwarzania danych osobowych.
6. Administrator Danych Osobowych jest zobowiązany kontrolować przestrzeganie przez podmiot przetwarzający przepisów RODO przez cały okres trwania umowy.
7. W przypadku naruszania przez podmiot przetwarzający przepisów RODO Administrator Danych Osobowych jest zobowiązany niezwłocznie zaprzestać współpracy z podmiotem przetwarzającym.
8. Administrator Danych Osobowych prowadzi ewidencję podmiotów przetwarzających, z którymi zawarł umowy o powierzenie przetwarzania danych osobowych.
9. Wzór ewidencji podmiotów przetwarzających stanowi Załącznik nr 6.

§ 9.

Administrator Danych Osobowych jako podmiot przetwarzający

1. W związku z prowadzoną działalnością Administrator Danych Osobowych może być podmiotem przetwarzającym dla innego administratora danych osobowych.
2. W przypadkach wskazanych w ust. 1 Administrator Danych Osobowych zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
3. W przypadkach wskazanych w ust. 1 Administrator Danych Osobowych wywiązuje się z obowiązków przewidzianych w umowie powierzenia przetwarzania danych osobowych, którą zawiera z innym administratorem danych osobowych.
4. W przypadkach wskazanych w ust. 1 Administrator Danych Osobowych może być zobowiązany do wyznaczenia Inspektora Ochrony Danych w związku z umową o powierzeniu przetwarzania danych osobowych zawartą z innym administratorem danych osobowych. W takiej sytuacji § 6 stosuje się odpowiednio.
5. W przypadkach wskazanych w ust. 1 Administrator Danych Osobowych prowadzi rejestr wszystkich kategorii czynności przetwarzania.
6. Wzór rejestru wszystkich kategorii czynności przetwarzania stanowi Załącznik nr 7.

§ 10.

Odbiorcy danych osobowych

1. Administrator Danych Osobowych ujawnia dane osobowe odbiorcom danych osobowych wyłącznie po zweryfikowaniu podstawy prawnej takiego ujawnienia.
2. W przypadku braku podstawy prawnej, o której mowa w ust. 1, Administrator Danych Osobowych odmawia ujawnienia danych osobowych jakiemukolwiek odbiorcy danych osobowych.
3. Administrator Danych Osobowych prowadzi ewidencję odbiorców danych osobowych.
4. Wzór ewidencji odbiorców danych osobowych stanowi Załącznik nr 8.
5. Administrator Danych Osobowych prowadzi rejestr żądań udostępnień danych osobowych.

6. Wzór rejestru żądań udostępnień danych osobowych stanowi Załącznik nr 9.

IV. PRZETWARZANIE DANYCH OSOBOWYCH

§ 11.
Zarządzanie ryzykiem

1. Administrator Danych Osobowych wdraża i utrzymuje procedurę zarządzania ryzykiem.
2. Administrator Danych Osobowych jest zobowiązany uwzględniać ryzyko w planowanych i prowadzonych procesach przetwarzania danych osobowych.
3. Procedura zarządzania ryzykiem stanowi Załącznik nr 10.

§ 12.
Ocena skutków dla ochrony danych osobowych

1. W przypadkach wskazanych w art. 35 ust. 1 RODO, art. 35 ust. 3 RODO oraz w odniesieniu do operacji przetwarzania znajdujących się w wykazie publikowanym przez Prezesa Urzędu Ochrony Danych Osobowych na podstawie art. 35 ust. 4 RODO Administrator Danych Osobowych jest zobowiązany przeprowadzić ocenę skutków dla ochrony danych osobowych.
2. Ocena skutków dla ochrony danych osobowych nie jest wymagana w odniesieniu do operacji przetwarzania znajdujących się w wykazie publikowanym przez Prezesa Urzędu Ochrony Danych Osobowych na podstawie art. 35 ust. 5 RODO.
3. Procedura przeprowadzania oceny skutków dla ochrony danych osobowych stanowi Załącznik nr 11.

§ 13.
Uprzednie konsultacje z Prezesem Urzędu Ochrony Danych Osobowych

1. Jeżeli z oceny skutków dla ochrony danych osobowych wynika, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator Danych Osobowych nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania Administrator Danych Osobowych jest zobowiązany skonsultować się z Prezesem Urzędu Ochrony Danych Osobowych.
2. Procedura przeprowadzania uprzednich konsultacji z Prezesem Urzędu Ochrony Danych Osobowych stanowi Załącznik nr 12.

§ 14.
Privacy by design i privacy by default

1. Administrator Danych Osobowych jest zobowiązany uwzględniać ochronę danych osobowych w fazie projektowania nowych systemów, programów, aplikacji, usług, a także w fazie projektowania nowych procesów i sposobów przetwarzania danych osobowych (privacy by design).

2. Administrator Danych Osobowych jest zobowiązany zapewnić domyślną ochronę danych osobowych, tj. domyślnie mogą być przetwarzane tylko te dane osobowe, które są niezbędne do osiągnięcia konkretnego celu przetwarzania (privacy by default). Rezygnacja z prywatności lub jej ograniczenie mogą nastąpić tylko na wyraźne żądanie podmiotu danych.
3. Procedura privacy by design i privacy by default stanowi Załącznik nr 13.

§ 15.

Inwentaryzacja

1. Administrator Danych Osobowych szczegółowo inwentaryzuje posiadane dane osobowe oraz procesy z nimi związane, ze szczególnym uwzględnieniem:
   a) danych szczególnych;
   b) danych karnych;
   c) danych dzieci;
   d) danych osobowych poddanych profilowaniu i zautomatyzowanemu podejmowaniu decyzji.
2. W celu zapewnienia pełnej kontroli nad przetwarzaniem danych osobowych oraz zapewnienia bezpieczeństwa przetwarzania danych osobowych Administrator Danych Osobowych prowadzi:
   a) ewidencję zbiorów danych osobowych — wzór ewidencji zbiorów danych osobowych stanowi Załącznik nr 14;
   b) ewidencję pomieszczeń — wzór ewidencji pomieszczeń stanowi Załącznik nr 15;
   c) ewidencję stacji roboczych, urządzeń przenośnych i nośników — wzór ewidencji stacji roboczych, urządzeń przenośnych i nośników stanowi Załącznik nr 16;
   d) ewidencję programów komputerowych (aplikacji) — wzór ewidencji programów komputerowych (aplikacji) stanowi Załącznik nr 17.
3. Administrator Danych Osobowych kontroluje przetwarzanie danych niezidentyfikowanych, o których mowa w art. 11 ust. 1 RODO, w szczególności w odniesieniu do nagrań (wizualnych, dźwiękowych, audiowizualnych), korespondencji elektronicznej i wszelkich innych strumieni, które potencjalnie mogą zawierać dane osobowe.

§ 16.

Rejestr czynności przetwarzania danych osobowych

1. Administrator Danych Osobowych prowadzi i aktualizuje rejestr czynności przetwarzania danych osobowych, który jest najważniejszym dokumentem w zakresie ochrony danych osobowych.
2. Rejestr czynności przetwarzania danych osobowych służy:
   a) inwentaryzowaniu i monitorowaniu sposobu przetwarzania danych osobowych;
   b) dokumentowaniu czynności przetwarzania danych osobowych;
   c) wykazaniu realizacji zasady rozliczalności.

3. Wzór rejestru czynności przetwarzania danych osobowych stanowi Załącznik nr 18.

§ 17.

Identyfikacja i weryfikacja podstaw prawnych przetwarzania danych osobowych

1. Administrator Danych Osobowych jest zobowiązany przetwarzać dane osobowe wyłącznie w oparciu o konkretną podstawę prawną.
2. Administrator Danych Osobowych jest zobowiązany w odniesieniu do każdej czynności przetwarzania danych osobowych zidentyfikować i zweryfikować podstawę prawną przetwarzania danych osobowych.
3. Wykaz podstaw prawnych stanowi Załącznik nr 19.
4. Administrator Danych Osobowych jest zobowiązany monitorować zmiany legislacyjne i w miarę konieczności aktualizować wykaz, o którym mowa w ust. 3.
5. Administrator Danych Osobowych jest zobowiązany wskazać w wykazie, o którym mowa w ust. 3, swoje prawnie uzasadnione interesy, legalizujące przetwarzanie danych osobowych na podstawie art. 6 ust. 1 lit. f RODO.
6. Osoby upoważnione do przetwarzania danych osobowych mają obowiązek znać podstawy prawne, w oparciu o które wykonują czynności związane z danymi osobowymi.

§ 18.

Przetwarzanie danych osobowych na podstawie zgody

1. Administrator Danych Osobowych przetwarza dane osobowe na podstawie zgody tylko wówczas, gdy nie ma innej podstawy przetwarzania danych osobowych. Nie należy uzyskiwać zgody na przetwarzanie danych osobowych związanych z zawarciem i wykonaniem umowy lub w odniesieniu do takich danych osobowych, których obowiązek przetwarzania wynika z przepisów prawa.
2. Przed podjęciem decyzji o przetwarzaniu danych osobowych na podstawie zgody Administrator Danych Osobowych jest zobowiązany zweryfikować, czy dane osobowe są adekwatne do założonego celu przetwarzania.
3. Zabronione jest wywieranie przymusu w celu uzyskania zgody, w szczególności poprzez odmowę wykonania umowy w przypadku niewyrażenia zgody na przetwarzanie danych osobowych.
4. Zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie je odróżnić od pozostałych kwestii.
5. Zgody muszą być formułowane w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
6. Wykaz stosowanych klauzul zgód stanowi Załącznik nr 20.
7. Zgoda może być cofnięta w każdym momencie. Administrator Danych Osobowych zapewnia, aby wycofanie zgody było równie proste, jak jej złożenie.

8. Administrator Danych Osobowych jest zobowiązany zapewnić system zarządzania zgodami, który pozwoli zweryfikować, czy dana osoba udzieliła zgody na przetwarzanie danych osobowych, czy i kiedy ją wycofała.

§ 19.

Profilowanie i zautomatyzowane podejmowanie decyzji

1. Jeżeli Administrator Danych Osobowych podejmuje czynności profilowania lub zautomatyzowanego podejmowania decyzji, jest zobowiązany zapewnić, aby te czynności odbywały się zgodnie z prawem.
2. Procedurę określającą zasady profilowania i zautomatyzowanego podejmowania decyzji określa Załącznik nr 21.

§ 20.

Minimalizacja

1. Administrator Danych Osobowych jest zobowiązany przestrzegać zasady minimalizacji.
2. W celu zapewnienia realizacji zasady minimalizacji Administrator Danych Osobowych w szczególności:
   a) weryfikuje ilość przetwarzanych danych osobowych — Administrator Danych Osobowych nie może przetwarzać większej ilości danych osobowych niż to wynika z założonego celu;
   b) weryfikuje zakres przetwarzanych danych osobowych — Administrator Danych Osobowych nie może podejmować większej liczby czynności przetwarzania niż to wynika z założonego celu;
   c) ogranicza dostęp do danych osobowych poprzez stosowanie środków prawnych (umowy z klauzulami poufności, system upoważnień), środków fizycznych (kontrola dostępu osób do budynków, pomieszczeń i systemów) oraz środków logicznych (kontrola uprawnień w systemach informatycznych i dostępu do systemów informatycznych);
   d) ogranicza czas przetwarzania danych osobowych — Administrator Danych Osobowych nie może przetwarzać danych osobowych dłużej niż to wynika z założonego celu.
3. Wykaz okresów przetwarzania danych osobowych stanowi Załącznik nr 22.
4. Procedura usuwania i niszczenia danych osobowych stanowi Załącznik nr 23.

§ 21.

Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych

1. Administrator Danych Osobowych jest zobowiązany kontrolować, czy przekazuje jakiekolwiek dane osobowe do państw trzecich lub organizacji międzynarodowych, w szczególności w przypadku korzystania z usług innych podmiotów.

2. Administrator Danych Osobowych jest zobowiązany zidentyfikować i zweryfikować podstawę prawną przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych.
3. Wykaz podstaw prawnych przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych stanowi Załącznik nr 24.
4. Administrator Danych Osobowych jest zobowiązany monitorować zmiany legislacyjne i w miarę konieczności aktualizować wykaz, o którym mowa w ust. 3.
5. Przypadki przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych są odnotowywane w rejestrze czynności przetwarzania danych osobowych.

V. UPRAWNIENIA OSÓB FIZYCZNYCH

§ 22.
Obowiązki informacyjne

1. Administrator Danych Osobowych jest zobowiązany realizować obowiązki informacyjne, o których mowa w art. 13 RODO i art. 14 RODO.
2. Administrator Danych Osobowych spełnia obowiązek informacyjny:
   a) w przypadku pozyskania danych bezpośrednio od podmiotu danych — w chwili pozyskiwania tych danych;
   b) w przypadku pozyskiwania danych osobowych nie od podmiotu danych:
      — w rozsądnym terminie po pozyskaniu danych, jednak nie później niż w terminie miesiąca;
      — najpóźniej przy pierwszej komunikacji z podmiotem danych, jeżeli dane osobowe mają być wykorzystywane do komunikacji;
      — przy pierwszym ujawnieniu, jeżeli dane osobowe mają być ujawnione innemu odbiorcy.
3. Administrator Danych Osobowych nie jest zobowiązany zrealizować obowiązku informacyjnego w przypadku pozyskiwania danych od podmiotu danych, gdy podmiot danych już posiada te informacje.
4. Administrator Danych Osobowych nie jest zobowiązany zrealizować obowiązku informacyjnego w przypadku pozyskiwania danych nie od podmiotu danych, gdy:
   a) podmiot danych dysponuje już tymi informacjami;
   b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1 RODO, lub o ile wykonanie obowiązku informacyjnego może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach Administrator Danych Osobowych podejmuje odpowiednie środki, by chronić prawa i wolności oraz

prawnie uzasadnione interesy podmiotu danych, w tym udostępnia informacje publicznie;
   c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii Europejskiej lub prawem polskim; lub
   d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii Europejskiej lub w prawie polskim, w tym ustawowym obowiązkiem zachowania tajemnicy.
5. Administrator Danych Osobowych informuje podmiot danych o planowanej zmianie celu przetwarzania danych osobowych.
6. Administrator Danych Osobowych informuje podmiot danych o planowanym uchyleniu ograniczenia przetwarzania danych osobowych.
7. Administrator Danych Osobowych udziela informacji w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
8. Administrator Danych Osobowych jest zobowiązany opracować zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
9. Wykaz stosowanych klauzul informacyjnych, stosowane polityki prywatności oraz wzory oświadczeń o zapoznaniu się z informacjami stanowią Załączniki nr 25a-e.

§ 23.

Rodzaje uprawnień osób fizycznych

1. Oprócz prawa do informacji, o których mowa w § 22, każdemu podmiotowi danych przysługuje prawo do:
   a) dostępu do danych osobowych i informacji o nich;
   b) uzyskania kopii jego danych osobowych;
   c) sprostowania danych osobowych i uzupełnienia niekompletnych danych osobowych;
   d) usunięcia danych osobowych (prawo do bycia zapomnianym);
   e) ograniczenia przetwarzania danych osobowych;
   f) uzyskania informacji o odbiorcach danych osobowych w przypadku sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych;
   g) uzyskania danych osobowych w określonym formacie i przesłania ich innemu administratorowi danych osobowych;
   h) żądania przesłania danych osobowych innemu administratorowi danych osobowych przez Administratora Danych Osobowych;
   i) wyrażenia sprzeciwu wobec przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. e RODO i art. 6 ust. 1 lit. f RODO, w tym profilowania;
   j) wyrażenia sprzeciwu wobec marketingu bezpośredniego, w tym profilowania;
   k) niepodlegania decyzji, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu.
2. Szczegółowy opis uprawnień osób fizycznych stanowi Załącznik nr 26.

§ 24.

Realizacja uprawnień osób fizycznych

1. Administrator Danych Osobowych jest zobowiązany ułatwiać podmiotom danych realizację ich uprawnień, o których mowa w § 23.
2. Administrator Danych Osobowych jest zobowiązany prowadzić komunikację z podmiotem danych w sprawie realizacji uprawnień związanych z przetwarzaniem danych osobowych.
3. Procedura realizacji uprawnień osób fizycznych stanowi Załącznik nr 27.
4. Administrator Danych Osobowych prowadzi rejestr informacji o wykonywaniu praw.
5. Wzór rejestru informacji o wykonywaniu praw stanowi Załącznik nr 28.

§ 25.

Pobieranie opłat za wykonywanie uprawnień

1. Udzielanie informacji, prowadzenie komunikacji oraz realizacja uprawnień związanych z przetwarzaniem danych osobowych co do zasady jest bezpłatne.
2. W przypadku, gdy żądania podmiotu danych są nieuzasadnione lub nadmierne, Administrator Danych Osobowych:
   a) za prowadzenie komunikacji lub podjęcie żądanych działań może pobrać rozsądną opłatę, wynikającą z kosztów administracyjnych, albo
   b) odmówić podjęcia działań w związku z żądaniem.
3. Pierwsza kopia danych osobowych przekazywana podmiotowi danych jest bezpłatna. Za wszelkie kolejne kopie Administrator Danych Osobowych może żądać rozsądnej opłaty, wynikającej z kosztów administracyjnych.

VI. BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH

§ 26.

Obowiązek zapewnienia bezpieczeństwa przetwarzania danych osobowych

1. Administrator Danych Osobowych wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych osobowych.
2. Dobór odpowiednich środków technicznych i organizacyjnych następuje w ramach procedury zarządzania ryzykiem oraz ewentualnie w oparciu o ocenę skutków dla ochrony danych osobowych.
3. Dobór odpowiednich środków technicznych i organizacyjnych następuje z uwzględnieniem:
   a) stanu wiedzy technicznej;
   b) kosztów wdrażania;
   c) charakteru, zakresu, kontekstu i celów przetwarzania;
   d) ryzyka naruszenia praw i wolności osób fizycznych.

4. Opis stosowanych środków technicznych i organizacyjnych stanowi Załącznik nr 29.
5. Zasady ochrony pomieszczeń stanowią Załącznik nr 30.
6. Schemat obiegu dokumentów stanowi Załącznik nr 31.
7. Dokumenty, o których mowa w ust. 4-6, nie są udostępniane ogółowi osób upoważnionych. Administrator Danych Osobowych określa, jakie osoby mogą uzyskać wgląd w treść opisów, o którym mowa w ust. 4-6.

§ 27.

Systemy informatyczne

1. Administrator Danych Osobowych — jeżeli zajdzie taka potrzeba — może wyznaczyć Administratora Systemów Informatycznych. Jeżeli takiej osoby nie wyznacza, Administrator Danych Osobowych samodzielnie zarządza systemami informatycznymi.
2. Wzór uchwały zarządu o wyznaczeniu Administratora Systemów Informatycznych / dokumentu wyznaczającego Administratora Systemów Informatycznych stanowi Załącznik nr 32.
3. Zasady związane z obsługą systemów informatycznych oraz ich zabezpieczeniem określa Instrukcja zarządzania systemami informatycznymi wraz z załącznikami.
4. Instrukcja zarządzania systemami informatycznymi stanowi Załącznik nr 33.
5. Instrukcja, o której mowa w ust. 3, nie jest udostępniana ogółowi osób upoważnionych. Administrator Danych Osobowych określa, jakie osoby mogą uzyskać wgląd w treść Instrukcji, o której mowa w ust. 3.

§ 28.

Zasady bezpieczeństwa i ich przestrzeganie

1. Administrator Danych Osobowych ustala i zapewnia przestrzeganie zasad bezpieczeństwa przez zatrudnionych.
2. Zasady bezpieczeństwa obowiązują wszystkie osoby przez niego zatrudnione, w tym praktykantów, stażystów i wolontariuszy, niezależnie od tego, czy biorą udział w przetwarzaniu danych osobowych i czy są upoważnione do przetwarzania danych osobowych.
3. Regulamin bezpieczeństwa dla zatrudnionych stanowi Załącznik nr 34.

§ 29.

Wykrywanie i klasyfikowanie naruszeń ochrony danych osobowych

1. Administrator Danych Osobowych jest zobowiązany wdrożyć środki umożliwiające jak najszybsze wykrywanie i klasyfikowanie naruszeń ochrony danych osobowych oraz reagowanie na dostrzeżone incydenty.
2. Procedura postępowania w przypadku naruszeń ochrony danych osobowych stanowi Załącznik nr 35.
3. Po stwierdzeniu naruszenia ochrony danych osobowych Administrator Danych Osobowych podejmuje wszelkie działania mające na celu zminimalizowanie skutków

naruszenia, ustalenie przyczyn i okoliczności naruszenia, jak również wprowadza środki techniczne lub organizacyjne, mające zapobiegać występowaniu podobnych naruszeń w przyszłości.

4. Administrator Danych Osobowych dokumentuje wszystkie przypadki naruszeń w rejestrze naruszeń ochrony danych osobowych.
5. Wzór rejestru naruszeń ochrony danych osobowych stanowi Załącznik nr 36.

§ 30.

Zawiadamianie o naruszeniu ochrony danych osobowych

1. W przypadku naruszenia ochrony danych osobowych Administrator Danych Osobowych zawiadamia o tym incydencie:
   a) Prezesa Urzędu Ochrony Danych Osobowych oraz
   b) podmioty danych osobowych, których dane dotyczą,

   chyba że zachodzi okoliczność wyłączająca obowiązek zawiadomienia.
2. Procedura zawiadamiania o naruszeniu ochrony danych osobowych stanowi Załącznik nr 37.

VII. KONTROLA I DOSKONALENIE SYSTEMU OCHRONY DANYCH OSOBOWYCH

§ 31.

Audyt wewnętrzny

1. Przynajmniej raz na 2 lata Administrator Danych Osobowych / Inspektor Ochrony Danych / przeprowadza kompleksowy audyt wewnętrzny w zakresie przestrzegania ochrony danych osobowych.
2. Audyt wewnętrzny może być dzielony na mniejsze zadania audytowe.
3. W przypadku poważnego naruszenia ochrony danych osobowych audyt wewnętrzny jest przeprowadzany niezwłocznie po usunięciu skutków naruszenia.

§ 32.

Kontrola przetwarzania danych osobowych

1. Przynajmniej raz na rok Administrator Danych Osobowych / Inspektor Ochrony Danych / dokonuje przeglądu:
   a) ilości przetwarzanych danych osobowych;
   b) procesów przetwarzania danych osobowych;
   c) upoważnień do przetwarzania danych osobowych;
   d) użytkowników w systemach informatycznych.
2. W zakresie wynikającym z przeglądu, o którym mowa w ust. 1, dokonuje się niezbędnych usunięć i aktualizacji, aby zapewnić zgodność z niniejszą Polityką.

§ 33.

Przegląd Polityki i załączników

1. Przynajmniej raz na rok Administrator Danych Osobowych / Inspektor Ochrony Danych / dokonuje przeglądu niniejszej Polityki oraz załączników.
2. Niniejsza Polityka wraz z załącznikami jest aktualizowana, rozwijana i modyfikowana:
   a) na potrzeby dostosowania do zmiany stanu prawnego;
   b) na potrzeby zwiększenia jej skuteczności;
   c) w związku z potrzebami Administratora Danych Osobowych.

§ 34.

Szkolenia

1. Administrator Danych Osobowych jest zobowiązany podejmować działania na rzecz zwiększenia świadomości z zakresu ochrony danych osobowych wśród osób przez siebie zatrudnionych oraz podnoszenia ich wiedzy i kwalifikacji w tym zakresie.
2. Administrator Danych Osobowych zapewnia osobom przez siebie zatrudnionym szkolenia z zakresu ochrony danych osobowych, których częstotliwość oraz stopień zaawansowania zależy od pozycji zatrudnionego w systemie ochrony danych osobowych.

VIII. WYKAZ ZAŁĄCZNIKÓW

§ 35.

Wykaz załączników

1. Poniższe Załączniki stanowią integralną część niniejszej Polityki:
   — Załącznik nr 1: wzór umowy o współadministrowanie danymi osobowymi;
   — Załącznik nr 2: procedura nadawania, zmiany i odbierania upoważnień do przetwarzania danych osobowych
   — Załącznik nr 3: wzór oświadczenia o zapoznaniu się z dokumentami z zakresu ochrony danych osobowych, oświadczenia o odbyciu szkolenia z zakresu ochrony danych osobowych, oświadczenia o przestrzeganiu ochrony danych osobowych oraz ustalonych procedur;
   — Załącznik nr 4: wzór ewidencji osób upoważnionych do przetwarzania danych osobowych;
   — Załącznik nr 5: wzór umowy o powierzenie przetwarzania danych osobowych;
   — Załącznik nr 6: wzór ewidencji podmiotów przetwarzających;
   — Załącznik nr 7: wzór rejestru wszystkich kategorii czynności przetwarzania;
   — Załącznik nr 8: wzór ewidencji odbiorców danych osobowych;
   — Załącznik nr 9: wzór rejestru żądań udostępnień danych osobowych;
   — Załącznik nr 10: procedura zarządzania ryzykiem;
   — Załącznik nr 11: procedura przeprowadzania oceny skutków dla ochrony danych osobowych;

— Załącznik nr 12: procedura przeprowadzania uprzednich konsultacji z Prezesem Urzędu Ochrony Danych Osobowych;
— Załącznik nr 13: procedura privacy by design i privacy by default;
— Załącznik nr 14: wzór ewidencji zbiorów danych osobowych;
— Załącznik nr 15: wzór ewidencji pomieszczeń;
— Załącznik nr 16: wzór ewidencji stacji roboczych, urządzeń przenośnych i nośników;
— Załącznik nr 17: wzór ewidencji programów komputerowych (aplikacji);
— Załącznik nr 18: wzór rejestru czynności przetwarzania danych osobowych;
— Załącznik nr 19: wykaz podstaw prawnych przetwarzania danych osobowych;
— Załącznik nr 20: wykaz stosowanych klauzul zgód;
— Załącznik nr 21: procedura określająca zasady profilowania i zautomatyzowanego podejmowania decyzji;
— Załącznik nr 22: wykaz okresów przetwarzania danych osobowych;
— Załącznik nr 23: procedura usuwania i niszczenia danych osobowych;
— Załącznik nr 24: wykaz podstaw prawnych przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych;
— Załączniki nr 25a-25e: wykaz stosowanych klauzul informacyjnych, polityki prywatności, oświadczenia o zapoznaniu się z informacjami;
— Załącznik nr 26: szczegółowy opis uprawnień osób fizycznych;
— Załącznik nr 27: procedura realizacji uprawnień osób fizycznych;
— Załącznik nr 28: wzór rejestru informacji o wykonywaniu praw;
— Załącznik nr 29: opis stosowanych środków technicznych i organizacyjnych;
— Załącznik nr 30: zasady ochrony pomieszczeń;
— Załącznik nr 31: schemat obiegu dokumentów;
— Załącznik nr 32: wzór uchwały zarządu o wyznaczeniu Administratora Systemów Informatycznych / dokumentu wyznaczającego Administratora Systemów Informatycznych
— Załącznik nr 33: instrukcja zarządzania systemami informatycznymi;
— Załącznik nr 34: regulamin bezpieczeństwa dla zatrudnionych;
— Załącznik nr 35: procedura postępowania w przypadku naruszeń ochrony danych osobowych;
— Załącznik nr 36: wzór rejestru naruszeń ochrony danych osobowych;
— Załącznik nr 37: procedura zawiadamiania o naruszeniu ochrony danych osobowych;

2. W przypadku ewidencji i rejestrów Administrator Danych Osobowych może zastąpić wzory, które stanowią Załączniki do niniejszej Polityki, dedykowanym oprogramowaniem służącym do tych samych celów.

IX. POSTANOWIENIA KOŃCOWE

§ 36.

Postanowienia końcowe

1. W zakresie nieuregulowanym niniejszą Polityką znajdują zastosowanie powszechnie obowiązujące przepisy prawa, w szczególności dotyczące ochrony danych osobowych.
2. W przypadku zmiany stanu prawnego, która będzie skutkować niezgodnością niniejszej Polityki z prawem, postanowienie takie traci moc. Administrator Danych Osobowych podejmuje niezwłoczne działania na rzecz dostosowania niniejszej Polityki do nowego stanu prawnego.
3. Niniejsza Polityka może być zmieniona lub uchylona w takim samym trybie, w jakim została przyjęta.
4. Niniejsza Polityka obowiązuje od dnia 25.05.2018 r.