Polityka ochrony danych
w Pearson & CO Sp. Z o. o.

Rozdział I
Postanowienia ogólne

§1

1. Polityka ochrony danych (zwana dalej „Polityką") określa zasady dotyczące przetwarzania i zabezpieczenia danych osobowych w Pearson & CO Sp. Z o. o. (zwanej dalej Firmą) zgodnie z wymaganiami 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 – zwanego dalej RODO).
2. Niniejszy dokument stanowi wykonanie obowiązku, o którym mowa w art. 24 ust. 2 RODO.
3. Polityka ma zastosowanie do wszystkich danych osobowych przetwarzanych w Firmie w ramach procesów przetwarzania danych osobowych.
4. Obowiązek ochrony danych osobowych przetwarzanych w Firmie dotyczy wszystkich osób, które mają do nich dostęp bez względu na zajmowane stanowisko oraz miejsce wykonywania pracy, jak również charakter stosunku pracy.
5. Każda osoba, która ma mieć dostęp do danych osobowych, będzie mogła je przetwarzać wyłącznie na podstawie otrzymania upoważnienia.
6. Osoby mające dostęp do danych osobowych są zobowiązane do zapoznania się z Polityką i innymi powiązanymi z nią dokumentami oraz stosowanie zawartych w nich regulacji.
7. Polityka zachowuje zgodność z innymi wewnętrznymi regulacjami z obszaru bezpieczeństwa informacji i systemów informatycznych obowiązującymi w Firmie.
8. Nadzór nad opracowaniem i aktualizacją Polityki sprawuje wyznaczony pracownik Firmy.

§2

Występujące w niniejszej Polityce zwroty oznaczają:
Administrator Danych Osobowych (ADO) – Pearson & Co Sp. Z o. o.
Dane osobowe – wszelkie informacje, dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby 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.
Dane osobowe wrażliwe – szczególne kategorie danych określone w art. 9 RODO, w tym: dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków

zawodowych, dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby, jak również dane osobowe dotyczące wyroków skazujących oraz naruszeń prawa, o których mowa w art. 10 RODO.
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.
Obszar przetwarzania danych osobowych – pomieszczenia lub części pomieszczeń we wszystkich lokalizacjach Firmie, w których są przetwarzane dane osobowe, zarówno w formie papierowej, jak i w systemie informatycznym.
Odbiorca danych – podmiot, któremu udostępniane są dane osobowe.
Osoba upoważniona – osoba upoważniona do przetwarzania danych osobowych przez Administratora danych lub osobę przez niego upoważnioną, mająca bezpośredni dostęp do danych, przetwarzanych w systemie informatycznym lub w dokumentacji papierowej.
Podmiot przetwarzający – podmiot, któremu Firma powierza czynności przetwarzanie danych osobowych w swoim imieniu.
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.
Przetwarzanie danych osobowych – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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.
PUODO – Prezes Urzędu Ochrony Danych Osobowych.
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 (ogólne rozporządzenie o ochronie danych).
UODO – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000).
Zasób danych osobowych – wszystkie dane osobowe, niezależnie od sposobu ich utrwalenia, zarówno w formie elektronicznej – w systemie informatycznym oraz na nośnikach (płyty CD/DVD/BD, pamięci flash i inne), jak i papierowej przetwarzane przez Firmę w celu realizacji jej zadań.

Rozdział II
Zarządzanie przetwarzaniem danych osobowych oraz ich bezpieczeństwem

§ 3

1. Pearson & CO Sp. Z o. o. jest odpowiedzialna za przetwarzanie i ochronę danych osobowych w Firmie, zgodnie przepisami prawa, w tym za zaakceptowanie niniejszej Polityki.
2. Pearson & CO Sp. Z o. o. wyznacza osobę odpowiedzialną za ochronę danych osobowych w Firmie, która wykonuje zadania w zakresie monitorowania zasad przetwarzania danych osobowych w Firmie.
3. Pearson & CO Sp. Z o. o. może wyznaczyć inne osoby, które wspomagają wykonywanie zadań monitorowania ochrony danych w Firmie.

§ 4

4. Pearson & CO Sp. Z o. o. jest odpowiedzialna za zarządzanie procesami przetwarzania danych osobowych w Firmie. Do obowiązków osoby zarządzającej Firmie należy:
a) zarządzanie czynnościami przetwarzania danych osobowych w ramach zadań, realizowanych przez Firmę;
b) występowanie z wnioskami do Pearson & CO Sp. Z o. o. o nadanie, zmianę lub cofnięcie uprawnień pracownikom do określonych zasobów danych osobowych przetwarzanych w systemie informatycznym, zgodnie z zakresem upoważnienia do przetwarzania danych osobowych;
c) zapoznanie podległych pracowników i innych osób (np. współpracowników) z zasadami przetwarzania i ochrony danych w Firmie;
d) wypełnianie obowiązków dotyczących zabezpieczenia obszaru przetwarzanych danych osobowych w Firmie;
e) zgłaszanie do osoby odpowiedzialnej za ochronę danych osobowych w Firmie zamiaru rozpoczęcia nowego procesu przetwarzania danych osobowych lub zmiany w czynnościach przetwarzania danych realizowanych w Firmie;
f) w przypadku zbierania danych osobowych, konsultowanie w Firmie i podstaw prawnych przetwarzania danych osobowych, w tym zbierania i archiwizowanie zgód osób na przetwarzanie ich danych osobowych wymaganych przypadkach;
g) ustalanie w porozumieniu z informatykiem, z którego usług korzysta Firma, zasad tworzenia kopii zapasowych plików z danymi osobowymi, znajdującymi się na stacjach roboczych użytkowników w Firmie;
h) realizacja procesu udostępniania danych osobowych innemu podmiotowi lub osobie, której dane dotyczą;
i) realizacja procesów związanych z powierzaniem przetwarzania danych osobowych przez Firmę innym podmiotom - zgodnie z zawartymi umowami powierzenia przetwarzania danych osobowych.

§ 5

1. Pearson & CO Sp. Z o. o. jest odpowiedzialna za:
a) przygotowanie upoważnienia do przetwarzania danych osobowych wraz z umową o pracę/zlecenia/dzieło;
b) przechowywanie nadanych upoważnień do przetwarzania danych osobowych oraz oświadczeń o zachowaniu tajemnicy danych osobowych i sposobów ich zabezpieczania wraz z aktami osobowymi pracowników lub umowami zlecenia.
c) prowadzenie aktualnej ewidencji osób upoważnionych do przetwarzania danych osobowych.
2. Pearson & CO Sp. Z o. o. jest odpowiedzialna za zarządzanie systemem informatycznym służącym do przetwarzania danych osobowych w Firmie.
3. Pearson & CO Sp. Z o. o. ściśle współpracuje z osobą odpowiedzialną za ochronę danych osobowych w Firmie w zakresie zapewnienia bezpieczeństwa systemów informatycznych przetwarzających dane osobowe.

Rozdział III
Upoważnianie osób do przetwarzania danych osobowych

§ 7

1. Wszystkie osoby, które wykonują czynności związane z przetwarzaniem danych osobowych w Firmie, w ramach wykonywania zadań służbowych na stanowiskach pracy lub prac zleconych, muszą posiadać pisemne upoważnienie do przetwarzania danych osobowych oraz podpisać oświadczenie o zachowaniu tajemnicy danych oraz sposobów ich zabezpieczenia.
2. Upoważnienia do przetwarzania danych osobowych nadaje Pearson & CO Sp. Z o. o.
3. Upoważnienia do przetwarzania danych są przygotowywane i przechowywane przez Pearson & CO Sp. Z o. o.
4. Każda osoba upoważniona do przetwarzania danych osobowych przechodzi szkolenie z zasad ochrony danych w Firmie.
5. Szkolenia wstępne i okresowe dla osób upoważnionych przeprowadzi osoba odpowiedzialna za ochronę danych osobowych w Firmie wg ustalonego planu.

Rozdział IV
Podstawowe zasady, które powinny przestrzegać osoby upoważnione do przetwarzania danych osobowych

§8

1. Osoba upoważniona do przetwarzania danych osobowych w Firmie jest zobowiązana do:
a) zapoznania się z obowiązującymi przepisami prawa z zakresu ochrony danych osobowych oraz dokumentacją dotyczącą ochrony danych osobowych w Firmie;
b) przechodzenia okresowych szkoleń z obszaru ochrony danych osobowych;
c) przetwarzania danych osobowych wyłącznie w celu i zakresie wynikającym z nałożonych obowiązków służbowych;
d) zachowania wyjątkowej staranności przy przetwarzaniu danych osobowych, w szczególności danych wrażliwych w celu ochrony interesów osób, których dane dotyczą;
e) stosowania określonych w Firmie procedur i środków przetwarzania oraz zabezpieczania danych osobowych;
f) podporządkowania się poleceniom osoby odpowiedzialnej za ochronę danych osobowych w Firmi;
g) zachowania w poufności danych osobowych oraz danych objętych tajemnicą przedsiębiorstwa;
h) zabezpieczenia danych osobowych przed: ich utratą, uszkodzeniem lub zniszczeniem, zmianą lub ich udostępnieniem osobom nieupoważnionym;
i) dopilnowania, aby przebywanie osób nieupoważnionych w pomieszczeniach, w których przetwarzane są dane osobowe, miało miejsce wyłącznie w obecności osoby upoważnionej;
j) dopilnowania, aby przeznaczone do usunięcia dokumenty, zawierające dane osobowe niszczone były w stopniu uniemożliwiającym ich odczytanie - zabronione jest wyrzucanie dokumentów do koszy na śmieci bez ich właściwej anonimizacji;
k) przestrzegania procedur właściwego użytkowania systemów informatycznych, w których przetwarza się dane osobowe, w tym do nieujawniania innym użytkownikom swoich loginów i haseł;
l) zachowania należytej staranności podczas przekazywania danych osobowych drogą telefoniczną (konieczność właściwej identyfikacji rozmówcy, konieczność ustalenia, czy rozmówca jest uprawniony do pozyskania danych osobowych, przekazywanie jedynie niezbędnych informacji);
m) przesyłania danych osobowych za pomocą sieci Internet jedyne z użyciem metod kryptograficznych (szyfrowanie danych, kanały bezpiecznej transmisji);
n) niewysyłania za pomocą wiadomości e-mail danych osobowych na prywatne adresy, niekopiowanie danych na inne nośniki bez uzasadnionej potrzeby biznesowej;
o) zachowania należytej ostrożności przy transporcie dokumentów oraz nośników informatycznych, zawierających dane osobowe, poza obszarem przetwarzania w Firmie.
p) niepozostawiania dokumentów, zawierających dane osobowe na urządzeniach wielofunkcyjnych (drukowanie, kopiowanie);
q) nieopuszczania stanowiska bez zabezpieczenia dokumentów papierowych, zawierających dane osobowe (zasada „czystego biurka”) oraz bez zabezpieczania

dostępu do danych przetwarzanych w systemie informatycznym (zasada „czystego ekranu”);
r) informowania o zdarzeniu operacyjnym dotyczącym danych osobowych, zgodnie z obowiązującymi w tym zakresie procedurami;
s) zaprzestania przetwarzania danych osobowych po ustaniu stosunku zatrudnienia.

Rozdział V
Prowadzenie rejestrów czynności przetwarzania danych osobowych

§ 9

1. Firma prowadzi rejestr czynności przetwarzania danych osobowych zgodnie z wymaganiami art. 30 ust. 1 RODO w stosunku do danych których Firma jest administratorem;
2. Wzór rejestru czynności jest określony w Załączniku nr 2 do niniejszej Polityki.
3. Za prowadzenie rejestrów czynności odpowiedzialna jest osoba odpowiedzialna za ochronę danych osobowych w Firmie.
4. Osoba odpowiedzialna za ochronę danych osobowych w Firmie inwentaryzuje procesy przetwarzania danych osobowych w Firmie, przypisując do nich określone czynności przetwarzania danych.
5. Osoba odpowiedzialna za ochronę danych osobowych w Firmie okresowo dokonuje przeglądów procesów przetwarzania danych w celach aktualizacji prowadzonych rejestrów.
6. Firma ma obowiązek na bieżąco informować osobę odpowiedzialną za ochronę danych osobowych Firmie o procesach przetwarzania danych osobowych realizowanych w Firmie oraz o wszelkich zmianach w tych procesach, w szczególności dotyczących:
a. celów przetwarzania danych, w tym realizowanych czynności;
b. kategorii osób, których dane są przetwarzane;
c. zakresów przetwarzanych danych;
d. podmiotów przetwarzających, którym dane są powierzane;
e. odbiorców danych, którym dane są udostępniane.

Rozdział VI
Realizacja obowiązków przy przetwarzaniu danych osobowych

§ 10

1. Osoby odpowiedzialne w Firmie za procesy, w których zbierane są dane osobowe, mają obowiązek zachowania szczególnej staranności przy ich zbieraniu, w tym:

a. sprawdzać czy są spełnione podstawy prawne na pozyskiwanie danych osobowych, zgodnie z art. 6 RODO oraz art. 9 – 10 RODO;
b. zbierać dane osobowe dla określonych, zgodnych z prawem celów realizowanych w Firmie;
c. zbierać dane w zakresie adekwatnym do celów w jakich dane będą przetwarzane w Firmie.
2. W przypadku konieczności odbierania zgody na przetwarzanie danych osobowych, należy zapewnić dobrowolność jej pozyskania oraz powiadamiać o prawie do odwołania takiej zgody.
3. Za stosowanie właściwych oświadczeń zgody przy zbieraniu danych osobowych odpowiada Firma.
4. Oświadczenia dotyczące odbierania zgody na przetwarzanie danych osobowych muszą być konsultowane z prawnikiem odpowiedzialnym za ochronę danych osobowych w Firmie.
5. Prawnik odpowiedzialny za ochronę danych osobowych w Firmie może ustalić obowiązujące wzory oświadczeń zgody dla poszczególnych procesów przetwarzania danych realizowanych w Firmie.

§ 11

1. Osoby, które wykonują zadania związane ze zbieraniem danych osobowych są odpowiedzialne za realizację obowiązków informacyjnych określonych w art. 13 i 14 RODO.
2. Za stosowanie właściwych klauzuli informacyjnych przy zbieraniu danych osobowych odpowiada Firma.
3. Klauzule informacyjne muszą być konsultowane z prawnikiem odpowiedzialnym za ochronę danych osobowych w Firmie.
4. Prawnik odpowiedzialny za ochronę danych osobowych w Firmie może ustalić obowiązujące wzory klauzul informacyjnych dla poszczególnych procesów przetwarzania danych realizowanych w Firmie.

§ 12

1. Dane osobowe zbierane w ramach procesów realizowanych w Firmie są przetwarzane przez czas określony przez właściwe przepisy prawa lub wewnętrzne przepisy Firmy.
2. Za określenie odpowiednich czasów retencji danych osobowych w procesach przetwarzania danych w Firmie odpowiada prawnik odpowiedzialny za ochronę danych osobowych w Firmie.
3. Dane osobowe, dla których okres przetwarzania nie wynika z obowiązujących przepisów prawa i dla których nie jest możliwe określenie z góry tego okresu w wewnętrznych przepisach Firmy, są przetwarzane tak długo, jak długo istnieje jednocześnie podstawa prawna oraz cel dla ich przetwarzania.
4. Ustanie celu przetwarzania danych jest równoznaczne z koniecznością usunięcia danych osobowych.

5. Dane osobowe przetwarzane wyłącznie w oparciu o przesłankę zgody na przetwarzanie danych osobowych są usuwane zawsze niezwłocznie po wycofaniu takiej zgody.
6. W Firmie, co najmniej jeden raz w każdym roku kalendarzowym odbywa się weryfikacja zasobów danych osobowych prowadzonych w formie papierowej jak i elektronicznej, obejmująca:
a. sprawdzenie, czy dane osobowe, dla których upłyną okres przechowywania wynikający z przepisów prawa lub wewnętrznych przepisów Firmy zostały usunięte;
b. sprawdzenie, czy w odniesieniu do danych osobowych, których czas przechowywania nie został określony przez właściwe przepisy prawa lub wewnętrzne przepisy Firmy, nadal istnieje podstawa prawna oraz cel przetwarzania danych osobowych.
7. W przypadku ustalenia w trakcie weryfikacji, o której mowa w ust. 6, że okres przetwarzania danych osobowych upłynął bądź nie istnieje podstawa prawna lub cel do dalszego przetwarzania danych osobowych, dane osobowe powinny zostać trwale usunięte z nośników papierowych, elektronicznych oraz systemów informatycznych.
8. Szczegółowe zasady usuwania lub anonimizacji danych w systemach informatycznych są ustalane i realizowane przez informatyka, z którego usług korzysta Firma.

§ 13

1. Osoby, które udostępniają w imieniu Firmy dane osobowe do podmiotu zewnętrznego (w formie papierowej lub elektronicznej), przed ich udostępnieniem mają obowiązek sprawdzić czy istnieją podstawy prawne umożliwiające wykonanie tych czynność, w tym:
a. wymóg prawa dotyczący udostępnienia danych;
b. zgoda osoby na udostępnienie danych innemu podmiotowi;
c. zapis w umowie z podmiotem współpracującym, przy spełnieniu warunku, że udostępnienie nie narusza praw i wolności osoby, której dane dotyczą;
d. wniosek o udostępnienie danych od podmiotu uprawnionego, ze wskazaniem podstawy prawnej do otrzymywania danego rodzaju danych osobowych.
2. Każda sytuacja dotycząca udostępnienia danych osobowych musi być konsultowana z prawnikiem odpowiedzialnym za ochronę danych osobowych w Firmie.

§ 14

1. W sytuacji powierzania czynności przetwarzania danych osobowych zewnętrznemu podmiotowi (podmiotowi przetwarzającemu), należy zawrzeć z nim umowę powierzenia przetwarzania danych osobowych zgodnie z art. 28 ust. 3 RODO.
2. W trakcie dokonywania wyboru podmiotu przetwarzającego należy zweryfikować czy podmiot ten zapewnia wystarczające gwarancje wdrożenia odpowiednich

środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi przepisów RODO i chroniło prawa osób, których dane dotyczą.
3. Osoby, które przygotowują w imieniu Firmie umowę z podmiotem zewnętrznym, któremu zlecone zostanie wykonywanie czynności związanych z przetwarzaniem danych osobowych zobowiązane są skonsultować odpowiednie zapisy dotyczące powierzenia przetwarzania danych z prawnikiem odpowiedzialnym za ochronę danych osobowych w Firmie.
4. Wzór umowy powierzenia znajduje się w Załączniku nr 3 do niniejszej Polityki.
5. Kontrola podmiotów przetwarzających, którym zostały powierzone czynności przetwarzania danych osobowych należących do Firmie jest przeprowadzana przez Inspektora lub inne wyznaczone osoby zgodnie z zapisami zawartymi w umowach powierzenia przetwarzania danych osobowych, w odniesieniu do uprawnienia określonego w art. 28 ust. 3 lit. h RODO.

§ 15

1. W sytuacji przekazywania danych osobowych do podmiotu znajdującego się w państwie trzecim (poza Europejskim Obszarem Gospodarczym) należy taką sytuację skonsultować z prawnikiem odpowiedzialnym za ochronę danych osobowych w Firmie.
2. Prawnik odpowiedzialny za ochronę danych osobowych w Firmie może ustalić wzory zapisów do umów w ramach, których dochodzi do transferu danych do państwa trzeciego lub organizacji międzynarodowej.

Rozdział VII
Realizacja praw osób, których dane dotyczą

§ 16

1. Każdej osobie, której dane osobowe są przetwarzane przez Firmie przysługują prawa określone w art. 15 – 22 RODO, w tym:
a. prawo dostępu do danych jej dotyczących;
b. prawo do sprostowania danych;
c. prawo do usunięcia danych;
d. prawo do ograniczenia przetwarzania;
e. prawo do przenoszenia danych;
f. prawo do sprzeciwu na przetwarzanie jej danych;
g. prawo do niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu.
2. Za rozpatrywanie złożonych do Firmy żądań w zakresie uprawnień, o których mowa w uat.1 odpowiada w Firmie.
3. W sytuacji powierzania danych podmiotom przetwarzającym lub udostępniania danych innym administratorom danych należy ich powiadamiać o każdym sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych, które było wynikiem realizacji wniosku otrzymanego od osoby, której dane dotyczą.

Rozdział VIII
Dobór środków technicznych i organizacyjnych dotyczących przetwarzania i zabezpieczania danych osobowych

§ 17

1. Dobór środków technicznych i organizacyjnych dotyczących przetwarzania i zabezpieczania danych osobowych w Firmie realizowany jest w oparciu o szacowanie ryzyka naruszenia praw i wolności osób, których dane dotyczą.
2. Przy doborze zabezpieczeń należy i oceniać ryzyko zarówno w kontekście skutków dla osoby, której dane dotyczą w tym np. dyskryminacja, pozbawienie przysługujących praw, szkody majątkowe i niemajątkowe), jak również ryzyko w kontekście skutków dla Firmie w przypadku niepodjęcia działań związanych z zapewnieniem przetwarzania danych osobowych zgodnie z RODO.
3. Ustalone wymagania dotyczące zabezpieczenia danych osobowych w odniesieniu do danego procesu przetwarzania danych osobowych są odnotowywane przez osobę odpowiedzialną za ochronę danych osobowych w Firmie w prowadzonym rejestrze czynności przetwarzania danych osobowych.

§ 18

1. Planowanie realizacji nowych procesów związanych z przetwarzaniem danych osobowych, w tym w szczególności nowych systemów informatycznych służących do przetwarzania danych osobowych, musi uwzględniać zasady ochrony danych w fazie projektowania („privacy by design”) oraz domyślnej ochrony danych („privacy by default”)
2. Za realizację w Firmie obowiązków, o których mowa w ust.1 odpowiada Firmie

§ 19

1. W przypadku realizacji procesów przetwarzania danych osobowych w Firmie, które ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, przed rozpoczęciem przetwarzania należy dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych zgodnie z art. 35 RODO.
2. Za realizację w Firmie obowiązków, o których mowa w ust. 1 odpowiada Firma.
3. Wykonanie oceny skutków dla danego procesu przetwarzania danych jest konsultowane z osobą odpowiedzialną za ochronę danych osobowych w Firmie, która stwierdza czy w danym przypadku takie działanie jest konieczne.
4. Osoba odpowiedzialna za ochronę danych osobowych w Firmie prowadzonym rejestrze czynności przetwarzania danych osobowych, wskazuje procesy dla których należy przeprowadzać ocenę skutków oraz odnotowuje jej przeprowadzenie.
5. Jeżeli dokonana ocena skutków dla ochrony danych wykaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby nie zostały zastosowane środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania należy

skonsultować się z PUODO.
6. W przypadku konieczności przeprowadzenia konsultacji z osobą odpowiedzialną za ochronę danych osobowych w Firmie przygotowuje odpowiedni wniosek o konsultacje zgodnie z art. 36 RODO i kontaktuje się w tej sprawie z organem.

Rozdział IX
Postępowanie w sytuacji naruszenia ochrony danych

§ 20

1. W sytuacji powzięcia informacji o naruszeniu lub podejrzeniu naruszenia ochrony danych osobowych należy postępować zgodnie z zasadami wynikającymi z art. 33 i 34 RODO.
2. Firma we współpracy z osobą odpowiedzialną za ochronę danych osobowych w Firmie przygotowuje wykaz sytuacji, które można uznać za naruszenie ochrony danych osobowych, z uwzględnieniem naruszenia prawa i wolności osób, których dane dotyczą.
3. Zgłoszenia naruszenia ochrony danych osobowych przez osobę, której dane dotyczą lub inną osobę inną osobę spoza Firmy są przyjmowane i rozpatrywane Firmę we współpracy z osobą odpowiedzialną za ochronę danych osobowych w Firmie.
4. Szacowanie ryzyka dotyczące sytuacji naruszenia ochrony danych jest przeprowadzane przez Firmę we współpracy z osobą odpowiedzialną za ochronę danych osobowych w Firmie.

§ 21

5. W sytuacji stwierdzenia wystąpienia naruszenia ochrony danych osobowych oraz prawdopodobieństwa zaistnienia ryzyka naruszenia praw lub wolności osób fizycznych, informacja o naruszeniu powinna zostać zgłoszona do PUODO.
6. Zgłoszenie naruszenia przygotowuje Firma we współpracy z osobą odpowiedzialną za ochronę danych osobowych w Firmie w terminie 72 godzin po stwierdzeniu naruszenia, zgodnie z wymaganiami art. 33 RODO.
7. Zgłoszenie przekazywane jest do PUODO w formie elektronicznej za pomocą systemu informatycznego zgodnie z trybem określonym przez organ.

§ 22

1. W sytuacji gdy stwierdzone naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, o naruszeniu należy zawiadomić wszystkie osoby, których dane dotyczą. Firma analizuje czy w odniesieniu do wymogów art. 34 ust. 3 RODO zawiadomienie osób, których dane dotyczą, będzie wymagane.
2. Zawiadomienie o naruszeniu Firma we współpracy z osobą odpowiedzialną za ochronę danych osobowych w Firmie po potwierdzeniu konieczności jego realizacji zgodnie z załącznikiem nr 5 do Polityki.

§ 23

1. Wszystkie stwierdzone naruszenia ochrony danych osobowych są dokumentowane przez osobę odpowiedzialną za ochronę danych osobowych w Firmie we współpracy z Firmą.
2. Wzór ewidencji naruszeń ochrony danych osobowych stanowi załącznik nr 4 do Polityki.

Rozdział X
Rozliczalność zgodności realizacji obowiązków RODO

§ 24

1. W celu weryfikacji zastosowanych w Firmie środków technicznych i organizacyjnych, zapewniających przetwarzanie danych osobowych zgodnie z RODO, wykonuję się ich monitorowanie.
2. Monitorowanie ochrony danych osobowych prowadzone jest:
a) na bieżąco przez osobę zarządzającą Firmą;
b) poprzez audyty okresowe i doraźne (w sytuacji wystąpienia incydentów naruszenia ochrony danych) wykonywane przez osobę odpowiedzialną za ochronę danych osobowych w Firmie;
c) podczas audytów wewnętrznych przeprowadzanych przez upoważnione podmioty.
3. Osoba odpowiedzialna za ochronę danych osobowych w Firmie okresowo analizuje zgodność dokumentacji przetwarzania danych osobowych przyjętej w Firmie i z przepisami o ochronie danych osobowych oraz nadzoruje jej aktualizację.

Rozdział XI
Odpowiedzialność karna za naruszenie zasad ochrony danych

§ 25

1. Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi, określonymi w art. 107 – 108 UODO oraz w art. 130, 266 - 269, 287 Kodeksu karnego.
2. Niezależnie od odpowiedzialności przewidzianej w przepisach, o których mowa w pkt 1, naruszenie zasad ochrony danych osobowych, obowiązujących Firmę, może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością na podstawie przepisów prawa pracy.

Rozdział XII
Postanowienia końcowe

§ 26

1. Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.

2. Firma jest obowiązany zapoznać z treścią Polityki swoich pracowników i współpracowników.

§ 27

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy RODO oraz UODO.
2. Pracownicy i współpracownicy Firmie zobowiązani są do bezwzględnego stosowania zasad określonych w Polityce.