zał. 3 do uchwały 14/11/2024

ZARZĄDZENIE nr .....
PREZESA ZARZĄDU ENSEMBLE3 SP.Z O.O
Z SIEDZIBĄ W WARSZAWIE
w przedmiocie wprowadzenia polityki bezpieczeństwa danych osobowych w Spółce
z dnia 21.10.2021 r.

§ 1.

1. 1.Wprowadzam jako obowiązującą, w ENSEMBLE^3 sp. z o.o, Politykę Bezpieczeństwa Danych Osobowych.
2. 2.Dokumentacja zawierająca Politykę Bezpieczeństwa Danych osobowych stanowi załącznik do niniejszego Zarządzenia.

§ 2.

Zarządzenie wchodzi w życie z dniem podpisania.

Prezes Zarządu

Dorota Anna Pawlak

Załącznik:

- Polityka Bezpieczeństwa Danych Osobowych w Ensemble3 spółka z ograniczoną odpowiedzialnością.

ZAŁĄCZNIK

do Zarządzenia Prezesa Zarządu Ensemble3

sp. z o.o. z dnia 21.10.2021 r.

Polityka Bezpieczeństwa Danych Osobowych

ENSEMBLE3

SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

1 Wstęp

1.1 Zarządzanie bezpieczeństwem informacji jest pojęciem obejmującym zasady zarządzania systemem chroniącym dane osobowe oraz sposoby reagowania na zagrożenia. Zapewnienie odpowiedniej wiedzy zarządzających jednostką oraz siecią informatyczną w zakresie pojawiających się nowych zagrożeń oraz metod ochrony jest kolejnym elementem zapewnienia bezpieczeństwa. Pracownicy obsługujący systemy przetwarzające dane osobowe są ogniwem zabezpieczeń, na którego skuteczność wpływa również zapewnienie rzetelnej informacji w zakresie sposobu bezpiecznego użytkowania oprogramowania i sprzętu.

1.2 Zastosowanie niniejszej PBDO powinno zapewnić zabezpieczenia adekwatne i proporcjonalne do kategorii danych, jednocześnie dopasowane do poziomu zagrożeń występujących dla przetwarzanych i przechowywanych danych osobowych w ENSEMBLE3 Spółka z ograniczoną odpowiedzialnością.

2 Cel

2.1 Niniejsza PBDO została sporządzona w celu zapewnienia właściwego przetwarzania i zabezpieczania danych osobowych zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych w ENSEMBLE3, w tym zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 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, oraz Ustawą.

2.2 PBDO jest jednocześnie dokumentem określającym zadania Kierowników KO i pracowników w zapewnieniu poufności, integralności, dostępności oraz rozliczalności przetwarzanych danych osobowych.

2.3 Przyjęta PBDO powinna być rozwijana w sposób ciągły i zmieniać się wraz ze zmianami w strukturze organizacyjnej, pojawianiem się nowych zagrożeń i rozwojem dostępnych środków zapobiegawczych. Rozwijający się proces informatyzacji ENSEMBLE3 wymaga, by stosowane zasady były sformalizowane oraz przyjęte jako obowiązujące reguły postępowania i sposoby zabezpieczeń danych osobowych. PBDO powinien być okresowo weryfikowany i dostosowywany do bieżących warunków prawnych, technologicznych i organizacyjnych zgodnie z zasadami przeglądu Systemu Zarządzania Bezpieczeństwem Informacji. W wyniku przeprowadzonych symulacji i treningów powinny być (jeśli to konieczne) zmodyfikowane odpowiednie fragmenty regulacji. Wprowadzane powinny być nowe elementy w przypadku pojawienia się niezdefiniowanych dotychczas zagrożeń lub zmiany wynikające z szacowania ryzyka w bezpieczeństwie informacji ENSEMBLE3.

2.4 Dla skutecznej realizacji niniejszej PBDO, ADO zapewnia:

2.4.1 odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,

2.4.2 szkolenia w zakresie przetwarzania danych osobowych i sposobu ich ochrony,

2.4.3 okresowe szacowanie ryzyka zagrożeń dla zbiorów danych,

2.4.4 analizę skutków dla ochrony danych osobowych,

2.4.5 kontrolę i nadzór nad przetwarzaniem danych osobowych,

2.4.6 monitorowanie zastosowanych środków ochrony.

3 Zakres stosowania

3.1 PBDO powinni stosować wszyscy pracownicy, którzy zostali zaangażowani w proces przetwarzania danych osobowych w ENSEMBLE3.

3.2 Dokument ma zastosowanie do wszystkich danych osobowych niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej i innej np. dane biometryczne).

3.3 Z dokumentem PBDO powinni zapoznać się:

3.3.1 Administrator Danych Osobowych.

3.3.2 Administratorzy Merytoryczni.

3.3.3 Kierownicy Komórek Organizacyjnych.

3.3.4 Inspektor Ochrony Danych.

3.3.5 Administratorzy Bezpieczeństwa Systemów Informatycznych .

3.3.6 Pracownicy przetwarzający dane osobowe.

3.4 Osoby przetwarzające dane osobowe w ENSEMBLE3 zapoznają się także z zasadami ochrony danych osobowych zawartych w innych dokumentach wewnętrznych.

3.5 Jeżeli przepisy szczególne, które odnoszą się do przetwarzania danych osobowych, przewidują dalej idącą ich ochronę niż to wynika z przepisów o ochronie danych osobowych, stosuje się przepisy tych aktów prawnych.

4 Terminologia

Użyte w niniejszej Polityce Bezpieczeństwa Danych Osobowych pojęcia i definicje oznaczają:

4.1 **ABSI** - Administratorzy Bezpieczeństwa Systemów Informatycznych.

4.2 **ADO - Administrator Danych Osobowych** – ENSEMBLE3 Spółka z ograniczoną odpowiedzialnością.

4.3 **AM** - Administrator Merytoryczny – Właściciel zasobu sieciowego, aplikacji lub zbioru danych osobowych.

4.4 **Dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Osobą możliwą do zidentyfikowania jest osoba fizyczna, której tożsamość 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.

4.5 **ENSEMBLE3** - ENSEMBLE3 Spółka z ograniczoną odpowiedzialnością.

4.6 **IOD** – Inspektor Ochrony Danych, osoba wyznaczona przez ADO zgodnie z art. 37 RODO, odpowiedzialna za monitorowanie przestrzegania zasad ochrony danych osobowych u ADO.

4.7 **Kierownik KO** – kierownik komórki organizacyjnej – Główny Księgowy, dyrektor działu lub biura, zastępca dyrektora działu lub biura, kierownik sekcji, samodzielne stanowisko podległe bezpośrednio Zarządowi ENSEMBLE3.

4.8 **KO** – dział, biuro, sekcja, zespół, samodzielne stanowisko pracy podległe bezpośrednio Zarządowi ENSEMBLE3.

4.9 **PBDO** – Polityka Bezpieczeństwa Danych Osobowych.

4.10 **Podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza lub będzie przetwarzał dane osobowe, po uzyskaniu rekomendacji IOD.

4.11 **Podmiot danych** – osoba, której dane dotyczą.

4.12 **Pracownik** - osoba pozostająca w stosunku pracy z ENSEMBLE3; postanowienia niniejszej Polityki dotyczące Pracownika stosuje się także do współpracownika tj. - osoby współpracującej z ENSEMBLE3 na podstawie umowy cywilnoprawnej.

4.13 **Przetwarzanie danych osobowych** – operacje wykonywane na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, np. 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.

4.14 **PUODO** - Prezes Urzędu Ochrony Danych Osobowych.

4.15 **RODO** – rozporządzenie Parlamentu Europejskiego 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).

4.16 **Zarząd ENSEMBLE3**- osoby uprawnione do reprezentacji ENSEMBLE3 lub osoby wyznaczone przez Zarząd ENSEMBLE3.

5 Organizacja ochrony danych osobowych

Obowiązki Inspektora Ochrony Danych

5.1 ADO wyznacza IOD. IOD realizuje obowiązki określone w RODO, w szczególności określone w art. 39 oraz powierzone mu z zachowaniem wymogów wynikających z art. 38 ust. 6 RODO.

Kryteria wyznaczenia IOD/Zastępcy

5.2 Funkcję IOD może pełnić osoba, która posiada wiedzę i praktykę w dziedzinie ochrony danych oraz wypełnienia zadania, o których mowa w RODO w szczególności w art. 39.

5.3 IOD podlega bezpośrednio Zarządowi ENSEMBLE3, który zapewnia mu zasoby niezbędne do wykonania zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby

niezbędne do utrzymania jego wiedzy fachowej.

Wyznaczenie IOD

5.4 ADO po wyznaczeniu IOD zawiadamia PUODO o jego wyznaczeniu, w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko, adres poczty elektronicznej lub numer telefonu inspektora.

5.5 ADO zawiadamia PUODO, o każdej zmianie danych, o których mowa w pkt 1 oraz o odwołaniu Inspektora, w terminie 14 dni od dnia zaistnienia zmiany lub odwołania.

Zadania i kompetencje IOD/Zastępcy

5.6 Do zadań IOD należy:

5.6.1 zapewnienie oraz monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz bezpieczeństwa ich przetwarzania w ENSEMBLE3;

5.6.2 opracowanie propozycji zmian w zakresie dostosowania procesów w organizacji do wymogów ochrony danych osobowych zgodnie z przepisami prawa, w tym opracowywanie i aktualizacja dokumentów dotyczących legalnego przetwarzania danych osobowych, w tym treści klauzul informacyjnych, klauzul zgody na przetwarzanie danych osobowych i klauzul poufności;

5.6.3 udzielanie pracownikom wskazówek w przedmiocie wdrożenia odpowiednich i skutecznych środków technicznych i organizacyjnych mających zabezpieczyć dane osobowe;

5.6.4 identyfikowanie ryzyk i monitorowanie zidentyfikowanych ryzyk związanych z przetwarzaniem danych osobowych, ich źródła, charakteru, prawdopodobieństwa i wagi oraz proponowanie działań minimalizujących ryzyka;

5.6.5 udzielanie zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitorowania ich wykonania zgodnie z przepisami prawa;

5.6.6 informowanie ADO i pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich w zakresie przetwarzania i ochrony danych osobowych,

5.6.7 nadzorowanie oraz audytowanie przestrzegania zasad przetwarzania danych osobowych w ENSEMBLE3;

5.6.8 organizowanie szkoleń w zakresie ochrony danych osobowych;

5.6.9 współpracowanie z PUODO w zakresie ochrony danych osobowych;

5.6.10 pełnienie roli punktu kontaktowego dla osób dane dotyczą składających wnioski o realizację ich praw wynikających z RODO;

5.6.11 prowadzenie przez osobę wskazaną przez IOD wykazów wytworzonych przez KO rejestrów czynności przetwarzania danych osobowych oraz rejestrów kategorii czynności przetwarzania danych osobowych oraz nadzorowanie ich realizacji i aktualizacji

5.6.12 rozwiązywanie bieżących problemów w obszarze ochrony danych osobowych oraz uczestnictwo w procesie zarządzania incydentami bezpieczeństwa.

5.6.13 zwracanie się przez IOD w imieniu ADO do Kierowników KO oraz pracowników ENSEMBLE3 o realizację zadań z zakresu ochrony danych osobowych.

5.7 IOD zobowiązany jest do współpracy i udzielania wsparcia KO podczas audytów realizowanych w obszarze ochrony danych osobowych.

5.8 IOD zobowiązany jest do uzgadniania poziomu zabezpieczeń stosowanych w systemach przetwarzających dane osobowe, tak aby zapewnił on właściwy poziom ochrony danych i był zgodny z przepisami o ochronie danych osobowych.

5.9 Osoba zastępująca IOD wykonuje zadania IOD wynikające z PBDO w czasie nieobecności IOD w pracy. IOD wskazuje osobę zastępującą, która na podstawie udzielonego jej przez ADO pełnomocnictwa realizuje zadania IOD w czasie jego nieobecności lub czasowej niemożności wykonywania przez niego obowiązków, w zakresie niezbędnym do zachowania ciągłości w ochronie danych osobowych.

Obowiązki pracowników i innych osób zaangażowanych w przetwarzanie danych osobowych

5.10 Pracownicy ENSEMBLE3 przetwarzający dane osobowe obowiązani są dołożyć szczególnej staranności w celu ochrony interesu osób, których dane dotyczą, a w szczególności należy przestrzegać, aby dane te były:

5.10.1 przetwarzane zgodnie z prawem,

5.10.2 zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,

5.10.3 merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,

5.10.4 przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

5.11 Kierownicy KO oraz pracownicy na stanowiskach samodzielnych zobowiązani są do przestrzegania przepisów o ochronie danych osobowych w obszarze swojej odpowiedzialności, a także do ścisłej współpracy oraz realizacji poleceń i zaleceń IOD wynikających z przepisów o ochronie danych osobowych. W tym celu zobowiązani są m.in. do:

5.11.1 bieżącej oceny funkcjonowania mechanizmów zabezpieczeń i ochrony,

5.11.2 występowania z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych,

5.11.3 prowadzenia rejestrów czynności przetwarzania danych osobowych oraz w stosownych przypadkach rejestrów kategorii czynności przetwarzania w ramach swoich KO, a także informowanie IOD o wszelkich zmianach w tych rejestrach,

5.11.4 zgłaszanie naruszeń ochrony danych osobowych do IOD,

5.11.5 wnioskowania o wydanie upoważnień do przetwarzania danych osobowych i nadzór nad aktualnością upoważnień w zakresie podległych im pracowników,

5.11.6 zbierania i przekazywania, zgodnie z poleceniem IOD, informacji niezbędnych do udzielenia odpowiedzi na wniosek podmiotu danych.

5.11.7 Kierownik KO wskazuje w podległej komórce organizacyjnej osobę do kontaktu i współpracy w zakresie realizacji zadań związanych z ochroną danych osobowych w ENSEMBLE3.

5.11.8 Wskazany przez IOD pracownik prowadzi i aktualizuje Wykaz osób, o których mowa w pkt powyżej.

5.12 Kierownicy KO wydają upoważnienia do przetwarzania danych osobowych dla pracowników podległej komórki organizacyjnej na podstawie pełnomocnictwa wydanego przez ADO.

5.13 Naruszenie postanowień PBDO może skutkować zablokowaniem dostępu pracownika do danych i systemu informatycznego. Ponadto, w przypadku ciężkich naruszeń, takie działanie może prowadzić do wszczęcia postępowania dyscyplinarnego oraz do rozwiązania umowy. W przypadku poniesienia szkody w wyniku naruszenia, ENSEMBLE3 może dochodzić roszczeń odszkodowawczych na drodze sądowej.

6 Rejestry czynności przetwarzania danych/rejestr kategorii przetwarzania

6.1 Każda KO ENSEMBLE3 tworzy i prowadzi rejestr czynności przetwarzania danych osobowych, wg wzoru zamieszczonego w załączniku nr 1 do niniejszej PBDO.

6.2 Za aktualizację i prawidłowe wypełnienie rejestru czynności przetwarzania danych osobowych odpowiada Kierownik KO.

6.3 W przypadku, gdy KO realizuje umowę, w ramach której inny podmiot powierza przetwarzanie danych osobowych ENSEMBLE3, to KO odpowiedzialna za realizację umowy zobowiązana jest prowadzić Rejestr kategorii przetwarzania danych osobowych dokonywanych w imieniu ADO. Wzór Rejestru kategorii przetwarzania stanowi załącznik nr 2 do niniejszej PBDO. Wszystkie rejestry i ich aktualizacje wymagają zgłoszenia do IOD.

6.4 Wskazany przez IOD pracownik prowadzi Wykaz rejestrów, o których mowa w pkt 6.1 oraz 6.3 na podstawie otrzymanych od Kierownika KO zaktualizowanych ww. rejestrów. O wszelkich zmianach w rejestrach informuje IOD.

7. Wydawanie upoważnień do przetwarzania danych osobowych

7.1 IOD wskaże osoby, które będą prowadziły szkolenia z zakresu ochrony danych osobowych w oparciu o zatwierdzoną przez niego prezentację oraz będą prowadziły ewidencję osób upoważnionych do przetwarzania danych osobowych, która powinna zawierać:

7.1.1 imię i nazwisko osoby upoważnionej,

7.1.2 datę nadania,

7.1.3 datę ustania uprawnień do przetwarzania danych osobowych,

7.1.4 zakres upoważnienia do przetwarzania danych osobowych zgodny z zakresem obowiązków,

7.2 Pracownik wyznaczony/IOD po przeprowadzeniu szkolenia odbiera od osoby przeszkolonej oświadczenie, które stanowi załącznik nr 3 do PBDO. Oryginał tego oświadczenia osoba szkoląca przekazuje do osoby/działu odpowiedzialnego za kwestie kadrowe w celu włączenia do teczek akt osobowych, natomiast skan do właściwego Dyrektora KO.

7.3 Dyrektor KO na podstawie posiadanego pełnomocnictwa zgodnego z załącznikiem nr 4 do

PBDO oraz otrzymanego oświadczenia, o którym mowa w punkcie 7.2, wydaje osobie przeszkolonej upoważnienie do przetwarzania danych osobowych zgodnie ze wzorem stanowiącym załącznik nr 5 do PBDO. Oryginał upoważnienia Dyrektor KO przekazuje do osoby/działu odpowiedzialnego za kwestie kadrowe w celu włączenia do teczki akt osobowych, natomiast skan do IOD.

7.4 Upoważnienie jest ważne do czasu realizowania czynności związanych z przetwarzaniem danych osobowych w ENSEMBLE3.

7.5 Dyrektorzy KO wydają upoważnienia do przetwarzania danych osobowych pracownikom podległej komórki organizacyjnej na podstawie upoważnienia udzielnego przez ADO.

8. Zasady przetwarzania danych osobowych

8.1 Dane mogą być zbierane dla oznaczonych, zgodnych z prawem celów i nie mogą podlegać dalszemu przetwarzaniu niezgodnemu z tymi celami,

8.2 Zbierane dane muszą być merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

8.3 Rodzaj i treść danych nie może wykraczać poza potrzeby wynikające z celu ich zbierania.

8.4 Zabronione jest zbieranie wszelkich danych nieistotnych, niemających znaczenia lub o większym stopniu szczegółowości, niż wynika to z określonego celu.

8.5 Dane mogą być przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

8.6 Okres przechowywania może zostać wydłużony nawet po osiągnięciu celu przetwarzania, jeżeli przepisy ustaw szczególnych takie postępowanie dopuszczają.

9. Ochrona danych w fazie projektowania oraz zasada domyślnej ochrony danych

9.1 Przepisy RODO obligują uwzględnienie i wbudowanie rozwiązań dla bezpieczeństwa danych i prywatności na każdym z etapów tworzenia oprogramowania, za pomocą którego przetwarzane są dane osobowe.

9.2 Każdy projekt dotyczący zmiany lub wprowadzenia nowych rozwiązań związanych z dużym prawdopodobieństwem wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych należy przeanalizować zgodnie z Zasadami privacy by default i privacy by design[1] w tworzeniu oprogramowania stanowiącymi załącznik nr 6 do niniejszej PBDO.

10. Ocena skutków

10.1 Zgodnie z art. 35 RODO w przypadku przetwarzania danych osobowych w szczególności z użyciem nowych technologii, które ze względu na swój charakter, zakres, kontekst, cele mogą spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, należy

[1] Zasada prywatności w fazie projektowania i zasada prywatności w ustawieniach domyślnych.

przeprowadzić ocenę skutków dla ochrony danych osobowych. PUODO ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania skutków dla ochrony danych. IOD monitoruje podawane przez PUODO informacje dotyczące rodzaju przetwarzań, dla których konieczne jest przeprowadzenie analizy skutków dla ochrony danych osobowych i przekazuje je do wiadomości KO.

10.2 IOD przekazuje Kierownikom KO informacje o obszarach, dla których należy przeprowadzić ocenę skutków dla ochrony danych osobowych.

10.3 Ocenę skutków należy przeprowadzić także, gdy KO planuje wprowadzenie nowego rodzaju przetwarzania danych osobowych, w szczególności nowego rozwiązania technicznego czy nowego programu, w którym są przetwarzane dane osobowe lub każdego innego nowego środka przetwarzania danych osobowych, które może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych. Kierownik KO przeprowadza ocenę skutków dla ochrony danych osobowych i niezwłocznie informuje o tym IOD, wskazując rodzaj i charakter nowego rozwiązania.

10.4 Ocenę skutków dla ochrony danych osobowych należy przeprowadzić zgodnie z „Wytycznymi dotyczącymi oceny skutków dla ochrony danych oraz pomagającymi ustalić czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679".

10.5 Wykonaną ocenę skutków dla ochrony danych Kierownik KO przekazuje do ADO celem jej zatwierdzenia.

10.6 ADO przed zatwierdzeniem oceny skutków może dokonać konsultacji z IOD

11. Realizacja praw osób, których dane dotyczą

11.1 ADO w przypadku realizacji praw osoby, której dane dotyczą, zobowiązany jest prowadzić z nią komunikację w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

11.2 ADO zobowiązany jest udzielić osobie, której dane dotyczą wszelkich informacji, o których mowa w art. 13 i 14 RODO oraz prowadzić z nią komunikację w zakresie realizacji art. 15–22 i 34 RODO w sprawie przetwarzania danych jej dotyczących.

11.3 Zasady realizacji praw osób, których dane dotyczą określa Instrukcja realizacji praw osób, których dane dotyczą w ENSEMBLE3, stanowiąca Instrukcję nr 1 do niniejszej PBDO.

12. Realizacja obowiązku informacyjnego

12.1 KO w przypadku zbierania danych osobowych bezpośrednio od osoby, której dane dotyczą, zarówno na formularzach papierowych, jak i elektronicznych, załącza klauzulę informacyjną, o której mowa w art. 13 RODO (jej wzór stanowi załącznik nr 7 do niniejszej PBDO).

12.2 W sytuacji braku podstawy prawnej do przetwarzania danych osobowych w konkretnym celu lub zakresie, należy pod klauzulą informacyjną umieścić klauzulę zgody wraz z odrębnym miejscem na podpis (przykładowa klauzula zgody stanowi załącznik nr 8 do niniejszej PBDO).

12.3 W sytuacji zbierania danych osobowych niebezpośrednio od osoby, której dane dotyczą,

należy spełnić wymagania określone w art. 14 RODO. Wzór klauzuli stanowi załącznik nr 9 do niniejszej PBDO.

13. Powierzenie przetwarzania danych osobowych

13.1 Zlecanie jakichkolwiek czynności związanych z przetwarzaniem danych osobowych podmiotom zewnętrznym w imieniu ENSEMBLE3 jest formą powierzenia przetwarzania danych osobowych.

13.2 Powierzenie przetwarzania danych osobowych odbywa się zgodnie z art. 28 RODO, na podstawie umowy zawartej na piśmie pomiędzy ENSEMBLE3 a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.

13.3 Przykładowe zapisy (umowa) dotyczące powierzenia przetwarzania danych osobowych zostały zamieszczone w załączniku nr 10 do niniejszej PBDO.

13.4 Kierownik KO jest odpowiedzialny za stosowanie odpowiednich zapisów dotyczących powierzania przetwarzania danych osobowych.

13.5 Podpisanie umowy związanej z powierzeniem przetwarzania danych osobowych nadzoruje Kierownik KO przygotowujący umowę główną.

13.6 Kserokopia podpisanej umowy powierzenia przetwarzania danych osobowych przekazywana jest do IOD niezwłocznie, nie później niż w terminie 3 dni od dnia jej podpisania.

13.7 W projekcie umowy/aneksu/paragrafu należy wyspecyfikować zakres czynności związanych z przetwarzaniem powierzonych danych osobowych, zakres danych oraz wymagania dotyczące ochrony danych.

13.8 W przypadku planowania powierzenia przetwarzania danych osobowych innemu podmiotowi, celem zapewnienia bezpieczeństwa przetwarzania danych osobowych przez ADO, należy przeprowadzić weryfikację podmiotu przetwarzającego. Zasady weryfikacji podmiotu przetwarzającego dane osobowe zostały zamieszczone w Instrukcji nr 2 do niniejszej PBDO.

13.9 W przypadku, gdy zlecanie czynności związanych z przetwarzaniem danych osobowych podmiotom zewnętrznym w imieniu ENSEMBLE3 dotyczy danych osobowych, które zostały powierzone ENSEMBLE3 zgodnie z art. 28 RODO, należy podpisać umowę dalszego powierzenia (podpowierzenia) po uzyskaniu pisemnej zgody i spełnieniu wymogów określonych przez podmiot, który powierzył ENSEMBLE3 dane osobowe.

14. Postępowanie w przypadku naruszenia bezpieczeństwa danych osobowych

14.1 Każdy pracownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować bezpośredniego przełożonego oraz IOD.

14.2 Tryb postępowania w przypadku stwierdzenia naruszenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych opisują Zasady zgłaszania naruszeń ochrony danych osobowych w ENSEMBLE3, zamieszczone w Instrukcji nr 3 do niniejszej PBDO.

15. Współpraca z organem nadzorczym

Zasady współpracy z PUODO określające sposób działania i współpracy pracowników ENSEMBLE3 w kontaktach z PUODO w zakresie realizacji przepisów o ochronie danych osobowych i opisane zostały w Instrukcji nr 4 do niniejszej PBDO.

16. Wykaz zbiorów danych osobowych oraz wykaz programów i systemów zastosowanych do przetwarzania danych

16.1 IOD prowadzi zbiorcze zestawienie rejestrów, o których mowa w rozdziale 6 powyżej.

17. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

17.1 ABSI prowadzi w formie elektronicznej Wykaz programów i systemów informatycznych, w których są przetwarzane dane osobowe w ENSEMBLE3 oraz informacje o powiązaniach i przepływie danych pomiędzy nimi w ENSEMBLE3. ABSI zobowiązany jest udostępnić Wykaz na każde żądanie IOD.

17.2 Wykaz programów i systemów informatycznych, w których są przetwarzane dane osobowe w ENSEMBLE3 oraz informacje o powiązaniach i przepływie danych pomiędzy nimi, ABSI opracowuje w porozumieniu z AM tych systemów.

17.3 ABSI przesyła Wykaz, o którym mowa w pkt 17.1 wraz z opisem stanu faktycznego do IOD każdego roku do dnia 30 stycznia oraz każdorazowo w przypadku jakichkolwiek zmian.

17.4 AM zobowiązany jest informować ABSI o wszelkich zmianach w wykazie, o którym mowa w pkt 17.1. powyżej.

17.5 Fakt powstania zbioru danych osobowych w nowym systemie informatycznym, zgłaszany jest pisemnie do ABSI przez AM tego systemu, lub w przypadku zgłoszenia przed wyznaczeniem AM – Kierownika KO. należy podać niżej wymienione informacje:

a) Nazwa zbioru danych osobowych,

b) Nazwa systemu informatycznego, w którym przetwarzany jest zbiór danych osobowych,

c) Zakres danych osobowych zawartych w zbiorze,

d) Cel zbierania danych,

e) Podstawa prawna zbierania danych,

f) Ewentualne powiązania z innymi systemami informatycznymi/bazami danych

18. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

18.1 Wszystkie dane osobowe w ENSEMBLE3 są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:

18.1.1 W każdym przypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla przetwarzania danych.

18.1.2 Dane są przetwarzane rzetelnie i w sposób przejrzysty.

18.1.3 Dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

18.1.4 Dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągniecia celu przetwarzania danych.

18.1.5 Dane osobowe są prawidłowe i w razie potrzeby uaktualniane.

18.1.6 Czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane.

18.1.7 Wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO.

18.1.8 Dane są zabezpieczone przed naruszeniami zasad ich ochrony.

18.2 ADO zobowiązany jest do zastosowania, adekwatnych do stwierdzonego poziomu ryzyka dla poszczególnych systemów, środków technicznych i organizacyjnych dla zapewnienia poufności, integralności, dostępności i rozliczalności przetwarzanych danych.

18.3 W zakresie środków organizacyjnych ENSEMBLE3 wdraża się w szczególności:

a) Ewidencję osób upoważnionych do przetwarzania danych osobowych. Wzór ewidencji stanowi załącznik nr 11 do niniejszego dokumentu.

b) Rejestr czynności przetwarzania danych osobowych.

c) Rejestr kategorii czynności przetwarzania danych osobowych.

d) Wzór postanowień (umowy) dotyczący powierzenia przetwarzania danych osobowych.

e) Rejestr Podmiotów, którym powierzono do przetwarzania dane osobowe ENSEMBLE3 zgodnie z załącznikiem nr 12.

18.4 W zakresie środków technicznych wdraża się:

a) Kontrolę dostępu do obszarów fizycznych przetwarzania danych osobowych.

b) Ochronę kryptograficzną przesyłanych danych.

c) Zabezpieczenia przed utratą danych (np. zapasowe zasilanie, wykonywanie kopii zapasowych itp.).

18.5 Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do: likwidacji, naprawy — pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.

18.6 Użytkując komputer przenośny zawierający dane osobowe należy zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem wskazanym w wykazie budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe. Należy stosować środki ochrony kryptograficznej w stosunku do danych osobowych przetwarzanych na komputerach przenośnych, o ile są używane poza obszarem przetwarzania danych osobowych.

18.7 Systemy chroniące dostęp z sieci publicznej do systemów przetwarzających dane osobowe muszą zapewniać:

18.7.1 Kontrolę przepływu informacji pomiędzy systemem informatycznym przetwarzającym dane osobowe a siecią publiczną.

18.7.2 Kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego ADO.

19. Współpraca IOD z działem prawnym/wsparciem prawnym/ radcą prawnym

19.1 Sporządzanie na wniosek IOD opinii prawnych dotyczących interpretacji przepisów RODO oraz krajowych przepisów o ochronie danych osobowych,

19.2 Weryfikowanie pod względem prawnym oraz przygotowywanie we współpracy z IOD odpowiedzi na wniosek podmiotu danych o realizację swoich praw, o których mowa w RODO,

19.3 Weryfikowanie umów przekazywanych przez komórki organizacyjne ENSEMBLE3 pod względem konieczności zawarcia w nich zapisów dotyczących ochrony danych osobowych.

20. Zasady rozpowszechniania

20.1 Z zapisami PBDO powinni zapoznać się wszyscy pracownicy, a także inne osoby mające dostęp do danych osobowych (np. stażyści, praktykanci).

20.2 Niniejszy dokument może być udostępniony w celu zapoznania się i zgodnego postępowania tylko uprawnionym podmiotom zewnętrznym.

20.3 Nadzór nad przestrzeganiem PBDO oraz dokumentów związanych pełni IOD.

20.4 Postępowanie niezgodne z niniejszą PBDO wiąże się ze skutkami przewidzianymi w Kodeksie pracy, Kodeksie cywilnym lub innych właściwych przepisach prawa.

21. Odstępstwa od reguł ochrony danych osobowych

Odstąpienie od zasad opisanych w PBDO jest możliwe wyłącznie po spełnieniu poniższych warunków:

a) Zwrócenie się z pisemnym wnioskiem do ADO o odstąpienie od reguł ochrony i uzasadnienie we wniosku powodu odstąpienia od przyjętych zasad bezpieczeństwa.

b) Otrzymanie pisemnej informacji od ADO.

22. Załączniki

Załącznik nr 1 – Wzór rejestru czynności przetwarzania danych.

Załącznik nr 2 – Wzór rejestru kategorii czynności przetwarzania danych.

Załącznik nr 3 – Wzór oświadczenia o zapoznaniu się z przepisami o ochronie danych osobowych.

Załącznik nr 4 – Pełnomocnictwo i upoważnienie do prowadzenie czynności w zakresie upoważnień do przetwarzania danych osobowych.

Załącznik nr 5 – Wzór upoważnienia do przetwarzania danych osobowych.

Załącznik nr 6 – Zasady privacy by default privacy by design w tworzeniu oprogramowania.

Załącznik nr 7 – Przykładowa klauzula informacyjna, zbieranie danych osobowych bezpośrednio od osoby, której dane dotyczą.

Załącznik nr 8 – Przykładowy wzór klauzuli zgody na przetwarzanie danych osobowych

Załącznik nr 9 – Przykładowa klauzula informacyjna, zbierania danych osobowych niebezpośrednio od osoby, której dane dotyczą.

Załącznik nr 10 – Wzór zapisy/umowa powierzenia przetwarzania danych osobowych.

Załącznik nr 11 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych.

Załącznik nr 12 – Wzór rejestr podmiotów, którym powierzono do przetwarzania dane osobowe.

Instrukcja nr 1 do PBDO – Instrukcja realizacji praw osób, których dane dotyczą.

Instrukcja nr 2 do PBDO – Instrukcja weryfikacji podmiotu przetwarzającego dane osobowe.

Instrukcja nr 3 do PBDO – Instrukcja zgłaszania naruszeń ochrony danych osobowych.

Instrukcja nr 4 do PBDO – Instrukcja współpracy z organem nadzorczym.

23. Dokumenty związane

23.1 Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

24. Rejestr zmian

Lp.	Data	Opis	Dotyczy stron(y)	Wprowadzający zmianę

Prezes
dr hab. Dorota A. Pawlak

ENSEMBLE Sp. z o.o.
ul. Wólczyńska 133
01-919 W A R S Z A W A
NIP 118 221 10 96, REGON 386406355
-HR-