INNOBALTICA

Polityka bezpieczeństwa danych osobowych w InnoBaltica Sp. z o.o.

METRYKA DOKUMENTU

Nazwa dokumentu	Polityka Bezpieczeństwa Danych Osobowych w InnoBaltica Sp. z o.o.		
Komórka nadzorująca	Koordynator-Administrator Bezpieczeństwa Informacji		
Autor dokumentu	BLUE ENERGY Sp. z o.o.	**Podpis**	
Sprawdził	Wiesław Telepski		
Zatwierdził	Krzysztof Rudziński		

HISTORIA ZMIAN

Wersja	Data	Autor	Zakres zmian	Opis zmian
1.0.			Cały dokument	Opracowanie i wdrożenie do stosowania

Spis treści

I. Cel Polityki Bezpieczeństwa Danych Osobowych

1. Celem niniejszego dokumentu jest określenie jednolitych standardów ochrony danych osobowych w spółce InnoBaltica Sp. z o.o. (dalej InnoBaltica).
2. Niniejszy dokument zawiera opis czynności umożliwiających zapewnienie zgodności z mającymi zastosowanie przepisami prawa w obszarze ochrony danych osobowych. Ponadto Polityka określa uprawnienia, odpowiedzialności i obowiązki pracowników InnoBaltica w przedmiotowym obszarze.
3. Niniejszy dokument zawiera zestaw wymagań przyjętych w spółce InnoBaltica, niezbędnych do zapewnienia zgodności z mającymi zastosowanie regulacjami prawnymi.

II. Podstawowe pojęcia i definicje

Administrator Danych Osobowych (ADO) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; rolę ADO na potrzeby stosowania niniejszej Polityki pełni członek Zarządu;

Administrator Systemów Informatycznych (ASI) – oznacza wyznaczonego pracownika InnoBaltica, który jest odpowiedzialny za nadzór oraz bezpieczeństwo systemów teleinformatycznych;

Dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, dane dotyczące zdrowia, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

Inspektor Ochrony Danych (IOD) – oznacza wyznaczonego pracownika InnoBaltica lub firmę zewnętrzną świadczącą usługę pełnienia nadzoru nad ochroną danych osobowych oraz monitorującą wypełnienie mających zastosowanie obowiązków wynikających z regulacji prawnych w obszarze danych osobowych w spółce InnoBaltica;

Kategoria osób, których dane dotyczą – oznacza kategorię/grupę osób, których dane osobowe są przetwarzane w spółce InnoBaltica (m.in. pracownicy, klienci, kontrahenci);

Naruszenie ochrony danych osobowych – oznacza naruszenie zasad bezpieczeństwa prowadzące do przypadkowego lub celowego, niezgodnego z prawem: zniszczenia, utracenia, zmodyfikowania, ujawnienia, nieuprawnionego uzyskania lub udzielenia dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu udostępnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie

z prawem Unii Europejskiej lub prawem Państwa Członkowskiego, nie są uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne powinno być zgodne z przepisami o ochronie danych osobowych mającymi zastosowanie stosownie do celów przetwarzania;

Ograniczenie przetwarzania – oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

Organ nadzorczy - oznacza niezależny organ publiczny ustanowiony przez Państwo Członkowskie zgodnie z art. 51 RODO;

Państwo trzecie – oznacza Państwo, które nie wchodzi w skład EOG (Europejskiego Obszaru Gospodarczego);

Podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu ADO;

Podmiot zewnętrzny – oznacza osobę fizyczną, jednostkę organizacyjną nieposiadającą osobowości prawnej lub osobę prawną z siedzibą w Polsce lub za granicą, organ administracji publicznej, oraz inne podmioty wykonujące zadania na rzecz Spółki, w tym konsultantów, doradców, audytorów i inne osoby w nich zatrudnione;

Pracownik – oznacza osobę zatrudnioną w spółce InnoBaltica na podstawie umowy o pracę: np. umowy o pracę na okres próbny, umowy o pracę na czas określony, umowy o pracę na czas nieokreślony, inne;

Przedstawiciel - oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii Europejskiej, która została wyznaczona na piśmie przez ADO lub podmiot przetwarzający na mocy art. 27 RODO do reprezentowania ADO lub podmiotu przetwarzającego w zakresie ich obowiązków;

Przetwarzanie - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

Pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było 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;

RODO – oznacza 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;

Strona trzecia - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, ADO, podmiot przetwarzający czy osoby, które – z upoważnienia ADO lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

Szczególne kategorie danych (tzw. dane wrażliwe) – oznacza informacje dotyczące pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub światopoglądowych, przynależności do związków zawodowych, stanu zdrowia, orientacji seksualnej oraz dane genetyczne i biometryczne;

Współpracownik – oznacza osobę realizującą powierzone zadania, obowiązki na podstawie umowy cywilnoprawnej np. umowy zlecenia, umowy o dzieło, kontrakty menedżerskie;

Zgoda – osoby, której dane dotyczą oznacza 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.

III. Podstawy prawne ochrony danych osobowych w spółce InnoBaltica

1. Podstawę prawną zasad określonych w niniejszej Polityce stanowią w szczególności:
   1.1. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 r. poz. 1000);
   1.2. 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.

IV. Deklaracja zgodności

1. ADO deklaruje, że przetwarzanie danych osobowych w spółce InnoBaltica jest zgodne z mającymi zastosowanie wymaganiami prawnymi.
2. Deklaracja ta opiera się w szczególności na zapewnieniu, że dane osobowe są:
   2.1. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
   2.2. zbierane w konkretnych, wyraźnych, prawnie uzasadnionych celach i przetwarzane w sposób zgodny z tymi celami,
   2.3. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,
   2.4. prawidłowe i w razie potrzeby uaktualniane,
   2.5. 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,
   2.6. przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

V. Podział obowiązków w zakresie ochrony danych osobowych w spółce InnoBaltica

1. ADO jest odpowiedzialny za:

1.1. wprowadzenie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych w organizacji danych osobowych,
1.2. dostarczenie niezbędnych zasobów do zapewnienia zgodności z mającymi zastosowanie wymaganiami prawnymi w obszarze ochrony danych osobowych,
1.3. powoływanie i odwoływanie IOD oraz wspieranie IOD w wypełnianiu przez niego zadań,
1.4. zapewnienie kwalifikacji IOD, a w szczególności fachowej wiedzy nt. prawa i praktyk w dziedzinie ochrony danych osobowych.

2. IOD jest odpowiedzialny za:
2.1. nadzorowanie opracowywanie, tworzenie i aktualizację wewnętrznych aktów normatywnych (niniejsza Polityka, procedury, instrukcje, regulaminy i inne dokumenty) dotyczących ochrony danych osobowych oraz nadzór nad ich przestrzeganiem
2.2. prowadzenie wymaganej przepisami prawa dokumentacji przetwarzania danych osobowych
2.3. utrzymywanie aktualnego Rejestru czynności przetwarzania danych osobowych (Załączniki nr 1 do niniejszej Polityki),
2.4. kontakty z właściwym organem administracji publicznej ds. ochrony danych osobowych związane ze składaniem wyjaśnień oraz współpracą w przypadku kontroli przeprowadzanej przez inspektorów organu nadzorczego,
2.5. prowadzenie szkoleń w zakresie ochrony danych osobowych oraz zapewnienie zapoznania pracowników i współpracowników przepisami o ochronie danych osobowych,
2.6. okresowe dokonywanie przeglądów zasobów informacyjnych InnoBaltica zawierających dane osobowe, oceny stanu bezpieczeństwa tych zasobów oraz raportowanie o wynikach i niezbędnych działaniach doskonalących do ADO,
2.7. sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, przeprowadzanie weryfikacji zgodności przetwarzania danych osobowych z mającymi zastosowanie regulacjami prawnymi w obszarze ochrony danych osobowych na żądanie organu ds. ochrony danych lub ADO,
2.8. konsultowanie merytoryczne umów powierzenia przetwarzania danych osobowych, nadzór nad realizacją umów.

3. ASI jest odpowiedzialny za:
3.1. administrację środowiskami informatycznymi przeznaczonymi do przetwarzania danych osobowych,
3.2. administrację uprawnieniami nadawanymi/modyfikowanymi/odbieranymi do systemów informatycznych przetwarzających dane osobowe,
3.3. zapewnienie ciągłości działania systemu informatycznego i optymalizację jego wydajności,
3.4. instalację i konfigurację sprzętu i oprogramowania,
3.5. konfigurację i administrację oprogramowaniem systemowym i sieciowym,
3.6. identyfikowanie i zgłaszanie do ADO oraz IOD ewentualnych problemów z zakresu bezpieczeństwa i ochrony danych osobowych,
3.7. zapewnienie bezpieczeństwa przechowywanych w systemie teleinformatycznym danych osobowych,
3.8. nadzór nad procesem administracji, środowiskami informatycznymi przeznaczonymi do przetwarzania danych osobowych,

3.9. nadzór nad procesem administracji, uprawnieniami nadawanymi/modyfikowanymi/odbieranymi do systemów informatycznych przetwarzających dane osobowe,
3.10. planowanie i realizację, w porozumieniu z IOD, działań podnoszących bezpieczeństwo systemów informatycznych, w tym inicjowanie, wdrażanie i koordynowanie wdrożenia nowych rozwiązań informatycznych,
3.11. kontrolowanie, za pomocą inspekcji (w tym nieplanowanych) i audytów przestrzegania zasad przetwarzania danych osobowych na stacjach roboczych użytkowników,
3.12. współpracę z IOD w wymaganym zakresie, na podstawie mających zastosowanie wymagań prawnych w obszarze ochrony danych osobowych (m.in. prowadzenie Rejestru czynności przetwarzania, usuwanie/modyfikowanie/uzupełnianie danych osobowych na wniosek osoby, której dane dotyczą).

4. Wszystkie osoby przetwarzające dane osobowe w InnoBaltica są odpowiedzialne za:
4.1. przetwarzanie danych osobowych zgodnie przyjętą Polityką oraz zapisami RODO,
4.2. przestrzeganie zasad ochrony danych osobowych określonych w Polityce i Instrukcji Zarządzania Systemami Teleinformatycznymi oraz dokumentach z nimi związanych. W tym celu każdy użytkownik zobowiązany jest zapoznać się przed dopuszczeniem do przetwarzania danych z wyżej wymienionymi dokumentami oraz złożyć stosowne Oświadczenie w formie zobowiązania pracownika do zachowania poufności danych osobowych, potwierdzające znajomość ich treści (Załącznik nr 2 do niniejszej Polityki),
4.3. spełnianie wymogu wynikającego z obowiązku informacyjnego, w szczególności poinformowania osoby, której dane dotyczą zgodnie z zakresem wskazanym w punkcie VIII.1 niniejszej Polityki,
4.4. uczestniczenie w obowiązkowym szkoleniu z zakresu ochrony danych osobowych,
4.5. bezzwłoczne zgłaszanie IOD lub ASI wszelkich dostrzeżonych nieprawidłowości w działaniu systemu informatycznego, w którym przetwarzane są dane osobowe,
4.6. bezzwłoczne zgłaszanie wszelkich incydentów, nieprawidłowości i dostrzeżonych zagrożeń związanych z bezpieczeństwem danych osobowych,
4.7. wnioskowanie do IOD o potrzebie uzupełnienia lub uaktualnienia Rejestru czynności przetwarzania danych osobowych, potrzebie dokonania zmian w procesie przetwarzania danych osobowych oraz informowanie o ustaniu celu przetwarzania tych danych,
4.8. niezwłoczne usunięcie/zaprzestanie przetwarzania danych osobowych w momencie ustania celu ich przetwarzania,
4.9. informowanie IOD o zamiarze powierzenia przetwarzania danych osobowych lub ich udostępnienia innemu podmiotowi oraz konsultowanie z IOD umowy o powierzeniu przetwarzania danych osobowych,
4.10. dołożenia szczególnej staranności podczas przetwarzania danych osobowych, aby proces przetwarzania odbywał się zgodnie z prawem, dane osobowe były merytorycznie poprawne, a ich przetwarzanie odbywało się wyłącznie w celu i zakresie, dla którego zostały zebrane.

VI. Rejestr czynności przetwarzania danych osobowych

1. Dla wszystkich zidentyfikowanych kategorii danych osobowych, IOD przy współpracy z ASI prowadzi Rejestr czynności przetwarzania danych osobowych (Załącznik nr 1).

2. Na rejestr czynności przetwarzania danych osobowych składają się co najmniej następujące pola:
   2.1. liczba porządkowa,
   2.2. opis kategorii osób, których dane dotyczą,
   2.3. cel przetwarzania danych osobowych,
   2.4. podstawa prawna przetwarzania,
   2.5. źródło danych osobowych,
   2.6. opis kategorii danych osobowych,
   2.7. informacja o przetwarzaniu danych wrażliwych,
   2.8. lokalizacje, w których przetwarzane są dane osobowe,
   2.9. systemy teleinformatyczne, w których przetwarzane są dane osobowe,
   2.10. informacja o przetwarzaniu danych osobowych w formie papierowej,
   2.11. planowany termin usunięcia danych osobowych,
   2.12. stosowane zabezpieczenia organizacyjne i techniczne,
   2.13. informacje o podmiotach, którym dokonano powierzenia i dalszego powierzenia danych osobowych,
   2.14. informacje o podmiotach, którym udostępniono dane osobowe,
   2.15. informacje o przekazaniu danych osobowych do Państwa trzeciego.
   2.16. Rejestr czynności przetwarzania danych osobowych może być prowadzony w formie papierowej, elektronicznej lub w systemie teleinformatycznym.

VII. Środki techniczne i organizacyjne ochrony danych osobowych

1. W celu zapewnienia ochrony danych osobowych przetwarzanych w InnoBaltica stosuje się następujące zabezpieczenia organizacyjne i techniczne:
   1.1. opracowano i wdrożono Politykę Bezpieczeństwa Danych Osobowych,
   1.2. opracowano i wdrożono Instrukcję Zarządzania Systemami Informatycznymi przetwarzającymi dane osobowe,
   1.3. zapewnia się realizację szkoleń dla wszystkich pracowników dopuszczonych do przetwarzania danych osobowych obejmujących zasady ich ochrony,
   1.4. do przetwarzania danych osobowych dopuszcza się jedynie pracowników, którzy uprzednio pisemnie zobowiązali się do zachowania ich poufności,
   1.5. przetwarzania danych osobowych dokonuje się w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych, w szczególności poprzez: kontrolę dostępu do pomieszczeń i budynków, instalację alarmową, monitoring. Zapewnia bezpieczeństwo w lokalizacjach, w których przetwarza się dane osobowe (szafy, biurka zamykane na klucz),
   1.6. każdą osobę przetwarzającą dane osobowe zobowiązuje się do przestrzegania podstawowych zasad bezpieczeństwa informacji,
   1.7. przebywanie osób nieupoważnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe dopuszcza się tylko w obecności pracownika oraz w warunkach zapewniających bezpieczeństwo danych,
   1.8. stosuje się pisemne umowy powierzenia przetwarzania danych osobowych przy współpracy z podmiotami zewnętrznymi przetwarzającymi dane osobowe (załącznik nr 6),

1.9. przetwarzanie danych osobowych odbywa się wyłącznie w ramach wykonywanych zadań służbowych,

2. zapewnia się zdolność do możliwie szybkiego przywrócenia dostępności danych osobowych w razie incydentu fizycznego lub technicznego,
3. zapewnia się zdolność do ciągłego zapewnienia poufności, integralności i dostępności danych osobowych przetwarzanych w systemach teleinformatycznych,
4. dokonuje się regularnych audytów i testów skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych,
5. zapewnia się zdolność systemów teleinformatycznych do spełnienia praw osób, których dane dotyczą (usunięcie, sprostowanie, sprzeciw, ograniczenie)

VIII. Realizacja obowiązku informacyjnego

1. Każdorazowo, podczas zbierania danych osobowych, przekazuje się osobie której dane dotyczą:
   1.1. tożsamość i dane kontaktowe ADO,
   1.2. dane kontaktowe IOD,
   1.3. cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania,
   1.4. informację, że przetwarzanie wykonywane jest do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO,
   1.5. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeśli istnieją,
   1.6. gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do Państwa trzeciego lub organizacji międzynarodowej oraz wzmiankę o stosowanych zabezpieczeniach, możliwościach uzyskania kopii tych danych lub o miejscu ich udostępnienia,
   1.7. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
   1.8. informacje o prawie do żądania od Spółki dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
   1.9. jeżeli przetwarzanie odbywa się na podstawie uzyskanej zgody - informacje o prawie do cofnięcia zgody na przetwarzanie danych osobowych,
   1.10. informację o prawie do wniesienia skargi do organu nadzorczego,
2. W przypadku, gdy dane osobowe zbierane są bezpośrednio od osoby, której dane dotyczą, należy przekazuje się informację czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i konsekwencjach niepodania danych,
3. W przypadku, gdy dane osobowe pozyskiwane są w inny sposób niż od osoby, której dane dotyczą, przekazuje się osobie której dane dotyczą informacje zawarte w pkt. 8.1. oraz uzupełnione o kategorie przetwarzanych danych osobowych, źródło pochodzenia danych osobowych, a gdy ma to zastosowanie również informacji czy pochodzą one ze źródeł publicznie dostępnych.

4. W przypadku, gdy planuje się dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, informuje się osobę której dane dotyczą, o nowym celu przetwarzania oraz udzielić jej stosowanych informacji zawartych w niniejszym punkcie.
5. Do realizacji obowiązku informacyjnego zobowiązani są wszyscy pracownicy Spółki
6. Obowiązek informacyjny w InnoBaltica realizuje się:
   6.1. ustnie – w przypadku bezpośredniego kontaktu z osobą, której dane dotyczą,
   6.2. pisemnie – jako integralną część umowy lub innego dokumentu z podmiotem zewnętrznym zawierającego dane osobowe,
   6.3. w formie elektronicznej – jako informacja w systemie teleinformatycznym przetwarzającym dane osobowe,
   6.4. w formie e-mail – w przypadku korespondencji e-mail.
7. Podstawowe informacje wymagane mającymi zastosowanie regulacjami prawnymi w obszarze ochrony danych osobowych udostępniane są na stronie internetowej InnoBaltica.
8. Informacje zawarte w niniejszym punkcie nie mają zastosowania w przypadku, gdy osoba, której dane dotyczą, dysponuje już tymi informacjami.
9. Przykładowa treść spełniająca wymagania obowiązku informacyjnego została zamieszczona w Załączniku nr 3 do niniejszej Polityki.

IX. Prawa osób których dane są przetwarzane przez InnoBaltica

1. Prawo dostępu przysługujące osobie, której dane dotyczą,
   1.1. Każda osoba, której dane dotyczą jest uprawniona do uzyskania potwierdzenia, czy w spółce InnoBaltica przetwarzane są jej dane osobowe.
   1.2. Na wniosek osoby, której dane dotyczą, należy przekazać informację o:
      a) celu przetwarzania danych osobowych,
      b) kategoriach przetwarzanych danych osobowych,
      c) odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w Państwach trzecich lub organizacjach międzynarodowych oraz zabezpieczeniach wykorzystywanych w związku z tym przekazaniem,
      d) w miarę możliwości planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, kryteriach tego okresu,
      e) prawie do żądania od ADO sprostowania, usunięcia lub ograniczenia przetwarzania jej danych osobowych, oraz prawie wniesienia sprzeciwu wobec takiego przetwarzania,
      f) prawie wniesienia skargi do organu nadzorczego,
      g) źródle pozyskiwania danych osobowych, jeśli nie zostały zebrane od osoby, której dane dotyczą,
      h) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, istotnych zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
   1.3. W przypadku wystąpienia przez osobę, której dane dotyczą, z wnioskiem o kopię jej danych osobowych, należy zgłosić taki fakt IOD.
   1.4. IOD dostarcza osobie, której dane dotyczą, kopię danych podlegających przetwarzaniu.

1.5. IOD podejmuje decyzję o formie, w której zostanie przekazana kopia danych oraz wysokościach opłat za wszelkie kolejne kopie.
1.6. IOD ma prawo odmowy przekazania kopii danych osobowych w przypadku, gdy może to wpłynąć na prawa i wolności innych osób.

2. Prawa do sprostowania, usunięcia, ograniczenia, przenoszenia danych osobowych oraz sprzeciwu wobec ich przetwarzania:
   2.1. Prawo do sprostowania - każda osoba, której dotyczą dane, ma prawo do żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Występująca osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
   2.2. Prawo do usunięcia danych („Prawo do bycia zapomnianym") - każda osoba, której dane dotyczą, ma prawo żądania niezwłocznego usunięcia jej danych osobowych.
   2.3. Prawo do ograniczenia przetwarzania - każda osoba, której dane dotyczą, ma prawo żądania od ADO ograniczania przetwarzania jej danych osobowych.
   2.4. Prawo do przenoszenia danych - osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczył ADO, oraz ma prawo przesłać te dane osobowe innemu Administratorowi bez przeszkód ze strony Administratora, któremu dostarczono te dane osobowe.
   2.5. Prawo do sprzeciwu - osoba, której dane dotyczą, ma prawo wnieść sprzeciw wobec przetwarzania jej danych osobowych.

3. Zasady realizacji praw osób, których dane dotyczą
   3.1. Wnioski o realizację praw osób, których dane dotyczą, kierowane są na adres: iod@ innobaltica.pl
   3.2. W przypadku, gdy wniosek zostanie skierowany do pracownika InnoBaltica, należy przekazać go do IOD.
   3.3. IOD dokonuje analizy wniosku oraz weryfikuje zasadność realizacji prawa osoby, której dane dotyczą.
   3.4. W przypadku braku zasadności realizacji prawa, IOD zobligowany jest do niezwłocznego (nie dłużej niż 1 miesiąc) przekazania tej informacji osobie wnioskującej wraz z właściwym uzasadnieniem decyzji.
   3.5. W przypadku pozytywnej oceny wniosku, IOD zobligowany jest do wszczęcia postępowania mającego na celu realizację prawa osoby wnioskującej. Po zakończeniu działań związanych z realizacją prawa osoby wnioskującej, IOD informuje o tym fakcie osobę wnioskującą. W przypadku, gdy czas realizacji prawa może przekroczyć 1 miesiąc IOD przekazuje osobie wnioskującej odpowiedź wraz z planowanym terminem realizacji prawa, o które wnioskowała.
   3.6. W przypadku realizacji prawa osoby, której dane dotyczą, IOD ma obowiązek przekazania obowiązku realizacji tego prawa do wszystkich podmiotów, którym powierzono dane do przetwarzania.
   3.7. W sytuacji, w której realizacja prawa osoby, której dane dotyczą, wymaga zaangażowania pracowników InnoBaltica, na wniosek IOD pracownicy ci są zobligowani do wykonania zadań niezbędnych do realizacji prawa wnioskującego.

X. Realizacja udostępnień danych osobowych

1. Dane osobowe udostępniane są wyłącznie na pisemny, umotywowany wniosek chyba, że przepisy prawa stanowią inaczej.
2. Udostępnienia danych osobowych może dokonać wyłącznie IOD. Wszyscy pracownicy spółki, w przypadku otrzymania wniosku o udostępnienie danych osobowych, zobligowani są do przekazania wniosku IOD.
3. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
4. Zgodę na udostępnienie danych osobowych wydaje IOD, po uzyskaniu, jeśli uzna to za konieczne, opinii prawne w kwestii zasadności samego wniosku oraz jego zakresu.
5. W przypadku wyrażenia zgody na udostępnienie, IOD przygotowuje udostępniane dane osobowe oraz odnotowuje fakt udostępnienia w Rejestrze udostępnień danych osobowych stanowiącym Załącznik nr 4 do niniejszej Polityki.
6. W przypadku udostępniania danych z systemów informatycznych, które nie odnotowują udostępnienia automatycznie, plik przekazywanych danych jest przechowywany przez IOD wraz z dokumentem wskazującym na podstawę udostępnienia i dodatkowym opisem wskazującym datę udostępnienia danych oraz określeniem odbiorcy danych (np. nazwa i adres instytucji).

XI. Zasady powierzania przetwarzania danych osobowych

1. Powierzenie przetwarzania danych osobowych przez InnoBaltica podmiotom zewnętrznym następuje wyłącznie w drodze pisemnej umowy powierzenia przetwarzania danych osobowych. Wzór treści umowy powierzenia przetwarzania danych osobowych stanowi Załącznik nr 6 do niniejszej Polityki. Dopuszczalne jest wykorzystanie innego wzoru jedynie w przypadku, gdy treść umowy spełnia minimalne wymagania wskazane w punkcie XI. Ust. 7.
2. Do powierzenia przetwarzania danych osobowych może dojść w każdej umowie bez względu na jej przedmiot (np. umowy serwisowe, remontowe, inwestycyjne itp.)
3. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych, nie może powierzyć do dalszego przetwarzania powierzonych mu danych bez wyraźnej zgody ADO.
4. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych, zobowiązany jest przetwarzać powierzone mu dane wyłącznie w celach, które zostały wskazane w zawartej z nim umowie.
5. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych, zobowiązany jest do spełnienia mających zastosowanie wymagań prawnych w obszarze danych osobowych.
6. Szczegółowe wymagania w zakresie wyboru podmiotów, którym InnoBaltica powierza dane osobowe do przetwarzania, znajdują się w dokumencie „Wymagania techniczne i organizacyjne wobec podmiotów, którym powierza się przetwarzanie danych osobowych”, stanowiącym Załącznik nr 5 do niniejszej Polityki.
7. Umowa, która zawiera zapisy o powierzeniu przetwarzania danych osobowych, powinna w szczególności zawierać zapisy dotyczące:
   7.1. przedmiotu i czasu trwania przetwarzania danych osobowych,
   7.2. charakteru i celu przetwarzania danych osobowych,
   7.3. rodzaju danych osobowych oraz kategorii osób, których dane dotyczą,
   7.4. obowiązków i praw ADO,

7.5. zobowiązań pracowników podmiotu przetwarzającego do zachowania powierzonych danych osobowych w poufności,
7.6. zapewnienia bezpieczeństwa organizacyjnego i technicznego przetwarzania danych osobowych,
7.7. zasad dalszego powierzania danych osobowych administrowanych przez InnoBaltica,
7.8. udziału w procesie udzielania odpowiedzi na żądanie osoby, której dane dotyczą, zgłaszania incydentów,
7.9. usunięciu lub zwróceniu powierzonych danych osobowych po zakończeniu świadczenia usługi,
7.10. udostępniania ADO wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w mających zastosowanie przepisach prawa w obszarze ochrony danych osobowych (np. audyty drugiej strony),
7.11. możliwości żądania natychmiastowego wstrzymania przetwarzania danych osobowych powierzonych w razie stwierdzenia niedostatecznej ochrony danych osobowych.
7.12. Każdy pracownik InnoBaltica ma obowiązek zasięgnąć opinii IOD w każdej sytuacji, w której ma nastąpić podpisanie umowy, której przedmiot choćby pośrednio wiąże się z powierzeniem innej firmie danych osobowych bądź z przyjęciem przez InnoBaltica danych osobowych do przetwarzania.

XII. Naruszenia ochrony danych osobowych

1. Za naruszenie ochrony danych osobowych uznaje się naruszenie bezpieczeństwa prowadzące do przypadkowego lub celowego, niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
2. Każdy z pracowników InnoBaltica w przypadku zidentyfikowania zdarzenia mogącego stanowić naruszenie ochrony danych osobowych, jest zobowiązany do niezwłocznego kontaktu z IOD osobiście lub poprzez e-mail: iod@innobaltica.pl
3. W uzasadnionych przypadkach osoba, która zgłosiła naruszenie, zobowiązana jest postępować zgodnie z wytycznymi IOD w zakresie zabezpieczenia materiału dowodowego i, jeśli zajdzie taka potrzeba, zaprzestania wykonywania obowiązków służbowych w celu nienaruszania materiałów dowodowych.
4. Jeżeli istnieje małe prawdopodobieństwo, iż naruszenie ochrony danych osobowych skutkować będzie naruszeniem praw lub wolności osób fizycznych, IOD nie jest zobligowany do zgłoszenia takiego naruszenia do organu nadzorczego.
5. Wszystkie zdarzenie zakwalifikowane jako naruszenie ochrony danych osobowych należy udokumentować zgodnie z wzorem Rejestru naruszeń ochrony danych osobowych, stanowiącym Załącznik nr 7 do niniejszej Polityki.
6. W przypadku gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób, których dotyczy naruszenie, należy je bez zbędnej zwłoki o tym poinformować, o ile jest to technicznie możliwe.
7. Jeżeli zgłoszenia zdarzeń w obszarze szeroko rozumianego bezpieczeństwa Spółki, a w szczególności w obszarze bezpieczeństwa przetwarzania danych osobowych, dotyczą

działania teleinformatycznych systemów, w których dane te są przetwarzane, należy je niezwłocznie zgłaszać również do ASI.

8. Zgłoszeniu do ASI podlegają również wszelkie stwierdzone słabe punkty oraz nieprawidłowości w działaniu systemów teleinformatycznych lub nietypowe, odbiegające od normy zachowania tych systemów.

XIII. Audyt ochrony danych osobowych

1. IOD jest zobowiązany do prowadzenia cyklicznych audytów przestrzegania zasad ochrony danych osobowych opisanych w regulacjach wewnętrznych InnoBaltica oraz mających zastosowanie wymaganiach prawnych. Zaleca się, aby audyty ochrony danych osobowych prowadzone były z co najmniej roczną częstotliwością.
2. Podczas określania zakresu audytu ochrony danych osobowych należy wziąć pod uwagę w szczególności:
   2.1. obszary, w których zostały zidentyfikowane naruszenia ochrony danych osobowych,
   2.2. rezultaty wcześniejszych audytów ochrony danych osobowych,
   2.3. zmiany w otoczeniu wewnętrznym i zewnętrznym organizacji,
   2.4. informację zwrotną od zainteresowanych stron.
3. Audytowi ochrony danych osobowych podlegają:
   3.1. systemy informatyczne przetwarzające dane osobowe (zgodność funkcjonalności i zabezpieczeń systemów z mającymi zastosowanie regulacjami prawnymi),
   3.2. zabezpieczenia fizyczne (zabezpieczenia pomieszczeń i budynków, w których przetwarzane są dane osobowe),
   3.3. zabezpieczenia organizacyjne (m.in. procedury komunikacji i informowania o naruszeniach, powołanie ról i odpowiedzialności, aktualność wewnętrznych aktów normatywnych),
   3.4. bezpieczeństwo osobowe (m.in. świadomość pracowników, realizacja szkoleń wstępnych i okresowych, aktualność uprawnień w systemach teleinformatycznych) oraz
   3.5. zgodność stanu faktycznego z wymaganiami mających zastosowanie aktów prawnych oraz wewnętrznych aktów normatywnych spółki.
4. Do przeprowadzania audytu ochrony danych osobowych upoważniony jest IOD lub osoba przez niego wyznaczona posiadająca niezbędną wiedzę i kwalifikacje.
5. W przypadku wystąpienia braku zgodności z wymaganiami prawnymi lub regulacjami wewnętrznymi, IOD inicjuje adekwatne działania mitygujące zidentyfikowane ryzyko lub ryzyka.

XIV. Szkolenia

1. Każdy pracownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub danymi osobowymi w wersji papierowej powinien być poddany przeszkoleniu w zakresie ochrony danych osobowych.
2. Za przeprowadzenie szkolenia odpowiada IOD lub osoby przez niego upoważnione.
3. Szkolenie powinno obejmować zaznajomienie pracownika z wymaganiami w zakresie ochrony danych osobowych zawartych w mających zastosowanie przepisach prawa oraz regulacjach wewnętrznych obowiązujących w InnoBaltica.

4. Każdorazowo w przypadku zmiany wymagań prawnych w zakresie ochrony danych osobowych, IOD jest zobowiązany do zapewnienia skutecznego przekazania tych zmian pracownikom spółki.
5. IOD jest zobowiązany do budowania świadomości i organizacji cyklicznych szkoleń lub kampanii informacyjnych poświęconych tematyce ochrony danych osobowych oraz podstawowych zasad bezpieczeństwa informacji. Zaleca się, aby każdy pracownik organizacji brał obowiązkowo udział w takim szkoleniu nie rzadziej niż raz na rok.
6. Opisywane powyżej szkolenia mogą odbywać się w dowolnej formie, ogólnie przyjętej u ADO.

XV. Retencja danych

1. Dane osobowe przetwarzane w InnoBaltica przechowywane są przez okres nie dłuższy niż jest to niezbędne. Okres przechowywania danych jest dostosowywany do celu, w którym zostały zebrane.
2. Okres retencji może:
   2.1. wynikać z przepisów prawa,
   2.2. zostać określony przez organ nadzorczy w zakresie ochrony danych osobowych,
   2.3. być ustalany przez komórki organizacyjne będące właścicielami przetwarzanych danych osobowych,
   2.4. lub wynikać z zapisów konkretnej umowy.
3. Wskazany przez komórkę organizacyjną okres retencji jest weryfikowany i akceptowany przez IOD.
4. Okres retencji danych osobowych odnotowany jest w Rejestrze czynności przetwarzania w stosunku do określonej kategorii i celu, w jakim dane osobowe zostały zebrane.
5. W przypadku dokumentacji w formie papierowej za zniszczenie danych po ustaniu okresu retencji odpowiedzialny jest każdy pracownik przetwarzający te dane. Dane powinny zostać zniszczone przy użyciu niszczarki spełniającej wymagania trzeciego stopnia poufności zgodnie z normą DIN 32757. Proces ten może zostać zlecony na zewnątrz organizacji.
6. W przypadku danych osobowych przetwarzanych w systemach teleinformatycznych, każdy pracownik przetwarzający te dane jest odpowiedzialny, w miarę możliwości, za usunięcie tych danych lub zgłoszenie potrzeby ich usunięcia (dowolną drogą – jak w p. XII.2) do IOD. Na podstawie tego wniosku IOD kontaktuje się z ASI w celu usunięcia danych w wersji elektronicznej.
7. Co najmniej raz w roku kierownicy komórek organizacyjnych w InnoBaltica odpowiedzialni są za przeprowadzenie weryfikacji czy cel przetwarzania danych osobowych w stosunku do danych, które przetwarzają, jest nadal aktualny oraz czy nie przetwarzają danych dłużej aniżeli zostało to określone w Rejestrze czynności przetwarzania.
8. Wyniki przeglądu są przekazywane do IOD na jego wniosek.

XVI. Zgody na przetwarzanie danych osobowych

1. W każdej sytuacji, w której nie zidentyfikowano podstawy prawnej innej niż zgoda osoby, której dane dotyczą, niezbędne jest uzyskanie takiej zgody.

2. Forma wyrażenia zgody na przetwarzanie danych osobowych jest dowolna (np. treść wiadomości e-mail, wydruk, checkbox w systemie teleinformatycznym). Forma zgody powinna gwarantować możliwość potwierdzenia uzyskania takiej zgody.
3. Brak zgody na przetwarzanie danych osobowych nie może stanowić podstawy do odmowy wykonania umowy/świadczenia usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do ich wykonania.
4. Za uzyskanie zgody na przetwarzanie danych osobowych odpowiedzialny jest pracownik pozyskujący dane osobowe od osoby, której dane dotyczą.
5. Zgoda na przetwarzanie danych osobowych powinna zawierać co najmniej:
   5.1. tożsamość ADO,
   5.2. zamierzone cele przetwarzania, dla których dane osobowe są zbierane,
   5.3. fakt wyrażenia zgody,
   5.4. informację o możliwości wycofania zgody.
6. Nie dopuszcza się sytuacji, w których łączy się zgody na przetwarzanie danych osobowych zbieranych dla spełnienia różnych celów. W przypadku zbierania danych osobowych dla kilku celów jednocześnie, należy uzyskać indywidualną zgodę dla każdego z celów.
7. W przypadku gdy zgoda dotyczy szczególnych kategorii danych (tzw. danych wrażliwych), konieczne jest zebranie jej w formie pisemnego oświadczenia od osoby, której dane dotyczą.
8. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę.
9. W przypadku uzyskania wniosku o wycofanie zgody na przetwarzanie danych osobowych, każdy pracownik jest zobowiązany do powiadomienia o tym fakcie IOD, który podejmuje właściwe kroki.
10. Wzór zgody na przetwarzanie danych osobowych stanowi załącznik nr 8 niniejszej Polityki

XVII. Załączniki

Załącznik nr 1 – Wzór Rejestru czynności przetwarzania danych osobowych

Załącznik nr 2 – Wzór Zobowiązania do zachowania poufności

Załącznik nr 3 – Wzór treści spełniającej obowiązek informacyjny

Załącznik nr 4 – Wzór Rejestru udostępnień danych osobowych

Załącznik nr 5 – Wymagania techniczne i organizacyjne wobec podmiotów, którym powierza się przetwarzanie danych osobowych

Załącznik nr 6 – Wzór umowy powierzenia danych osobowych

Załącznik nr 7 – Wzór Rejestru naruszeń ochrony danych osobowych

Załącznik nr 8 – Wzór zgody na przetwarzanie danych osobowych

Załącznik nr 9 – Procedura Zarządzania Incydentami