POLITYKA PRYWATNOŚCI I OCHRONY DANYCH OSOBOWYCH

Fundacji INTERIZON

w ramach

POMORSKIEGO KLASTRA ICT / INTERIZON

Wstęp

Niniejsza Polityka prywatności i ochrony danych osobowych przedstawia **zasady i procedury stosowane w odniesieniu do ochrony i przetwarzania danych osobowych przez Administratora**. Określa także reguły i wskazówki w sposobie zarządzania danymi oraz mechanizmy ich ochrony i udostępniania innym podmiotom współpracującym z Administratorem.

Politykę prywatności i ochrony danych stosuje się do wszelkich czynności, stanowiących w myśl przepisów prawnych, przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady ujęte w Polityce.

Rygorowi Polityki podlegają także dane powierzone Administratorowi do przetwarzania na podstawie umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego oraz dane osobowe, które zostały Administratorowi udostępnione.

Słownik pojęć używanych w dokumencie

1. **Administrator** – oznacza Administratora Danych Osobowych w rozumieniu RODO, którym jest

   Fundacja INTERIZON z siedzibą w Gdańsku, przy ul. Trzy Lipy 3, 80-172 Gdańsk, wpisana przez Sąd Rejonowy Gdańsk-Północ w Gdańsku VII Wydział Krajowego Rejestru Sądowego do rejestru przedsiębiorców oraz rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej KRS pod nr 0000454776, REGON: 221853817, NIP: 9571068390;

   Fundacja działa w ramach i na rzecz Klastra INTERIZON / POMORSKIEGO KLASTRA ICT (dalej „Klaster"), jako podmiot celowy powołany do realizacji zadań Klastra w zakresie budowania społeczeństwa opartego na wiedzy i innowacji, rozwoju sieci współpracy, partnerstwa przedsiębiorców i innych podmiotów z instytucjami otoczenia biznesu oraz z instytucjami edukacyjnymi, w charakterze Administratora i Koordynatora Klastra na mocy Umowy partnerstwa Klastra z dnia 29.10.2009r. oraz Umowy trójstronnej (z Politechniką Gdańską) z dnia 10.07.2013r., zmienionej Aneksem z 01.03.2016r. oraz w związku z realizacją przyjętej Strategii Klastra (głównie celów: 1.Rozwoj innowacyjnych produktów i usług w ramach interdyscyplinarnych projektów; 2.Nowe możliwości biznesowe; 3.Konkurencyjność na poziomie krajowym i międzynarodowym).
2. **Dane osobowe** - – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"), gdzie poprzez możliwą do zidentyfikowania osobę fizyczną rozumie się osobę, 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.
3. **Państwo trzecie** - państwo nienależące do Europejskiego Obszaru Gospodarczego.
4. **Podmiot przetwarzający/ Procesor** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora.
5. **Polityka** – niniejszy dokument ustanawiający zasady ochrony danych osobowych.
6. **Pracownik** – osoba współpracująca z Administratorem Danych na podstawie umowy o pracę lub umowy cywilnoprawnej.

7. **Przetwarzanie** - operacja 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,
8. **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),
9. **Ustawa** - Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2019 r., poz. 1781).

1. Obowiązku Administratora

Za przetwarzanie danych osobowych w jednostce Administratora, w ramach Klastra INTERIZON oraz ich ochronę odpowiada Administrator. **Zgodnie z wytycznymi RODO i Ustawy, na dzień sporządzenia niniejszego dokumentu u Administratora nie powstaje obowiązek powołania inspektora ochrony danych osobowych (IOD).** Na odrębnych zasadach, osobami odpowiedzialnymi za przetwarzanie danych są osoby upoważnione do przetwarzania danych osobowych.

Administrator jest odpowiedzialny za:

- zapewnienie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z określonymi zasadami przetwarzania danych osobowych (zgodnie z RODO)
- zapewnienie środków umożliwiających prawidłową realizację praw osób, których dane dotyczą
- prowadzenie rejestru przetwarzania danych osobowych
- (w)prowadzenie odpowiednich polityk, procedur ochrony danych osobowych,
- prowadzenie rejestru kategorii przetwarzania danych osobowych,
- współpracę z organem nadzorczym,
- wdrożenie odpowiednich środków organizacyjnych i technicznych, aby zapewnić stopień bezpieczeństwa odpowiadający istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą,
- zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu oraz osobie, której dane dotyczą w sytuacji zaistnienia przesłanek,
- nadawanie upoważnień osobom (realizującym prace na rzecz Klastra) do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych,
- dokumentowanie wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych.

2. Ogólne zasady przetwarzania danych osobowych

W każdym przypadku, w którym dochodzi do przetwarzania danych osobowych, winny być one przetwarzane zgodnie z zasadami określonymi w art. 5 RODO, tj.

- Zgodnie z prawem – w oparciu o odpowiednią przesłankę przetwarzania zawartą w art. 6 lub 9 RODO,
- Zgodnie z zasadą rzetelności, czyli z uwzględnieniem interesów podmiotu danych,
- Zgodnie z zasadą przejrzystości,
- W konkretnych, wyraźnych i prawnie uzasadnionych celach,
- Zgodnie z zasadą minimalizacji danych, czyli adekwatnie stosownie do tego, co niezbędne do celów, w których dane są przetwarzane,
- Zgodnie z zasadą prawidłowości, czyli uwzględniając ich prawidłowość i uaktualnianie w razie potrzeby,
- Zgodnie z zasadą ograniczonego przetwarzania, czyli przez okres nie dłuższy, który jest niezbędny dla osiągnięcia celów przetwarzania,
- Zgodnie z zasadą integralności i poufności, czyli zapewniając bezpieczeństwo i ochronę danych.

3. Zakres ochrony i przetwarzania danych

Ochroną objęte są wszystkie dane osobowe w zasobach danych Administratora i przetwarzane są przez Administratora wg zasad określonych w niniejszej Polityce, bez względu na to jaką formę przybiera dany zasób danych (papierowo czy elektronicznie, rozproszony czy scentralizowany).

Zgodnie z art. 30 RODO, Administrator prowadzi *Rejestr czynności przetwarzania danych osobowych*, zawierając w nim następujące informacje:

- nazwę oraz dane kontaktowe Administratora oraz wszelkich współadministratorów,
- nazwę czynności przetwarzania i jednostkę organizacyjną,
- cel przetwarzania (na podstawie art. 30 ust. 1 pkt. b RODO),
- kategorie osób, których dane są przetwarzane (na podstawie art. 30 ust. 1 pkt. c RODO),
- kategorie danych (na podstawie art. 30 ust. 1 pkt. C RODO),
- podstawę prawną przetwarzania danych,
- źródło danych,
- wskazanie planowanego terminu usunięcia danych, jeśli jest to możliwe (na podstawie art. 30 ust 1 pkt 1 RODO),
- wskazanie, czy dane są przetwarzane przez podmiot przetwarzający wraz ze wskazaniem jego adresu (art. 30 ust 1 pkt. d RODO)
- kategorie odbiorców (innych niż podmiot przetwarzający) (na podstawie art. 30 ust 1 pkt 6 RODO),
- nazwę systemu lub oprogramowania – dla danych przetwarzanych w systemie/oprogramowaniu,
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa jest to możliwe,
- DPIA - ocena skutków dla ochrony danych (jeśli tak, lokalizacja raportu)
- gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń.

Powyższy rejestr prowadzony jest przez Administratora w formie elektronicznej. W przypadku żądania zgłoszonego przez organ nadzoru Administrator ujawni prowadzony przez siebie rejestr.

4. Ogólne zasady bezpieczeństwa ochrony danych osobowych

1. Dostęp do danych osobowych mają jedynie pracownicy lub osoby współpracujące z Administratorem na podstawie stosunku prawnego innego niż umowa o pracę (dalej pracownicy) tylko i wyłącznie na podstawie udzielonego upoważnienia do przetwarzania danych.
2. Osoby nieuprawnione do przebywania w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne jedynie w obecności osoby posiadającej upoważnienie.
3. Pracownicy zobowiązani są do zachowania w tajemnicy wszelkich informacji o przetwarzanych danych osobowych w tym również o środkach stosowanych do zabezpieczeń i sposobach ich ochrony.
4. Pracownicy zobowiązani są do zabezpieczenia dokumentów, materiałów zawierających w swojej treści dane osobowe i nie udostępniania ich osobom nie upoważnionym. Ponadto zabronione jest udzielanie informacji dotyczących danych osobowych innym podmiotom na podstawie próśb w jakiejkolwiek formie (pisemnej, telefonicznej, ustnej itd.) bez ważnej podstawy prawnej.
5. Niedopuszczalnym jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych.
6. Hasła i identyfikatory służące pracownikowi do indywidualnego logowania do systemu informatycznego lub innego w miejscu pracy nie może być udostępnione innej osobie.
7. Wiadomości wysyłane do wielu osób wymaga zastosowania opcji „kopia ukryta".
8. Pracownicy zobowiązani są w miejscu pracy do stosowania zasady tzw. Czystego biurka, która cechuje się niepozostawianiem materiałów, dokumentów zawierających dane osobowe w miejscu, w którym osoby nieupoważnione mogą mieć dostęp do danych. Ponadto pracownicy zobowiązani są do niszczenia notatek na brudno, błędnych lub zbędnych kopii dokumentacji w sposób uniemożliwiający jej odtworzenie np. poprzez użycie niszczarki.
9. W czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe.
10. Po zakończeniu pracy w systemie informatycznym, w którym przetwarzane są dane osobowe należy się z niego skutecznie wylogować.

5. Osoby upoważnione do przetwarzania danych osobowych

Wyłącznie upoważnione przez Administratora osoby fizyczne mogą mieć dostęp oraz uprawnienie do przetwarzania danych osobowych.

Administrator w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie osobom, które uzyskały uprzednie, stosowne upoważnienie do przetwarzania danych osobowych.

Upoważnienie do przetwarzania danych osobowych nadawane jest w formie pisemnej, po przeprowadzeniu szkolenia lub zaznajomieniu w innej formie, osoby upoważnianej z zasadami ochrony danych osobowych obowiązującymi w strukturze Administratora.

Upoważnienia do przetwarzania danych osobowych są indywidualne oraz wskazują zbiory danych objęte upoważnieniem.

Upoważnienie do przetwarzania danych osobowych zawiera zobowiązanie do zachowania ich w poufności, oraz oświadczenie o zapoznaniu się z zasadami ochrony danych osobowych, ustanowionymi zwłaszcza w niniejszej Polityce ochrony danych.

Osoby posiadające nadane przez Administratora upoważnienie do przetwarzania danych osobowych zobowiązane są do ich ochrony zgodnie z przepisami powszechnie obowiązującymi i niniejszym dokumentem. Ponadto osoba upoważniona zobowiązana jest do zachowania w tajemnicy informacji o danych osobowych oraz środkach, sposobach ich ochrony i zabezpieczeniach.

Naruszenie obowiązku ochrony danych osobowych m.in. obowiązku zachowania w tajemnicy skutkuje poniesieniem odpowiedzialności karnej oraz stanowi ciężkie naruszenie obowiązków umownych, (pracowniczych lub z tytułu innej umowy, na podstawie której osoba ta świadczy pracę).

Upoważnienia do przetwarzania danych osobowych rejestrowane są *Ewidencji osób upoważnionych* do przetwarzania danych osobowych, która prowadzone jest przez Administratora.

6. Udostępnienie danych osobowych

Administrator dopuszcza, by dane osobowe, których jest administratorem były przekazywane innym administratorom w formie udostępnienia danych, zgodnie z przepisami prawa oraz zapewniając, aby udostępnienie danych osobowych nastąpiło w oparciu o co najmniej jedną przesłankę spośród wskazanych w art. 6 RODO i/lub art. 9 RODO.

Podmioty lub kategorie podmiotów, którym udostępnia się dane osobowe muszą zostać obligatoryjnie wskazane w *Rejestrze czynności przetwarzania danych osobowych*.

7. Powierzenie danych osobowych

W sytuacjach uzasadnionych i zgodnych z przepisami RODO i Ustawy, Administrator może przekazać podmiotowi zewnętrznemu do przetwarzania w jego imieniu dane osobowe których jest Administratorem, na podstawie wiążącego aktu prawnego, tj. co do zasady na mocy zawartej umowy powierzenia przetwarzania danych osobowych, lub wyjątkowo na podstawie innego instrumentu prawnego, podlegającemu prawu UE lub prawu państwa członkowskiego UE.

Umowa powierzenia przetwarzania danych osobowych powinna odpowiadać postanowieniom art. 28 RODO tj. winna określać:

- przedmiot powierzenia
- czas trwania powierzenia
- charakter i cel przetwarzania danych
- rodzaj powierzanych danych
- kategorie osób, których danych dotyczą
- warunki podpowierzenia przetwarzania danych
- obowiązki i prawa Administratora danych
- obowiązki podmiotu przetwarzającego

Umowa powierzenia danych osobowych może zostać zawarta w formie pisemnej, w tym również elektronicznej. Umowa powierzenia przetwarzania danych osobowych podpisywana jest zgodnie z zasadami reprezentacji Administratora Danych lub udzielonymi pełnomocnictwami.

Przed zawarciem ww. umowy i przed przekazaniem danych osobowym Podmiotowi przetwarzającemu, celem spełnienia obowiązku (art. 28 ust. 1 RODO) korzystania wyłącznie z podmiotów, które

zapewniają wystarczającą gwarancję wdrożenia odpowiednich środków technicznych i organizacyjnych dla ochrony przetwarzania danych osobowych, niezbędne jest poddanie tego podmiotu analizie pod kątem prawidłowości przetwarzania danych osobowych zgodnie z przepisami powszechnie obowiązującymi. Do wykonania takiej analizy wykorzystuje się ustandaryzowaną na potrzeby Administratora *Ankietę oceny procesora*.

Prawidłowość przetwarzania przez Podmiot przetwarzający winna być na bieżąco monitorowana, m.in. poddają go sprawdzeniu zgodnie z ww. Ankietą co najmniej raz w roku. Ponadto, Administrator winien wykonywać prawo kontroli Podmiotu przetwarzającego na zasadach, jakie strony określiły w zawartej Umowie powierzenia przetwarzania danych osobowych.

Powierzenie danych osobowych zostaje odnotowane w *Rejestrze czynności przetwarzania* danych osobowych Administratora.

Administrator może również przetwarzać dane osobowe powierzone przez podmioty, na rzecz których świadczy usługi. Przyjęcie takich danych osobowych winno również poprzedzać zawarcie umowy powierzenia przetwarzania danych osobowych oraz zostać odnotowane w Rejestrze przetwarzania – w ramach kategorii czynności przetwarzania danych osobowych.

Podmiot przetwarzający nie powinien korzystać z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora na podpowierzenie Szczegółowe zasady ewentualnego podpowiedzenia winny zostać uregulowane w umowie powierzenia lub w osobnym dokumencie sporządzonym w formie pisemnej, w tym również elektronicznej.

Administrator zapewnia, iż umowy powierzenia przetwarzania danych osobowych są zawierane na przejrzystych i ustandaryzowanych zasadach, w oparciu o przyjęty u Administratora wzór uregulowań w tym względzie, dostosowując go do określonej sytuacji powierzenia przetwarzania, tak aby zapewnić właściwą ochronę danych.

8. Przekazywanie danych osobowych do państw trzecich

W przypadku przekazywania przez Administratora danych osobowych do Państwa trzeciego lub organizacji międzynarodowej, konieczne jest spełnienie warunków określonych w Rozdziale V RODO. Wskazany warunek dotyczy również takiego przekazania danych osobowych przez Podmiot przetwarzający dane na rzecz Administratora.

Przekazanie danych do Państw trzecich lub organizacji międzynarodowej może mieć formę udostępnienia danych, jak i powierzenia danych osobowych.

Przekazanie danych osobowych do Państwa trzeciego może nastąpić w sytuacji, jeżeli Komisja Europejska wydała decyzję, że dane państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Wówczas takie przekazanie nie wymaga specjalnego zezwolenia.

W razie braku decyzji Komisji Europejskiej Administrator może przekazać dane osobowe do Państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy podmiot ten zapewni iż posiada odpowiednie zabezpieczenia i pod warunkiem, że obowiązują prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej.

Odpowiednie zabezpieczenia Administrator może zapewnić, bez konieczności uzyskania zezwolenia ze strony organu nadzorczego, za pomocą:

- prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi,
- wiążących reguł korporacyjnych zatwierdzonych przez organ nadzorczy, mających zastosowanie do każdego z członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą,

- standardowych klauzul ochrony danych przyjętych lub zatwierdzonych przez Komisję Europejską,
- standardowych klauzul ochrony danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję Europejską,
- zatwierdzonego kodeksu postępowania wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą, lub
- zatwierdzonego mechanizmu certyfikacji wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą.

Z zastrzeżeniem zezwolenia właściwego organu nadzorczego odpowiednie zabezpieczenia, o których powyżej Administrator Danych może zapewnić w szczególności za pomocą:

- klauzul umownych między Administratorem Danych lub podmiotem przetwarzającym a Administratorem Danych, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej, lub
- postanowień uzgodnień administracyjnych między organami lub podmiotami publicznymi, w których przewidziane będą egzekwowalne i skuteczne prawa osób, których dane dotyczą.

W przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony wydawanej przez Komisję Europejską lub braku odpowiednich zabezpieczeń wskazanych powyżej, w tym wiążących reguł korporacyjnych, jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej jest możliwe jedynie pod warunkiem, że:

- osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którymi może się dla niej wiązać proponowane przekazanie, wyrazi na nie wyraźną zgodę,
- przekazanie jest niezbędne do wykonania umowy zawartej z osobą, której dane dotyczą,
- przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą,
- przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,
- przekazanie jest niezbędne ze względu na posiadane roszczenia,
- przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą lub
- przekazanie nastąpi z publicznego rejestru.

9. Współadministrowanie danymi osobowymi.

W zakresie swojej działalności Administrator dopuszcza możliwość przyjęcia współadministrowania danymi osobowymi z innym podmiotem/podmiotami.

Współadministrowanie danymi zachodzi wówczas, gdy co najmniej dwóch administratorów wspólnie podejmuje decyzje dotyczące celów i środków przetwarzania danych. Podmioty te powinny spełniać trzy warunki:

- być administratorem danych, na zasadzie art. 4 pkt 7 RODO,
- wspólnie ustalać cele przetwarzania danych osobowych,
- wspólnie ustalać techniczne i organizacyjne sposoby przetwarzania danych osobowych.

Współadministratorzy danych w drodze wspólnych uzgodnień określają w sposób przejrzysty zakresy swojej odpowiedzialności w zakresie obowiązków wynikających z RODO.

Współadministratorzy winny zawrzeć stosowną umowę o współadministrowaniu, zakreślając odpowiednio (tj. adekwatnie do uzgodnionego zakresu obowiązków) zakresy swojej odpowiedzialności dotyczącej wypełnienia obowiązków wynikających z RODO i Ustawy (w szczególności obowiązek informacyjny poprzez przekazywanie Klauzuli informacyjnej RODO), jako że zasadnicza część uzgodnień między współadministratorami winna być dostępna podmiotom, których dane dotyczą (art. 26 ust. 2 RODO).

10. Audyt zgodności przetwarzania danych osobowych

Audyt zgodności przetwarzania danych osobowych przeprowadzany jest w celu sprawdzenia stosowanych w jednostce organizacyjnej rozwiązań technicznych i organizacyjnych służących przetwarzaniu i ochronie danych osobowych pod kątem skuteczności oraz spełnienia wymogów wynikających z przepisów przez osobę wyznaczoną przez Administratora .

Audyt przeprowadzany jest raz do roku w terminie do końca roku.

Osoba upoważniona do przeprowadzenia audytu dokumentuje czynności przeprowadzone w toku sprawdzenia, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz sporządza Sprawozdanie z audytu. Dokumentowanie może polegać, w szczególności, na utrwaleniu danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych na informatycznym nośniku danych lub dokonaniu wydruku tych danych oraz na:

- sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
- odebraniu wyjaśnień osoby, której czynności objęto sprawdzeniem;
- sporządzeniu kopii otrzymanego dokumentu;
- sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;
- sporządzeniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu

Sprawozdanie z audytu, powinno zawierać:

- oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania;
- datę i miejsce sprawozdania
- imię i nazwisko administratora bezpieczeństwa informacji (jeśli został powołany);
- wykaz czynności podjętych przez osobę upoważnioną do przeprowadzenia audytu w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach;
- datę rozpoczęcia i zakończenia sprawdzenia;
- określenie przedmiotu i zakresu sprawdzenia;
- opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
- stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem;
- wyszczególnienie załączników stanowiących składową część sprawozdania;
- podpis osoby upoważnionej do przeprowadzenia audytu informacji,

Sprawozdanie jest sporządzane w postaci elektronicznej albo w postaci papierowej. Osoba upoważniona do sporządzenia sprawozdania przekazuje Administratorowi sprawozdanie nie później niż w terminie 30 dni od zakończenia audytu.

11. Realizacja paw osób, których dane dotyczą

Administrator uwzględnia w zachodzących w jego strukturze procesach przetwarzania danych osobowych, procedury i zasady ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy przepisów RODO, w tym, w szczególności

- prawo do wycofania wyrażonej zgody (art. 7 ust. 3 RODO),
- prawo dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO),
- prawo do sprostowania danych (art. 16 RODO),
- prawo do usunięcia danych (*prawo do bycia zapomnianym*) (art. 17 RODO),
- prawo do ograniczenia przetwarzania (art. 18 RODO),
- prawo do przenoszenia danych (art. 20 RODO),
- prawo sprzeciwu (art. 21 RODO),
- prawo do niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu (art. 22 RODO).

12. Ochrona danych osobowych w fazie projektowania oraz domyślna ochrona danych osobowych

Administrator uwzględnia ochronę danych osobowych i ich prywatności na każdym etapie tworzenia oraz istnienia technologii obejmującej ich przetwarzanie. Oznacza to, iż zasady ochrony prywatności będą „wbudowane" w każdy projekt zakładający przetwarzanie danych osobowych w taki sposób, aby od samego początku jego istnienia ochrona prywatności stanowiła jego część składową. Dodatkowo ustawienia aplikacji czy systemów przetwarzających dane domyślnie powinny udostępniać minimalną ilość informacji o użytkowniku.

Wdrażając odpowiednie środki techniczne i organizacyjne, aby dokonywać ochrony przetwarzania danych i ich prywatności, jak m.in. pseudonimizacja, anonimizacja czy też minimalizacja w dokonywaniu przetwarzania danych, Administrator uwzględnia

- stan wiedzy technicznej
- koszt wdrożenia
- charakter, zakres, kontekst i cele przetwarzania danych
- ryzyko naruszenia praw lub wolności osób fizycznych o różnych prawdopodobieństwie wystąpienia i wadze zagrożenia wynikającego z przetwarzania.

Zastosowane środki techniczne i organizacyjne zapewniają również, aby dane osobowe nie były udostępniane nieokreślonej licznie osób.

Administrator wykazuje, iż spełnia swoje obowiązki odpowiednio je dokumentując np. w formie notatki, e-maila, raportu, wydruku z systemu.

13. Ocena skutków dla ochrony danych osobowych (Data Protection Impact Assessment)

W sytuacjach uzasadnionych okolicznościami i obowiązującymi przepisami, Administrator na zasadach określonych przepisami RODO, oraz w wykazaniu wypełnienia obowiązku rozliczalności, dokonuje

oceny skutków dla ochrony danych osobowych w celu opisania przetwarzania danych osobowych oraz oceny, konieczności i proporcjonalności.

14. Incydent ochrony danych osobowych

Administrator osobowych jest podmiotem odpowiedzialnym za bezpieczeństwo przetwarzanych danych osobowych. Aby zapobiec naruszeniom Administrator czynnie przeciwdziała dostępowi osób niepowołanych do pomieszczeń oraz systemów, w których przetwarzane są dane osobowe oraz podejmowania działań w przypadku wystąpienia naruszeń ochrony danych osobowych.

W przypadku naruszenia ochrony danych osobowych, skutkującego obowiązkiem notyfikacji do organu nadzorczego, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu. W przypadku przekroczenia 72 godzinnego terminu do zgłoszenia załącza się wyjaśnienie przyczyn opóźnienia.

Zgłoszenie powinno zawierać co najmniej:

- opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorię i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
- opisywać środki zastosowane lub proponowane przez Administratora Danych w celu zaradzeniu naruszenia ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków

Administrator może odstąpić od zgłoszenia w sytuacji gdy mało prawdopodobne jest, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze, poprzez *Rejestr przypadków naruszenia*.

15. Przeglądy i aktualizacja Polityki

Osoba upoważniona przez Administratora dokonuje w razie potrzeby, nie rzadziej jednak niż raz na dwa lata okresowego przeglądu niniejszej Polityki pod kątem jej adekwatności w stosunku do procesów funkcjonujących w strukturach Administratora i Klastra INTERIZON oraz obowiązujących przepisów prawa odnoszących się do ochrony danych osobowych.

Ponadto weryfikacji Polityki dokonuje się niezwłocznie w przypadku zmian przepisów prawa.

.....

podpis Administratora Danych