POLITYKA BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH OSOBOWYCH
FUNDACJI WISŁA WARSZAWIE

Fundacja Wisła Warszawie

Adres: ul. Morszyńska 63, 02-925 Warszawa

KRS: 0000560498

NIP: 5213698257

zwana dalej „Fundacja Wisła Warszawie" lub „Administrator Danych Osobowych"

Data i miejsce sporządzenia dokumentu:	2018.07.10
Podpis Administratora Danych Osobowych:	Konrad Zatonski

1. Źródło wymagań

    1.1. Realizując postanowienia Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz stworzonych w oparciu o nie aktów prawnych w zakresie ochrony danych osobowych (dalej RODO) wprowadza się w ramach Fundacji Wisła Warszawie zestaw reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej pozwalający na zapewnienie ochrony danych osobowych.

2. Cel Polityki Bezpieczeństwa Danych Osobowych

    2.1. Celem niniejszego dokumentu jest zapewnienie ochrony danych osobowych przed wszelkiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

3. Definicje

Przez użyte w niniejszym dokumencie określenia należy rozumieć:

Administrator Danych Osobowych/ Administrator	Fundacja Wisła Warszawie z siedzibą w Warszawie (02-925), ul. Morszyńska 63, wpisana do rejestru stowarzyszeń Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m.st. Warszawy z siedzibą w Warszawie, XIII Wydział Gospodarczy KRS pod numerem KRS: 0000560498, NIP: 5213698257, REGON: 361653610;
administrator systemu	osoba nadzorująca pracę systemu informatycznego używanego w ramach Fundacji Wisła Warszawie oraz wykonująca w nim czynności wymagające specjalnych uprawnień
baza danych osobowych	zbiór uporządkowanych i powiązanych ze sobą tematycznie zapisanych w systemie danych; baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe
dane osobowe (dane)	wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
dane szczególnej kategorii	wszelkie informacje o przekonaniach filozoficznych, przynależności wyznaniowej, przynależności partyjnej, dane biometryczne, genetyczne, o preferencjach seksualnych i stanie zdrowia
działanie korygujące	działanie przeprowadzane w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji
działanie zapobiegawcze	działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej
incydent	naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność
Instrukcja	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
kontrola	systematyczna, niezależna i udokumentowana ocena skuteczności systemu ochrony danych osobowych, na podstawie wymagań ustawowych, niniejszej Polityki i Instrukcji
korekcja	działanie w celu wyeliminowania skutków incydentu
nośnik komputerowy (wymienny)	nośnik służący do zapisu i przechowywania informacji np. CD, dyskietki, dyski twarde
osoba uprawniona	osoba, której dane są przetwarzane
Polityka Bezpieczeństwa / Polityka	niniejsza Polityka Bezpieczeństwa przetwarzania danych osobowych obowiązująca i stosowana w ramach Fundacji Wisła Warszawie
prawo do bycia zapomnianym	prawo do zgłoszenia Administratorowi wniosku w przedmiocie trwałego usunięcia danych osobowych z systemu
przetwarzanie danych	wykonywanie jakichkolwiek operacji na danych osobowych np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie

RODO	Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 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
system informatyczny (system)	zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych
Ustawa	krajowa regulacja w zakresie ochronie danych osobowych
usuwanie danych	zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą
użytkownik	osoba posiadająca uprawnienia do pracy w systemie informatycznym zgodnie ze swoim zakresem obowiązków
zabezpieczenie systemu informatycznego	wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem, także pozyskaniem danych osobowych lub ich utratą
zagrożenie	potencjalna możliwość wystąpienia incydentu
zbiór danych	zestaw danych osobowych posiadający określoną strukturę, prowadzony według określonych kryteriów oraz celów
zgoda osoby, której dane dotyczą	oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana na podstawie oświadczenia woli o innej treści

4. Dokumenty powiązane

Jako Załącznik do niniejszej Polityki opracowano i wdrożono Instrukcję Zarządzania Systemem Informatycznym w ramach Fundacji Wisła Warszawie. Określa ona sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa.

5. Bezpieczeństwo przetwarzania danych osobowych

5.1. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez samych użytkowników systemu.

5.2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

5.2.1. integralność i poufność danych - rozumianą jako właściwość zapewniającą, że dane osobowe przetwarzane są w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych,

5.2.2. rozliczalność danych - rozumianą jako właściwość zapewniającą, że Administrator Danych Osobowych jest w stanie wykazać przestrzeganie zasad dotyczących ochrony danych osobowych,

5.2.3. integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji nim, zarówno zamierzonej, jak i przypadkowej.

5.2.4. zgodność z prawem, rzetelność i przejrzystość – rozumianą jako właściwość zapewniającą, że przetwarzanie następuje zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,

5.2.5. ograniczenie celu – rozumiane jako zbieranie danych osobowych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzanie dalej w sposób niezgodny z tymi celami,

5.2.6. minimalizację danych – rozumianą jako właściwość zapewniającą, że zbierane dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,

5.2.7. prawidłowość danych – rozumianą jako właściwość zapewniającą, że zbierane dane osobowe są prawidłowe i w razie potrzeby uaktualniane,

5.2.8. ograniczenie przechowywania – rozumiane jako przechowywanie danych osobowych w formie umożliwiającą identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane są przetwarzane.

5.3. W zakresie przedmiotowym Politykę niniejszą stosuje się do danych osobowych przetwarzanych w systemie informatycznym Fundacji Wisła Warszawie oraz danych osobowych zapisanych na zewnętrznych nośnikach informacji oraz informacji dotyczących bezpieczeństwa przetwarzania danych osobowych, w szczególności dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.

5.4. W zakresie podmiotowym, Polityka obowiązuje wszystkich pracowników Fundacji Wisła Warszawie oraz inne osoby mające dostęp do danych osobowych, w tym osoby współpracujące z Fundacją Wisła Warszawie na podstawie innej umowy cywilnoprawnej.

6. Poziom bezpieczeństwa

6.1. Przy przetwarzaniu danych osobowych należy stosować wysoki poziom bezpieczeństwa w rozumieniu art. 32 RODO, ponieważ urządzenia systemu służącego do przetwarzania danych osobowych połączone są z siecią publiczną.

7. Zarządzanie ochroną danych osobowych

7.1. Podstawowe zasady

7.1.1. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z obowiązkami służbowymi oraz rolą sprawowaną w procesie przetwarzania danych w ramach Fundacji Wisła Warszawie.

7.1.2. Każda z osób mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia.

7.1.3. Należy zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych.

7.1.4. Należy stosować adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa przetwarzania danych osobowych.

7.2. Procedury postępowania z danymi osobowymi

7.2.1. Dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.

7.2.2. Dane osobowe należy przetwarzać wyłącznie za pomocą autoryzowanych urządzeń służbowych.

7.3. Upoważnienie do przetwarzania danych osobowych

7.3.1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby o których mowa w treści art. 4 pkt. 10 RODO, posiadające upoważnienie nadane na mocy art. 28 ust. 3 lit. b w zw. z art. 32 ust. 4 RODO.

7.3.2. Upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych przez Administratora Danych Osobowych.

7.3.3. W celu upoważnienia do przetwarzania danych osobowych należy dostarczyć do Administratora Danych Osobowych podpisane oświadczenie, którego wzór stanowią Załączniki: nr 5., nr 6., nr 7. lub nr 8.

7.3.4. Na podstawie otrzymanego oświadczenia Administrator Danych Osobowych upoważnia formalnie wnioskującego do przetwarzania danych osobowych i wydaje upoważnienie sporządzane wg wzoru stanowiącego Załącznik nr 4. do niniejszej Polityki.

7.3.5. Upoważnienia, o których mowa powyżej, przechowywane są w aktach osobowych pracownika i obowiązują do czasu ustania stosunku pracy lub obowiązków związanych z przetwarzaniem danych osobowych (Załącznik nr 18. - Archiwum upoważnień, oświadczeń pracowników oraz zmian w ewidencjach).

7.4. Ewidencja osób upoważnionych

7.4.1. Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona przez Administratora Danych Osobowych w postaci dokumentu - Załącznik nr 9. Ewidencja osób upoważnionych do przetwarzania danych osobowych.

7.4.2. Przełożeni osób upoważnionych odpowiadają za natychmiastowe zgłoszenie do Administratora Danych Osobowych osób, które utraciły uprawnienia dostępu do danych osobowych.

7.5. Zachowanie danych osobowych w tajemnicy

7.5.1. Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których uzyskały dostęp w trakcie zatrudnienia, również po ustaniu zatrudnienia.

7.6. Znajomość regulacji wewnętrznych

7.6.1. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są zapoznać się z regulacjami wewnętrznymi dotyczącymi ochrony danych osobowych w ramach Fundacji Wisła Warszawie, w szczególności z niniejszą Polityką oraz Instrukcją.

7.7. Zgodność

7.7.1. Niniejsza Polityka powinna być aktualizowana w ramach Fundacji Wisła Warszawie wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.

7.7.2. Okresowy przegląd Polityki powinien mieć na celu stwierdzenie czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności Fundacji Wisła Warszawie oraz stanowi prawnemu aktualnemu w momencie dokonywania przeglądu.

7.7.3. Zmiany niniejszej Polityki wymagają przeglądu innych dokumentów dotyczących ochrony danych osobowych obowiązujących w ramach Fundacji Wisła Warszawie.

8. Ewidencja obszarów przetwarzania, zbiorów danych oraz oprogramowania

8.1. Prowadzona jest ewidencja obszarów przetwarzania, zbiorów danych i oprogramowania, na którą składa się:

8.1.1. wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowe,

8.1.2. wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,

8.1.3. opis przepływu danych pomiędzy poszczególnymi systemami,

8.1.4. opis struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi.

8.2. Ewidencja stanowi Załącznik nr 10.

9. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

9.1. Zabezpieczenia organizacyjne w ramach Fundacji Wisła Warszawie:

9.1.1. Została opracowana i wdrożona Polityka;

9.1.2. Została opracowana i wdrożona Instrukcja;

9.1.3. Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające ważne upoważnienia nadane przez Administratora Danych Osobowych;

9.1.4. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;

9.1.5. Osoby zatrudnione przy przetwarzaniu danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;

9.1.6. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;

9.1.7. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;

9.1.8. Przebywanie osób nieupoważnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności i pod nadzorem osoby upoważnionej do

przetwarzania danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;

9.1.9. Stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe;

9.1.10. Prowadzony jest rejestr czynności przetwarzania (Załącznik nr 11 – Rejestr czynności przetwarzania danych osobowych) i rejestr kategorii czynności przetwarzania (Załącznik nr 12 – Rejestr kategorii czynności przetwarzania danych osobowych).

9.2. Zabezpieczenia ochrony fizycznej danych osobowych:

9.2.1. Zabezpieczenia fizyczne opisane są w Załączniku nr 10. - Ewidencja zbiorów, pomieszczeń i przepływów.

9.3. Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

9.3.1. Zabezpieczenia sprzętowe stosuje się dla fizycznych elementów systemu informatycznego, ich połączeń oraz systemów operacyjnych. Szczegółowy opis zabezpieczeń zawarty jest w Instrukcji.

9.4. Zabezpieczenia narzędzi programowych i baz danych:

9.4.1. Zabezpieczenia (techniczne i programowe) stosuje się dla procedur, aplikacji, programów i innych narzędzi programowych przetwarzających dane osobowe. Szczegółowy opis zabezpieczeń zawarty jest w Instrukcji.

10. Szkolenia użytkowników

10.1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej, winien być poddany przeszkoleniu w zakresie ochrony danych osobowych zgodnie z nadawanym upoważnieniem.

10.2. Za przeprowadzenie szkolenia odpowiada Administrator Danych Osobowych, a za jego zorganizowanie odpowiada przełożony szkolonych użytkowników.

10.3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami obowiązujące Ustawy o ochronie danych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Polityką i Instrukcją obowiązującymi w ramach Fundacji Wisła Warszawie, a także o zobowiązaniu się do ich przestrzegania.

10.4. Szkolenie zostaje zakończone podpisaniem przez słuchacza Oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.

10.5. Dokument ten jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

11. Zarządzanie usługami zewnętrznymi

11.1. Bezpieczeństwo usług zewnętrznych

11.1.1. Fundacja Wisła Warszawie zapewnia, aby usługi zewnętrzne były prowadzone wyłącznie zgodnie z wymaganiami bezpieczeństwa przetwarzania danych osobowych obowiązującymi w ramach Fundacji Wisła Warszawie oraz wymaganiami powszechnie obowiązującego prawa.

11.1.2. Wymagania bezpieczeństwa przetwarzania danych osobowych, zakres usług oraz poziom ich dostarczania należy określić w umowie świadczenia usług.

11.1.3. Powierzanie przetwarzania danych osobowych może mieć miejsce wyłącznie na podstawie umowy określającej w szczególności zakres i cel przetwarzania danych.

11.1.4. Umowa musi określać również zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy. Co więcej, Umowa określa przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa Administratora Danych Osobowych.

11.1.5. Powierzenie przetwarzania danych osobowych musi uwzględniać wymogi określone w art. 5 i art. 32 RODO. W szczególności podmiot zewnętrzny, któremu ma zostać powierzone przetwarzanie danych osobowych, jest obowiązany przed rozpoczęciem przetwarzania danych do podjęcia środków zabezpieczających dane osobowe zgodnie z art. 28 RODO oraz uwzględniać zobowiązanie podmiotu zewnętrznego do zastosowania odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo oraz odpowiedni poziom ochrony danych.

11.1.6. Powierzenie przetwarzania danych osobowych nie oznacza zwolnienia z odpowiedzialności Fundacji Wisła Warszawie za zgodne z prawem przetwarzanie powierzonych danych, co wymaga w umowach stanowiących podstawę powierzenia przetwarzania danych umieszczenia prawa Fundacji Wisła Warszawie do kontroli wykonania przedmiotu umowy w siedzibie podmiotu zewnętrznego m. in. w zakresie przestrzegania obowiązujących regulacji wewnętrznych, umów i właściwych przepisów prawa.

11.1.7. Stosowana w ramach Fundacji Wisła Warszawie Umowa powierzenia (której wzór stanowi Załącznik nr 19.) przetwarzania danych osobowych stanowi w szczególności, że podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie Fundacji Wisła Warszawie, co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba, że obowiązek taki nakłada na niego prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje Fundację Wisła Warszawie o tym obowiązku prawnym, o ile prawo to nie zabrania udzielenia takiej informacji z uwagi na ważny interes publiczny;

11.1.8. Podmiot przetwarzający:

11.1.8.1. zapewnia, że osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;

11.1.8.2. podejmuje wszelkie środki wymagane na mocy powszechnie obowiązujących przepisów prawa;

11.1.8.3. biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Fundacji Wisła Warszawie poprzez odpowiednie środki techniczne i organizacyjne, wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw;

11.1.8.4. uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Fundacji Wisła Warszawie wywiązać się z obowiązków nałożonych na Administratora Danych Osobowych przez powszechnie obowiązujące przepisy prawa;

11.1.8.5. po zakończeniu świadczenia usług związanych z przetwarzaniem, zależnie od decyzji Fundacji Wisła Warszawie, usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazuje przechowywanie danych osobowych;

11.1.8.6. udostępnia Fundacji Wisła Warszawie wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w powszechnie obowiązujących przepisach prawa oraz umożliwia Fundacji Wisła Warszawie lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

11.1.8.7. dokonuje podpowierzenia przetwarzania danych osobowych w oparciu o pisemną zgodę Fundacji Wisła Warszawie zarówno w przypadku zgody blankietowej jak i w przypadku zgody udzielonej przez Administratora na korzystanie z usług określonym podmiotom; informuje Fundację Wisła Warszawie o wszelkich zmianach w tym zakresie;

11.1.8.8. prowadzi rejestr przetwarzania powierzonych danych osobowych (Załącznik nr 2 rejestr podmiotów, którym zostało powierzone przetwarzanie danych osobowych),

11.1.8.9. prowadzi rejestr incydentów (Załącznik nr 16 – Ewidencja naruszeń ochrony danych osobowych oraz ocenę skutków przetwarzania w szczególności w związku z sytuacji z przetwarzaniem danych z użyciem nowych technologii oraz w sytuacji przetwarzania danych w ramach profilowania).

12. Udostępnianie danych osobowych

12.1. Fundacja Wisła Warszawie udostępnia dane osobowe na wniosek osoby uprawnionej lub innych podmiotów w wypadkach w określonych przepisami prawa.

12.2. Zgłoszenie wniosku w przedmiocie udostępnienia danych osobowych może być złożone drogą:

- elektroniczną na adres: fundacja@wislawarszawie.pl,
- drogą listowną na adres: ul. Morszyńska 63, 02-925 Warszawa.

12.3. Osoba uprawniona, wnosząc o realizację prawa do udostępnienia danych wskazuje czy chce:

12.3.1. uzyskać informację o fakcie przetwarzania jej danych osobowych;

12.3.2. skorzystać ze swojego prawa w zakresie dostępu do danych osobowych;

12.3.3. otrzymać kopię swoich danych osobowych.

12.4. Administrator Danych Osobowych po otrzymaniu zgłoszenia:

12.4.1. może zwrócić się o uzupełnienie wniosku w terminie 2 dni;

12.4.2. potwierdza otrzymanie wniosku odnośnie dostępu do danych oraz informuje, w jakim terminie prawo dostępu do danych zostanie zrealizowane;

12.4.3. dokonuje weryfikacji tożsamości żądającej dostępu osoby, której dane dotyczą, w szczególności w kontekście usług internetowych i identyfikatorów internetowych.

12.5. Fundacja Wisła Warszawie w ramach realizacji prawa dostępu do danych, na wniosek osoby uprawnionej, zapewnia:

12.5.1. zdalny dostęp do danych;

12.5.2. możliwość uzyskania kopii danych, w tym kopii elektronicznych;

12.5.3. selekcjonowanie danych, zgodnie z wnioskiem uprawnionego.

12.6. Realizacja prawa dostępu do danych przez Administratora nie może naruszać tajemnicy handlowej lub własności intelektualnej, w szczególności praw autorskich chroniących oprogramowanie.

12.7. Fundacja Wisła Warszawie udostępnia dane osobowe, zgodnie ze zgłoszonym wnioskiem w zakresie:

12.7.1. celów przetwarzania;

12.7.2. kategorii odnośnych danych osobowych;

12.7.3. informacji o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;

12.7.4. informacji o planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

12.7.5. informacji o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;

12.7.6. informacji o prawie wniesienia skargi do organu nadzorczego;

12.7.7. informacji o źródle, z którego zostały zebrane dane w przypadku, uzyskania danych osobowych od podmiotu innego niż osoba uprawniona;

12.7.8. informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą (Załącznik nr 13 – Klauzula informacyjna związana z przetwarzaniem danych w ramach profilowania).

12.7.9. informacji o stosowanych zabezpieczeniach w zakresie przetwarzania danych osobowych w przypadku, gdy dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej.

12.8. Administrator udostępniając dane osobowe osobie uprawnionej oraz innym podmiotom odnotowuje fakt udostępnienia bezpośrednio w systemie informatycznym z którego udostępniono dane lub w inny zatwierdzony sposób.

12.9. Odnotowaniu podlegają informacje odnośnie odbiorcy danych, dacie i zakresie udostępnionych danych osobowych Załącznik nr 3 – Ewidencja udostępniania danych osobowych.

12.10. Udostępniając dane osobowe innym podmiotom należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

13. Monitorowanie i przegląd usług strony trzeciej.

13.1. Monitorowanie usług strony trzeciej powinno być udokumentowane i powinno zawierać informacje o: poziomie wykonania usługi, incydentach bezpieczeństwa teleinformatycznego oraz ochrony danych osobowych, śladach audytowych, problemach operacyjnych, awariach, błędach i zakłóceniach.

14. Prawo do bycia zapomnianym

14.1. Administrator na wniosek osoby uprawnionej, w określonych przypadkach, jest zobowiązany do usunięcia jej danych osobowych (prawo do bycia zapomnianym).

14.2. Zgłoszenie wniosku w przedmiocie usunięcia danych osobowych może być złożone drogą:

- elektroniczną na adres: fundacja@wislawarszawie.pl,
- drogą listowną na adres: ul. Morszyńska 63, 02-925 Warszawa.

14.3. Przesłanka dla usunięcia danych osobowych przez Fundację Wisła Warszawie na wniosek, może być fakt, iż:

14.3.1. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

14.3.2. osoba, której dane dotyczą, cofnęła zgodę, na której opierało się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;

14.3.3. osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania dotyczących jej danych osobowych:

14.3.4. wniosek o usuniecie danych wynika z przyczyn związanych ze szczególną sytuacją osoby uprawnionej – wobec przetwarzania dotyczących jej danych osobowych opartego na interesie publicznym lub prawnie uzasadnionych interesach i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;

14.3.5. przetwarzanie danych osobowych obywało się w ramach marketingu bezpośredniego;

14.3.6. dane osobowe były przetwarzane niezgodnie z prawem;

14.3.7. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;

14.3.8. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 RODO;

14.3.9. zgoda wyrażona została przez podmiot, który już nie jest dzieckiem.

14.4. Fundacja Wisła Warszawie po otrzymaniu wniosku o usunięcie danych może zwrócić się do osoby uprawnionej o uzupełnienie wniosku w terminie 2 dni. Potwierdza także otrzymanie wniosku o usunięciu danych oraz informuje w jakim terminie prawo do bycia zapomnianym zostanie zrealizowane.

14.5. Fundacja Wisła Warszawie weryfikuje wskazane przez osobę uprawnioną podstawy prawne jak i samą osobę wnioskodawcy i w razie potrzeby zwraca się o wyjaśnienie.

14.6. Po pozytywnej analizie, Fundacja Wisła Warszawie usuwa dane osobowe osoby uprawnionej zarówno z systemu informatycznego jak i z istniejących i dokonywanych kopii zapasowych.

14.7. W przypadku, gdy dane osobowe, które zostały objęte procedurą prawa do bycia zapomnianym zostały upublicznione Fundacji Wisła Warszawie podejmie działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, że został zgłoszony wniosek o usuniecie danych, celem usunięcia przez administratorów wszelkich łączy do tych danych, kopii lub ich replikacji.

14.8. Fundacja Wisła Warszawie odmawia uwzględnienia wniosku w zakresie usunięcia danych wówczas, gdy dalsze przetwarzanie danych jest niezbędne:

14.8.1. do korzystania z prawa do wolności wypowiedzi i informacji;

14.8.2. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

14.8.3. z uwagi na cele zdrowotne;

14.8.4. z uwagi na interes publiczny w dziedzinie zdrowia publicznego;

14.8.5. do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych;

14.8.6. do ustalenia, dochodzenia lub obrony roszczeń.

15. Prawo do ograniczenia przetwarzania danych

15.1. Fundacja Wisła Warszawie realizuje także na wniosek osoby uprawnionej prawo do ograniczenia przetwarzania danych osobowych.

15.2. Zgłoszenie wniosku w przedmiocie ograniczenia przetwarzania danych osobowych może być złożone drogą:

- elektroniczną na adres: fundacja@wislawarszawie.pl,
- drogą listowną na adres: ul. Morszyńska 63, 02-925 Warszawa.

15.3. Przesłanką dla ograniczenia przetwarzania danych osobowych przez Fundację Wisła Warszawie może być fakt, iż:

15.3.1. osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;

15.3.2. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;

15.3.3. administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

15.3.4. osoba, której dane dotyczą, wniosła sprzeciw z przyczyn związanych z jej szczególną sytuacją, wobec przetwarzania dotyczących jej danych osobowych opartego na interesie publicznym lub prawnie uzasadnionych interesach.

15.4. Fakt ograniczenia przetwarzania danych osobowych przez Fundację Wisła Warszawie zostanie wyraźnie zaznaczony w systemie Fundacji Wisła Warszawie.

15.5. W przypadku, gdy przetwarzanie zostało ograniczone, przetwarza takie dane osobowe, z wyjątkiem przechowywania:

15.5.1. za zgodą osoby, której dane dotyczą;

15.5.2. w celu ustalenia, dochodzenia lub obrony roszczeń;

15.5.3. w celu ochrony praw innej osoby fizycznej lub prawnej;

15.5.4. z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

15.6. Fundacja Wisła Warszawie wprowadzając ograniczenie w zakresie przetwarzania danych osobowych stosuje:

15.6.1. czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania,

15.6.2. środki uniemożliwiające użytkownikom dostępu do wybranych danych,

15.6.3. dokonuje czasowego usunięcie opublikowanych danych ze strony internetowej.

16. Prawo przenoszenia danych

16.1. Na wniosek osoby uprawnionej Fundacja Wisła Warszawie gwarantuje realizację prawa do przenoszenia danych osobowych, w przypadku, gdy podstawą przetwarzania danych osobowych jest:

16.1.1. zgoda;

16.1.2. umowa,

16.1.3. okoliczność przetwarzania danych osobowych w sposób zautomatyzowany.

16.2. Zgłoszenie wniosku w przedmiocie przeniesienia danych osobowych może być złożone drogą:

- elektroniczną na adres: fundacja@wislawarszawie.pl,
- drogą listowną na adres: ul. Morszyńska 63, 02-925 Warszawa.

16.3. Wniosek o przeniesienie danych złożony przez osobę uprawnioną może dotyczyć:

16.3.1. wydania osobie uprawnionej zgromadzonych na jej temat danych osobowych w ustrukturyzowanym, powszechnie używanym formacie, nadającym się do odczytu maszynowego, celem samodzielnego przekazania danych przez osobę uprawnioną innemu administratorowi,

16.3.2. przekazania zgromadzonych danych osobowych osoby uprawnionej innemu administratorowi.

16.4. Fundacja Wisła Warszawie po otrzymaniu wniosku o przeniesienie danych realizuje uprawnienie na rzecz osoby uprawnionej w terminie 1 miesiąca, jeśli jest to technicznie możliwe lub odmawia w sytuacji, gdyby łączyło się to z nadmiernymi kosztami lub prowadziłoby do naruszenia praw innych osób uprawnionych.

17. Obowiązki informacyjne

17.1. Fundacja Wisła Warszawie dokonując przetwarzania danych zgodnie z art. 13 ust. 1 i 2 RODO przed dokonaniem przetwarzania przekazuje podmiotom uprawnionym informacje odnośnie:

17.1.1. nazwy i forma prawnej Fundacji Wisła Warszawie jako administratora danych osobowych (dalej ADO); w tym dane dotyczące numeru KRS, numeru NIP, numeru REGON;

17.1.2. danych Inspektora Danych osobowych, w tym numeru telefonu oraz adresu e-mail;

17.1.3. informacje odnośnie podstawy przetwarzania danych osobowych: np.: zgody przetwarzanego, decyzji organu, uzasadnionego interesu ADO, inne.

17.1.4. celu przetwarzania danych osobowych;

17.1.5. odbiorców danych osobowych;

17.1.6. możliwości uzyskania dostępu do danych;

17.1.7. możliwości uzyskania kopii w zakresie danych osobowych przekazywanych do Państw trzecich;

17.1.8. prawa dostępu do swoich danych, poprawiania, zmienia ich i uzupełniania, prawa do wniesienia sprzeciwu w zakresie przetwarzania, prawa do przenoszenia danych, prawa do cofnięcia zgody na przetwarzanie., złożenia wniosku o usunięcie danych;

17.1.9. czasu przez jaki dane będą przetwarzane lub przez czas objęty określonym zdarzeniem;

17.1.10. przysługującego uprawnienia w przedmiocie wniesienia skargi do organu nadzoru, w przypadku zaistnienia zagrożenia przetwarzane danych osobowych niezgodnie z prawem;

17.1.11. obowiązku przekazania danych osobowych wraz z informacją prawa odmowy w tym zakresie (ustawa/umowa/ warunek zawarcia umowy);

17.1.12. przetwarzania danych w sposób zautomatyzowany w formie profilowania,

17.1.13. przekazywania danych osobowych do Państwa trzecich.

17.2. Treść danych przekazywanych osobie uprawnionej w ramach Klauzuli informacyjnej stanowi Załącznik nr 13. do Polityki.

18. Obowiązek informacyjny związany z profilowaniem

18.1. Fundacja Wisła Warszawie w przypadku przetwarzaniem danych osobowych w związku z profilowaniem realizuje wymagane przez RODO obowiązki informacyjne wobec osoby uprawnionej.

18.2. Fundacja Wisła Warszawie dokonując profilowania informuje osobę, której dane dotyczą, o fakcie profilowania oraz o konsekwencjach takiego profilowania, a także o możliwości złożenia sprzeciwu wobec profilowania przed przystąpieniem do profilowania.

18.3. Stosowana przez Fundację Wisła Warszawie klauzula informacyjna stanowi Załącznik nr 13.

19. Ocena ryzyka i przeglądy

19.1. Ocena ryzyka

19.1.1. Systemy informatyczne i aplikacje powinny być poddawane ocenie ryzyka pod kątem identyfikacji zagrożeń dla bezpieczeństwa przetwarzania danych osobowych nie rzadziej niż jeden raz w miesiącu.

19.1.2. Narzędzia informatyczne służące do oceny ryzyka bezpieczeństwa przetwarzania danych powinny być chronione przed nieautoryzowanym lub nieuprawnionym dostępem a ich użycie odpowiednio kontrolowane.

19.2. Przeglądy bezpieczeństwa

19.2.1. Przeglądy bezpieczeństwa przetwarzania danych osobowych powinny być przeprowadzane okresowo, nie rzadziej niż jeden raz w miesiącu w celu określenia wymaganego poziomu zabezpieczeń pozwalającego na ograniczenie ryzyka do poziomu akceptowalnego.

19.2.2. Narzędzia informatyczne służące do przeprowadzania przeglądów bezpieczeństwa przetwarzania danych osobowych powinny być chronione przed nieautoryzowanym lub nieuprawnionym dostępem a ich użycie odpowiednio kontrolowane.

19.3. Fundacja Wisła Warszawie przeprowadzi ocenę skutków przetwarzania danych przetwarzania w sytuacji:

19.3.1. podejmowania działań związanych z prowadzeniem systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osoby uprawnione,

19.3.2. przetwarzania na dużą skalę szczególne kategorii danych osobowych - danych wrażliwych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa,

19.3.3. systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie,

19.3.4. prowadzenia cen lub punktacji, w tym profilowania i prognozowania w szczególności na podstawie „aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą,

19.3.5. automatycznego podejmowania decyzji o skutku prawnym lub podobnie znaczącym skutku,

19.3.6. dopasowywania lub łączenia zbiorów danych np. pochodzących z, co najmniej dwóch operacji przetwarzania danych przeprowadzonych w różnych celach lub przez różnych administratorów danych w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą

19.3.7. innowacyjnego wykorzystania lub stosowania nowych rozwiązań technologicznych lub organizacyjnych, takich jak połączenie technologii

19.4. Fundacja Wisła Warszawie stosuje następujące kryteria oceny skutków ochrony danych dopuszczalnych (w zależności od sytuacji) poprzez:

19.4.1. zapewnienie systematycznego opisu operacji przetwarzania z uwzględnieniem charakteru, zakresu, kontekstu oraz celów przetwarzania;

19.4.2. prowadzenie rejestru przetwarzania zawierającego dane osobowe, informacje o odbiorcach i okresie przechowywania danych osobowych;

19.4.3. sporządzanie funkcjonalnych opisów operacji przetwarzania oraz identyfikacji zasobów, z którymi styczność mają dane osobowe (m.in. sprzęt komputerowy, oprogramowanie, sieci, osoby, opracowania lub kanały transmisji opracowań);

19.4.4. wskazanie środków, których podjęcie jest planowane w celu zapewnienia przestrzegania warunków związanych z bezpieczeństwem przetwarzania danych osobowych w związku z oceną skutków przetwarzania.

19.4.5. wprowadzenie środków przyczyniających się do proporcjonalności i niezbędności przetwarzania z zachowaniem prawnie uzasadnionych celów,

19.4.6. zapewnienie zgodność przetwarzania danych z prawem,

19.4.7. wprowadzeni ograniczenia w zakresie czasu przechowywania danych,

19.4.8. wprowadzenie środków przyczyniających się do zachowania praw osób, których dane dotyczą poczynając od poinformowanie osoby, której dane dotyczą, o prawie dostępu i prawie do przenoszenia danych, prawie do sprostowania i do usunięcia danych; prawie do sprzeciwu i prawo do ograniczenia przetwarzania;

19.4.9. zapewnienie wysokich standardów w zakresie powierzenia przetwarzania danych oraz przy międzynarodowym przekazywaniu danych,

19.4.10. prowadzenie niezbędnych konsultacji,

19.4.11. przeprowadzenie działania w zakresie zarządzania ryzykiem naruszenia praw i wolności osób, których dane dotyczą z uwzględnieniem źródła, charakteru, specyfiki, powagi i ryzyka;

19.4.12. zidentyfikowanie możliwych skutków dla praw i wolności osób, których dane dotyczą, w przypadku zdarzeń takich jak bezprawny dostęp, niepożądane zmiany i zniknięcie danych; o zidentyfikowano zagrożenia, które mogłyby doprowadzić do bezprawnego dostępu, niepożądanych zmian i zniknięcia danych; o oszacowano prawdopodobieństwo i powagę,

19.4.13. stosowanie środków, których podjęcie jest planowane w celu zaradzenia ryzykom.

20. Zarządzanie incydentami

20.1. Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.

20.2. Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności: nieautoryzowany dostęp do danych, nieautoryzowane modyfikacje lub zniszczenie danych, udostępnienie danych nieautoryzowanym podmiotom, nielegalne ujawnienie danych, pozyskiwanie danych z nielegalnych źródeł.

20.3. Każdy pracownik, użytkownik lub inna osoba mająca dostęp do danych, która stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązana niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu. Przełożony zgłasza fakt Administratorowi danych.

20.4. Ustala się następującą klasyfikację naruszeń:

20.4.1. Zdarzenia losowe zewnętrzne;

20.4.2. Zdarzenia losowe wewnętrzne;

20.4.3. Zdarzenia świadome lub celowe;

20.5. Typowe sytuacje, gdy ww. osoba powinna powiadomić Administratora danych:

20.5.1. ślady na drzwiach, oknach i szafach wskazują na próbę włamania;

20.5.2. dokumentacja jest niszczona bez użycia niszczarki;

20.5.3. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;

20.5.4. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

20.5.5. niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych,

20.5.6. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;

20.5.7. wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia;

20.5.8. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;

20.5.9. stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);

20.5.10. telefoniczne próby wyłudzenia danych osobowych;

20.5.11. kradzież komputerów lub twardych dysków z danymi osobowymi;

20.5.12. utrata kontroli nad kopią danych osobowych;

20.5.13. maile zachęcające do ujawnienia identyfikatora i/lub hasła;

20.5.14. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;

20.5.15. istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki"

20.5.16. hasła do systemów przechowywane są w pobliżu komputera.

20.6. Każdy pracownik, użytkownik lub inna osoba mająca dostęp do danych, która stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.

20.7. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia osoby upoważnionej przez Administratora danych.

20.8. Administrator Systemu IT jest zobowiązany do informowania Administratora danych o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

20.9. Administrator danych podejmuje następujące kroki:

20.9.1. zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy,

20.9.2. odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,

20.9.3. ocenia poziom istotności incydentu, kierując się następującymi kryteriami: wpływ incydentu na ciągłość działania organizacji, krytyczność systemów dotkniętych incydentem, wrażliwość informacji objętych incydentem, rozległość incydentu, rozmiar szkód, koszt usunięcia incydentu, szacowny czas przywrócenia ciągłości działania dotkniętego incydentem zakresu organizacji,

20.9.4. nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).

20.10. Administrator danych zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń.

20.11. Administrator danych dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając raport - Załącznik nr 17.

20.12. Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

20.13. W przypadku naruszenia ochrony danych osobowych, Administrator danych bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu

naruszenia – zgłasza je Urzędowi ochrony danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

20.14. Zgłoszenie, o którym mowa w ust. 20.12, musi co najmniej:

20.14.1. opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

20.14.2. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

20.14.3. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

20.14.4. opisywać środki zastosowane lub proponowane przez Administratora w celu zapobiegania naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach - środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

20.15. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

20.16. Administrator danych dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

20.17. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator danych bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

20.18. Zawiadomienie, o którym mowa w ust. 20.16, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w poprzednich ustępach.

20.19. Zawiadomienie, o którym mowa w ust. 20.16, nie jest wymagane, w następujących przypadkach:

20.19.1. Administrator danych wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

20.19.2. Administrator danych zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

20.19.3. wymagałoby ono niewspółmiernie dużego wysiłku.

W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

21. Transfer danych osobowych do państw trzecich

    21.1. Fundacja Wisła Warszawie w przypadku prowadzenia transferu danych osobowych do państw trzecich zachowuje wszystkie wymagania określone RODO.

    21.2. Podmioty z USA, które będą przetwarzać dane osobowe przekazywane przez Fundację Wisła Warszawie gwarantują przestrzeganie: prawa do informacji, obowiązku zapewnienia integralności danych oraz ograniczenia celu przetwarzania, prawa wyboru, zapewnienia bezpieczeństwa przetwarzania, zapewnienia dostępu do danych.

    21.3. Fundacja Wisła Warszawie w razie braku stwierdzenia odpowiedniego stopnia ochrony danych przekazywanych do państw trzecich jest zobowiązany zastosować środki rekompensujące brak ochrony danych w państwie trzecim, zapewniając osobie, której dane dotyczą, odpowiednie zabezpieczenia w postaci skorzystania z wiążących reguł korporacyjnych, standardowych klauzul ochrony danych przyjętych przez Komisję Europejską, standardowych klauzul ochrony danych przyjętych przez krajowy organ nadzorczy, klauzul umownych dopuszczonych przez organ nadzorczy.

    21.4. Dodatkowo transfer danych do państw trzecich będzie możliwy również wtedy, gdy: przekazanie jest niezbędne do zawarcia umowy, transfer jest konieczny dla ochrony żywotnych interesów osoby, której dane dotyczą, przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń.

22. Postanowienia końcowe

    22.1. Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.

    22.2. Administrator Danych Osobowych obowiązany jest zapoznać z treścią Polityki każdego Użytkownika danych.

    22.3. Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce Bezpieczeństwa dotyczą również przetwarzania danych osobowych w bazach danych osobowych prowadzonych w jakiejkolwiek innej formie.

    22.4. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.

    22.5. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub, odpowiednio, nienależytego wykonania zobowiązania.

    22.6. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

    22.7. Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z Ustawą oraz możliwości wniesienia wobec niej powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

    22.8. W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa mają zastosowanie przepisy RODO, Ustawy oraz wydane na jej podstawie akty wykonawcze.

ZAŁĄCZNIKI I POWIĄZANE DOKUMENTY

1. Dokument powiązany: Instrukcja
2. Załącznik nr 2 – Rejestr umów powierzenia przetwarzania danych osobowych
3. Załącznik nr 3 – Ewidencja udostępniania danych osobowych
4. Załącznik nr 4 – Wzór upoważnienia do przetwarzania danych osobowych
5. Załącznik nr 5 – Wzór oświadczenia pracownika
6. Załącznik nr 6 – Wzór oświadczenia zleceniobiorcy/wykonawcy dzieła
7. Załącznik nr 7 – Wzór oświadczenia podmiotu współpracującego z Fundacją Wisła Warszawie na podstawie umowy o współpracy
8. Załącznik nr 8 – Wzór oświadczenia Członka Zarządu/Członka Rady Nadzorczej
9. Załącznik nr 9 – Ewidencja osób upoważnionych do przetwarzania danych osobowych
10. Załącznik nr 10 – Ewidencja zbiorów, pomieszczeń i przepływów
11. Załącznik nr 11 – Rejestr czynności przetwarzania danych osobowych
12. Załącznik nr 12 – Rejestr kategorii czynności przetwarzania danych osobowych
13. Załącznik nr 13 – Klauzula informacyjna ogólna
14. Załącznik nr 14 – Klauzula informacyjna związana z przetwarzaniem danych w ramach profilowania.
15. Załącznik nr 15 – Struktura zbiorów
16. Załącznik nr 16 – Ewidencja naruszeń ochrony danych osobowych
17. Załącznik nr 17 - Raport z naruszenia ochrony danych
18. Załącznik nr 18 – Archiwum upoważnień, oświadczeń pracowników oraz zmian w ewidencjach.
19. Załącznik nr 19 – Umowy powierzenia danych osobowych do przetwarzania – wzór