

Załącznik nr 1 do uchwały Zarządu z dnia 11 listopada 2013
w sprawie przyjęcia polityki bezpieczeństwa danych osobowych

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W FUNDACJI MANUS

Podstawa prawna: USTAWA z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 r. Nr 101 poz. 926) z późn. zm.

§ 1

Dokument niniejszy określa środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, sposób przepływu danych pomiędzy poszczególnymi systemami, zawiera wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, a także tryb postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych w systemach informatycznych lub kartotekach, albo w sytuacji powzięcia podejrzenia o takim naruszeniu.

§ 2

Ileokroć w Polityce jest mowa o:

1. **dane osobowe** uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
2. **osobą możliwą do zidentyfikowania** jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.
3. **zbiore danych** - rozumie się przez to każdy posiadający strukturę, zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów,
4. **przetwarzaniu danych** - rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie,
5. **dane zwykłe** – dane identyfikujące osobę,
6. **dane wrażliwe** – dane sensytywne, szczególnie rodzaj danych osobowych uwzględnionych w katalogu przez Ustawodawcę,
7. **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń , programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
8. **kartotece** - rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierającej dane osobowe,
9. **administratorze danych osobowych (ADO)** - rozumie się przez to **FUNDACJĘ MANUS**
10. **administratorze bezpieczeństwa informacji (ABI)** - rozumie się przez to osobę nadzorującą przestrzeganie zasad ochrony, która jest obowiązana zastosować środki techniczne

i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną (wyznaczoną przez Zarząd),

11. **użytkownika** – rozumie się przez to osobę wyznaczoną przez Administratora lub osobę przez niego upoważnioną, uprawnioną do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym oraz kartotekach,
12. **pomieszczeniach** - rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez ADO, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem przenośnego sprzętu komputerowego oraz gromadzone w kartotekach.
13. **GIODO** – Główny Inspektor Ochrony Danych Osobowych

§ 3

1. Ochrona danych osobowych jest realizowana poprzez użytkowników.
2. Dane osobowe gromadzone są w podziale na dane „zwykłe” i „wrażliwe”.
3. ADO zobowiązany jest do:
 - wypełniania obowiązku informacyjnego wobec osób, których dane osobowe są przetwarzane,
 - uzyskania zgody osoby, których dane mają być przetwarzane na ich przetwarzanie,
 - udzielania odpowiedzi lub odmowy udzielenia odpowiedzi osobom, których dane osobowe są przetwarzane przez administratora w sytuacjach przewidzianych w przepisach prawa,
 - rozpatrywania wniosków osób, których dane są przetwarzane przez administratora w sytuacjach przewidzianych w przepisach prawa,
 - dokonania zgłoszenia zbiorów danych osobowych, które będą przetwarzane w instytucji Generalnego Inspektora Ochrony Danych Osobowych (GIODO), w sytuacji podlegania obowiązkowi rejestracyjnemu.
4. Zastosowane zabezpieczenia gwarantują: poufność danych, ich integralność, rozliczalność oraz integralność systemu i uwierzytelnianie.
5. Realizację § 3 ust. 2 powinny zagwarantować następujące działania :
 - stosowanie procedur określających postępowanie użytkowników oraz ich odpowiedzialność za bezpieczeństwo tych danych,
 - przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych,
 - przypisanie użytkownikom identyfikatorów (np. hasło, identyfikatory), zapewniających dostęp do różnych poziomów baz danych osobowych – stosownie do indywidualnego zakresu upoważnienia,
 - podejmowanie niezbędnych działań w celu likwidacji ewentualnych zagrożeń,
 - okresowe sprawdzanie wdrożonych metod postępowania.

§ 6

1. Każdy nowy użytkownik - przed dopuszczeniem do dostępu do danych osobowych – podlega przeszkoleniu w zakresie przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków. Wszyscy użytkownicy podlegają okresowym szkoleniom, stosownie do potrzeb .
2. Za organizację szkoleń, odpowiedzialny jest ABI.

§ 7

1. Do podstawowych zabezpieczeń przed naruszeniem ochrony danych osobowych należą: wyposażenie pomieszczenia w zamykaną szafę, zabezpieczenie wejścia zamkami.
2. Dokumenty zawierające dane osobowe są przechowywane wyłącznie w przeznaczonych do tego pomieszczeniach
3. Kartoteki przechowywane są w przeznaczonych do tego szafach, do których dostęp mają wyłącznie użytkownicy.
4. Wyznaczone pomieszczenia gwarantują prawidłową ochronę i zabezpieczenie przez wglądem osób nieupoważnionych :
 - pomieszczenia, szafki i biurka, w których przechowywane są wydruki zawierające dane osobowe, są zamykane na klucz, dostęp do nich posiadają wyłącznie użytkownicy,
 - pomieszczenia zabezpiecza się przed dostępem osób nieupoważnionych,

§ 8

1. Przetwarzanie danych osobowych z użyciem stacjonarnego i przenośnego sprzętu komputerowego oraz karotek odbywa się wyłącznie na obszarze wyznaczonym przez ADO.
2. Przetwarzanie danych osobowych za pomoc urządzeń przenośnych może odbywać się poza obszarem przetwarzania danych wyłącznie za zgodą ABI.
3. Szczegółowy wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar w którym przetwarzane są dane osobowe określa **załącznik Nr 1** do niniejszego dokumentu.

§ 9

1. Stosuje się następujące zabezpieczenia:
 - drzwi wejściowe mogą być otwierane przez uprawnione osoby,
 - pomieszczenia, w których gromadzone są dane osobowe posiadają system ochrony przeciwpożarowej, budynku pilnuje firma ochroniarska, które regularnie sprawdza pomieszczenia, klucze pobierane są w całodobowej portierni przez osoby upoważnione, parter budynku jest wyposażony w monitoring wizyjny.
 - przebywanie osób trzecich w pomieszczeniach może odbywać się wyłącznie w obecności użytkowników lub za zgodą ADO.

§ 10

ABI jest odpowiedzialny za całość zagadnień dotyczących ochrony i bezpieczeństwa danych osobowych. Przeprowadza on okresowe kontrole i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad postępowania w przypadku naruszenia ochrony danych osobowych.

§ 12

Szczegółowy wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania określa **załącznik Nr 2** do niniejszego dokumentu.

§ 13

Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, określa **załącznik nr 3** do Polityki.

§ 14

1. Każdy użytkownik zobowiązany jest sprawdzać stanu urządzeń komputerowych oraz dokonywać oględzin swojego stanowiska pracy, każdorazowo przed przystąpieniem do pracy.
2. W przypadku stwierdzenia naruszenia ochrony danych osobowych lub takiej ewentualności, użytkownik zobowiązany jest do bezwzględnego powiadomienia o tym ABI.
3. Po powiadomieniu, do czasu przybycia ABI, użytkownik powstrzymuje się od rozpoczęcia lub kontynuowania pracy, zabezpiecza elementy systemu informatycznego lub kartotek oraz podejmuje inne niezbędne czynności, stosownie do zaistniałych okoliczności.
4. W przypadku stwierdzenia naruszenia ochrony danych osobowych lub takiej ewentualności, ABI ocenia zaistniałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, a także identyfikuje wielkość negatywnych następstw incydentu, wysłuchuje relacji osoby, która dokonała powiadomienia oraz podejmuje decyzje o toku dalszego postępowania.
5. ABI sporządza raport opisujący zdarzenie.
6. ABI podejmuje kroki zmierzające do likwidacji naruszeń zabezpieczeń danych osobowych i zapobieżenia wystąpieniu ich w przyszłości.

§ 15

1. Każdy użytkownik zobowiązany jest złożyć oświadczenie, z którego wynika, że został zaznajomiony z przepisami ustawy o ochronie danych osobowych, wydanymi na jej podstawie aktami wykonawczymi, obowiązującą Polityką bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Wzór oświadczenia, określa załącznik Nr 4 .
2. ADO zobowiązany jest prowadzić i aktualizować Rejestr osób upoważnionych do przetwarzania danych osobowych w Fundacji MANUS. Rejestr stanowi załącznik E.

§ 16

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych.
2. Użytkownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.

Spis załączników:

- A. Szczegółowy wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar w którym przetwarzane są dane osobowe
- B. Szczegółowy wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania
- C. Opis struktury zbiorów danych osobowych
- D. OŚWIADCZENIE osób upoważnionych do przetwarzania danych
- E. Rejestr osób upoważnionych do przetwarzania danych osobowych w Fundacji MANUS