POLITYKA BEZPIECZEŃSTWA
OCHRONY DANYCH OSOBOWYCH
W ZIARN-POL Sp. z o.o.

Data publikacji: 01.02.2018r

Sporządził: Karolina Mertin – Administrator Bezpieczeństwa Informacji

Zatwierdził: Ryszard Szczukowski – Prezes Spółki

Grzegorz Sowa – Wiceprezes Spółki

Podpis, data

Rejestr zmian w dokumencie

Wersja	Data	Opracował	Opis nowelizacji
II	25.05.2018	Karolina Mertin	Dodano: Załącznik nr 14

Spis treści

Cel wprowadzania Polityki Bezpieczeństwa

Niniejszy dokument określa zasady bezpieczeństwa przetwarzania danych osobowych jakie muszą być przestrzegane i stosowane w ZIARN-POL Sp. z o.o. przez pracowników i współpracowników, którzy przetwarzają dane osobowe.

Stosowanie zasad określonych w niniejszym dokumencie ma na celu zapewnienie prawidłowej ochrony danych osobowych przetwarzanych przez ZIARN-POL Sp. z o.o. rozumianej jako ochronę danych przed ich udostępnieniem osobom nieuprawnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.

Zakres stosowania Polityki Bezpieczeństwa

Politykę stosuje się do danych osobowych przetwarzanych w systemie informatycznym, danych osobowych zapisanych na zewnętrznych nośnikach informacji oraz informacji dotyczących bezpieczeństwa przetwarzania danych osobowych, w szczególności dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.

W zakresie podmiotowym Polityka obowiązuje wszystkich pracowników ZIARN-POL Sp. z o.o. oraz inne osoby mające dostęp do danych osobowych, w tym stażystów, osoby zatrudnione na umowę zlecenia lub umowę o dzieło.

Wykaz skrótów zastosowanych w dokumencie

Polityka bezpieczeństwa danych osobowych: zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych (zwana dalej „Polityką")

Administrator danych: Przetwarzający, albo podmiot, który zawarł z przetwarzającym Umowę o powierzeniu przetwarzania danych osobowych. W tym przypadku administratorem danych jest ZIARN-POL Sp. z o.o.

GIODO – Generalny Inspektor Ochrony Danych Osobowych

ABI – Administrator Bezpieczeństwa Informacji – osoba wyznaczona przez Kierownictwo, odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzanie są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.

Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania 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.

Przetwarzanie danych: jakiekolwiek operacje wykonywane na danych osobowych takie jak: utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie a zawłaszcza te, które wykonuje się w systemach informatycznych.

Kierownictwo – Zarząd ZIARN-POL Sp. z o.o.

Osoba upoważniona – osoba posiadająca formalne upoważnienie wydane przez Administratora danych lub przez osobę przez niego wyznaczoną, do przetwarzania danych osobowych.

Ustawa – Ustawa z dnia 29 sierpnia 1997r o ochronie danych osobowych (tj. Dz.U. z 2002r., Nr 101, poz. 926 z późn, zm.).

Zbiór danych osobowych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, prowadzony w systemie informatycznym lub poza nim, w szczególności w formie kartoteki, skorowidza, księgi, wykazu, lub innego zbioru ewidencyjnego.

Deklaracja Kierownictwa

Informacja jest jednym z najważniejszych zasobów spółki ZIARN-POL Sp. z o.o., dlatego powinna być chroniona na każdym szczeblu organizacji. Zarząd spółki ZIARN-POL Sp. z o.o. zobowiązuje się do podejmowania niezbędnych działań mających na celu zapewnienie ochrony informacji na pożądanym poziomie, poprzez bezpośredni udział w tworzeniu Polityki bezpieczeństwa informacji , a tym samym spełnienie wymaganego poziomu bezpieczeństwa systemów informacyjnych.

Zapisy zawarte w Polityce dotyczą wszystkich osób korzystających z zasobów informatycznych i nieinformatycznych: pracowników firmy ZIARN-POL Sp. z o.o. oraz osób współpracujących.

Zapisy powinny być aktualizowane przy każdym wystąpieniu zmian w systemie, ale nie rzadziej niż raz w roku.

Odpowiedzialnym za aktualizację jest Administrator Bezpieczeństwa Informacji.

Odpowiedzialność Kierownictwa

Do obowiązków Kierownictwa należy zrozumienie oraz zapewnienie świadomości bezpieczeństwa przetwarzania danych osobowych, jego problematyki oraz wymagań. Do obowiązków należy również:

- podejmowanie odpowiednich i niezbędnych kroków mających na celu zapewnienie prawidłowiej ochrony danych osobowych,
- podział zadań i obowiązków związanych z organizacją ochrony danych osobowych, w szczególności wyznaczenie Administratora Bezpieczeństwa informacji,
- wprowadzenie do stosowania procedur zapewniających prawidłowe przetwarzanie danych osobowych,
- egzekwowanie rozwoju środków bezpieczeństwa przetwarzania danych osobowych,
- poddawanie przeglądom skuteczność polityki bezpieczeństwa przetwarzania danych osobowych,
- zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia,
- zapewnienie aktualności ,adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu,
- zapewnienie niezbędnych środków potrzebnych dla zapewnienia bezpieczeństwa przetwarzania danych osobowych.

Odpowiedzialność Administratora Bezpieczeństwa Informacji

Do obowiązków Administratora Bezpieczeństwa Informacji należy nadzorowanie przestrzegania zasad ochrony danych osobowych, zarówno w systemach informatycznych, jak również w zbiorach danych osobowych prowadzonych w formie papierowej i elektronicznej. Do obowiązków należy również:

- określenie wymagań bezpieczeństwa przetwarzania danych osobowych.

Do kompetencji Administratora Bezpieczeństwa Informacji należy:

a. określenie zasad ochrony danych osobowych,
b. wnioskowanie o ukaranie osób winnych naruszenia przepisów i zasad dotyczących ochrony danych osobowych.

Do obowiązków Administratora Bezpieczeństwa Informacji należy:

a. nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych,
b. nadawanie, zmienianie oraz cofanie uprawnień do przetwarzania danych osobowych,
c. nadzór nad zapewnieniem dostosowania funkcjonalności systemów przetwarzających dane osobowe do wymogów określonych w Rozporządzeniu,
d. prowadzenie dokumentacji opisującej zastosowaną ochronę danych osobowych (niniejsza Polityka oraz wynikające z niej instrukcje i procedury) oraz zapewnienie ich publikacji i dystrybucji,
e. zapoznawanie pracowników oraz współpracowników ZIARN-POL Sp. z o.o. z przepisami i zasadami ochrony danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzaniem,
f. reprezentowanie ZIARN-POL Sp. z o.o. w kontaktach z biurem GIODO,
g. przygotowywanie zgłoszeń zbiorów danych osobowych do rejestracji w Biurze GIODO,
h. analizę sytuacji okoliczności i przyczyn, które doprowadziły do naruszenia ochrony danych osobowych i przygotowanie oraz przedstawienie Kierownictwu zaleceń i rekomendacji dotyczących eliminacji ryzyka ich ponownego wystąpienia,
i. sprawdzanie wypełnienia obowiązków technicznych i organizacyjnych związanych z ochroną danych osobowych,
j. prowadzenie pełnej dokumentacji związanej z ochroną danych osobowych,
    - ewidencję zbiorów danych osobowych,
    - ewidencję osób upoważnionych do przetwarzania danych osobowych,
    - wykaz obszarów przetwarzania danych osobowych,
    - dokumenty z audytów i przeglądów bezpieczeństwa,
    - oryginały i kopie dokumentów dotyczących ochrony danych osobowych w szczególności uchwały Kierownictwa, polityki bezpieczeństwa, instrukcje, regulaminy, procedury,
    - programy szkoleń, listę przeszkolonych osób,
    - raport z wypełnienia obowiązku informacyjnego (kopie wniosków, pism z klauzulami informacyjnymi).

Administrator Bezpieczeństwa Informacji w zakresie realizacji swoich obowiązków, ma prawo żądania od pozostałych zatrudnionych, bez względu na rangę ich stanowiska udzielenia natychmiastowej pomocy w razie stwierdzenia, że doszło do naruszenia przepisów o ochronie danych osobowych, które może skutkować postawieniem ZIARN-POL Sp. z o.o. zarzutu popełnienia przestępstw, wykazanych w Rozdziale 8 Ustawy.

Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony

danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do swojej stacji roboczej. Do obowiązków należy również:

- przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami,
- postępowania zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych,
- zachowania tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia,
- ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,
- informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe do przełożonego, który ma obowiązek poinformować Administratora Bezpieczeństwa Informacji.

Sankcje za naruszenie ochrony danych osobowych

1. Naruszenie ochrony danych osobowych przez pracownika, może skutkować postawieniem mu zarzutu popełnienia jednego z przestępstw określonych w Rozdziale 8 Ustawy lub przestępstwa określonego w Art. 266 Kodeksu Karnego. W takim przypadku zgodnie z przepisem art. 66 Kodeksu Pracy umowa o pracę z pracownikiem tymczasowo aresztowanym wygasa z upływem 3 miesięcy nieobecności pracownika w pracy z powodu tymczasowego aresztowania, chyba że pracodawca rozwiąże wcześniej bez wypowiedzenia umowę o pracę z winy pracownika.
2. Zgodnie z art. 100§2 pkt 5 Kodeksu Pracy, pracownik jest obowiązany przestrzegać tajemnicy określonej w odrębnych przepisach. Dane osobowe, którym ZIARN-POL Sp. z o.o. nadaje charakter poufny mają charakter takiej tajemnicy, a jej ujawnienie w zależności o zakresu ujawnionych danych osobowych oraz nastawienie pracownika dopuszczającego się nieuprawnionego ujawnienia danych, może mieć charakter naruszenia lub ciężkiego naruszenia obowiązków pracowniczych.
3. Pracownik dopuszczający się nieuprawnionego ujawnienia lub wykorzystania danych osobowych w sposób sprzeczny z ich przeznaczeniem (np. wykorzystania danych osobowych do celów prywatnych) czy też ich przetwarzania w sposób niezgodny z przyjętymi w ZIARN-POL Sp. z o.o. procedurami może zostać ukarany karą upomnienia lub karą nagany.
4. W razie ciężkiego naruszenia obowiązku zachowania danych osobowych w tajemnicy lub przetwarzania ich w sposób rażąco sprzeczny z przyjętymi zasadami i procedurami, ZIARN-POL Sp. z o.o. może rozwiązać bez wypowiedzenia umowę o pracę z winy pracownika.
5. Sankcje dotyczące ujawnienia poufnych danych osobowych stosuje się analogicznie do ujawnienia przez pracownika informacji dotyczących zabezpieczenia danych osobowych w ZIARN-POL Sp. z o.o.

Obowiązek informacyjny

Pracownicy zbierający dane osobowe, w szczególności na formularzach, umowach, drukach (zarówno papierowych jak i elektronicznych) odpowiadają za umieszczenie na nich klauzuli informującej o przetwarzaniu danych osobowych.

Treść klauzuli podlega uzgodnieniu z ABI

Szkolenia w zakresie ochrony danych osobowych

1. Przed rozpoczęciem przetwarzania danych osobowych, pracownik powinien zostać przeszkolony przez ABI. Zakres szkolenia powinien obejmować zaznajomienie pracownika z przepisami o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi i instrukcjami obowiązującymi Administratora Danych.
2. Za przeprowadzenie szkolenia odpowiada ABI.
3. Szkolenie powinno być powtarzane okresowo lub na żądanie, gdy zaistnieje taka potrzeba.
4. Szczegółowy zakres szkolenia ustala ABI.

Dopuszczenie osób do przetwarzania danych osobowych

1. Przetwarzanie danych osobowych jest możliwe wyłącznie po uzyskaniu przez pracownika formalnego upoważnienia do przetwarzania danych osobowych wystawionego przez Administratora Danych lub osobę przez niego upoważnioną. W tym celu przełożony pracownika przed dopuszczeniem pracownika do pracy przy przetwarzaniu danych osobowych:
    a) zapoznaje pracownika z przepisami dotyczącymi ochrony danych osobowych oraz uregulowaniami wewnętrznymi obowiązującymi w tym zakresie w ZIARN-POL Sp. z o.o.,
    b) przyjmuje od pracownika podpisane „ Oświadczenie pracownika zatrudnionego przy przetwarzaniu danych osobowych w zbiorach danych przetwarzanych przez ZIARN-POL Sp. z o.o., którego wzór stanowi **załącznik nr 1** niniejszej Polityki,
    c) wnioskuje do ABI o formalne upoważnienie pracownika do przetwarzania danych osobowych sporządzane wg wzoru niniejszej Polityki stanowiącego **Załącznik nr 2** niniejszej Polityki.
2. Oświadczenia i upoważnienia, o których mowa w ust. 1 przechowuje się w aktach osobowych pracownika lub w aktach dotyczących zawarcia i wykonania umowy ze współpracownikami.
3. Ewidencja osób upoważnionych do przetwarzania danych osobowych stanowi **Załącznik nr 3** do niniejszej Polityki.

Wymiana informacji dotyczących danych osobowych

Pracownicy oraz współpracownicy ZIARN-POL Sp. z o.o. w celu ochrony wymienianych informacji dotyczących danych osobowych powinni podczas przetwarzania uwzględnić zasady bezpieczeństwa ustalone i zakomunikowane przez ABI.

Przede wszystkim:

1. Wszelkie dane osobowe przekazywane drogą elektroniczną muszą być szyfrowane za pomocą programu szyfrującego dostępnego na każde stacji roboczej.
2. Dane osobowe przekazywane w formie tradycyjnej, papierowej, nie mogą być widoczne dla osób trzecich – nieupoważnionych.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Wykaz zbiorów danych osobowych w postaci dokumentacji papierowej i elektronicznej zawierającej dane osobowe wraz ze wskazaniem programów służących do ich przetwarzania opisany jest w **Załączniku nr 4** do niniejszej Polityki

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiazania między nimi

Opis struktury zbiorów danych osobowych przedstawiono w **Załączniku nr 5** do niniejszej Polityki

Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

Szczegółowe rozmieszczenie zbiorów dokumentacji papierowej i elektronicznej zawierającej dane osobowe opisane jest w **Załączniku nr 6** do niniejszej Polityki.

Sposób przepływu danych pomiędzy poszczególnymi systemami

Sposób przepływu danych osobowych między systemami, w których przetwarzane są dane osobowe przedstawiono w **Załączniku nr 7** do niniejszej Polityki.

Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Zabezpieczenia organizacyjne:
   a. został wyznaczony Administrator Bezpieczeństwa Informacji (ABI) nadzorujący przestrzeganie ochrony danych osobowych,
   b. została opracowana i wdrożona Polityka Bezpieczeństwa,
   c. została opracowana i wdrożona Instrukcja Zarządzania Systemem Informatycznym,
   d. do przetwarzania danych osobowych zostali dopuszczeniu wyłącznie pracownicy posiadający upoważnienia nadane przez Administratora Danych lub osobę przez niego upoważnioną,
   e. prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,
   f. osoby zatrudnione przy przetwarzaniu danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony tych danych oraz z zasadami zabezpieczeń systemu informatycznego,
   g. osoby zatrudnione przy przetwarzaniu danych osobowych zostały zobowiązane do zachowania ich w tajemnicy,
   h. przetwarzanie danych osobowych prowadzone jest w warunkach zabezpieczających je przed dostępem osób niepowołanych,
   i. stosuje się pisemnie umowy powierzenia przetwarzania danych osobowych dla współpracy ze stronami przetwarzającymi dane osobowe, których administratorem jest ZIARN-POL Sp. z o.o.

2. W celu ochrony danych osobowych stosuje się następujące zabezpieczenia fizyczne:
   a. serwer znajduje się w klimatyzowanym pomieszczeniu zabezpieczonym drzwiami, wyposażonym w zamek patentowy oraz instalację alarmową,
   b. dostęp do pomieszczeń, w których odbywa się przetwarzanie danych osobowych z użyciem stacjonarnego sprzętu komputerowego oraz przechowywane są kopie zapasowe zbiorów danych osobowych oraz programów służących do przetwarzania danych osobowych, jest zabezpieczony przed osobami postronnymi,
   c. dostęp do serwerowni posiadają wyłącznie użytkownicy upoważnieni przez Administratora Danych,
   d. serwer przetwarzający zbiory danych osobowych zabezpieczony jest przed spadkiem napięcia i zakłóceniami z sieci zasilającej,
   e. w serwerowni umieszczono gaśnicę.
3. Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej:
   a. Administrator Danych wykorzystuje zaporę sieciową w celu separacji sieci lokalnej od sieci publicznej,
   b. korzystanie z zasobów sieci wewnętrznej możliwe jest tylko po podaniu nazwy użytkownika i hasła,
   c. Administrator Danych stosuje zabezpieczenie oprogramowaniem antywirusowym oraz oprogramowaniem firewall na routerze by zminimalizować ryzyko ingerencji przez złośliwe wirusy oraz osoby niepożądane w Systemy Informatyczne i Dane Osobowe,
   d. Administrator Danych stosuje technologię VPN w celu zabezpieczenia zdalnego dostępu do systemów informatycznych.

Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

1. Poniższe postanowienia mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych jak i zbiorach nieinformatycznych.
2. Przed przystąpieniem do pracy pracownicy zobowiązani są dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.
3. Za okoliczności, które uznaje się za naruszenie lub podejrzenie naruszenia ochrony systemu przetwarzającego dane osobowe uważa się w szczególności:
   a. nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się znajdują,
   b. nieuprawnione naruszenie lub próba naruszenia poufności, integralności i rozliczalności systemu,
   c. niezamierzoną zmianę lub utratę danych zapisanych na kopiach zapasowych,
   d. nieuprawniony dostęp do danych osobowych (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
   e. udostępnienie osobom nieupoważnionym danych osobowych lub ich części,
   f. inny stan sytemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy,
   g. wydarzenia losowe obniżające poziom ochrony sytemu (np. brak zasilania lub pożar),
   h. kradzież sprzętu informatycznego lub nośników zewnętrznych zawierających dane osobowe (np. wydruków komputerowych, dyskietek, płyt CD-ROM, dysków twardych, pamięci zewnętrznych, itp.),

4. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych pracownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie ABI.
5. Do czasu przybycia ABI zgłaszający:
   a. powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,
   b. zabezpiecza elementy systemu informatycznego lub kartotek przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym,
   c. podejmuje stosownie do zaistniałej sytuacji wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
6. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych ABI z pomocą Administratora Systemu, po przybyciu na miejsce:
   a. ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe oraz stan urządzeń, a także szacuje wielkość negatywnych następstw incydentu,
   b. wysłuchuje relacji osoby, która dokonała powiadomienia oraz innych osób związanych z incydentem,
   c. podejmuje decyzję o toku dalszego postępowania, stosownie do zakresu naruszenia i zasadności podejrzenia naruszenia ochrony danych osobowych.
7. ABI sporządza raport z przebiegu zdarzenia, w którym powinny się znaleźć w szczególności informacje o:
   a. dacie i godzinie powiadomienia,
   b. sytuacji jaką zastał.
   c. podjętych działaniach i ich uzasadnieniu,
   d. stanie sytemu po podjęciu działań naprawczych,
   e. wnioskach w sprawie ograniczenia możliwości ponownego wystąpienia naruszenia ochrony danych osobowych.
8. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od ABI lub Administratora Systemu.
9. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej w ZIARN-POL Sp. z o.o. dyscypliny pracy, ABI wyjaśnia wszystkie okoliczności incydentu i podejmuje stosowne działania wobec osób, które dopuściły się wskazanego naruszenia.
10. Po zakończeniu czynności naprawczych system powinien utrzymać poziom ochrony nie niższy niż przed wystąpieniem incydentu związanego z naruszeniem ochrony danych osobowych.

Zasady ochrony danych osobowych w zbiorach nieinformatycznych

1. Zbiory nieinformatyczne powinny być odpowiednio zabezpieczone przed nieuprawnionym dostępem i zniszczeniem.
2. Dokumenty i wydruki zawierające dane osobowe należy przechowywać w zamykanych pomieszczeniach, do których dostęp mają jedynie osoby uprawnione.
3. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający ich skuteczne usunięcie lub zanonimizowanie.

Postanowienia końcowe

1. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.
2. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997r o ochronie danych osobowych (tj. Dz.U. z 2002r., Nr 101, poz. 926 z późn, zm.) oraz przepisy wykonawcze do tej Ustawy.

Spis załączników

Załącznik nr 1	Oświadczenie pracownika zatrudnionego przy przetwarzaniu danych osobowych w zbiorach danych przetwarzanych przez ZIARN-POL Sp. z o.o.
Załącznik nr 2	Upoważnienie do przetwarzania danych osobowych.
Załącznik nr 3	Ewidencja osób upoważnionych do przetwarzania danych osobowych.
Załącznik nr 4	Wykaz zbiorów danych osobowych, których Administratorem Danych jest ZIARN-POL Sp. z o.o.
Załącznik nr 5	Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych.
Załącznik nr 6	Wykaz obszarów przetwarzania danych osobowych.
Załącznik nr 7	Sposób przepływu danych.
Załącznik nr 8	Wzór aktu powołania Administratora Bezpieczeństwa Informacji.
Załącznik nr 9	Wzór umowy powierzenia przetwarzania danych osobowych.
Załącznik nr 10	Rejestr podmiotów, które powierzyły przetwarzanie danych osobowych na rzecz ZIARN-POL Sp. z o.o.
Załącznik nr 11	Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych.
Załącznik nr 12	Procedura udostępniania danych osobowych.
Załącznik nr 13	Procedura prowadzenia kontroli przetwarzania danych osobowych.
Załącznik nr 14	Wzór aktu powołania Inspektora Ochrony Danych Osobowych.