POLITYKA BEZPIECZEŃSTWA

Stowarzyszenie rodzin STX BP1 z siedzibą w Żelechowie

Spis treści

I. Wprowadzenie

Zgodnie z art. 24 ust. 1 i 2 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 („**ogólne rozporządzenie o ochronie danych**" lub „**RODO**"), uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, **administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać**. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki te powinny obejmować wdrożenie odpowiednich polityk ochrony danych.

Niniejszy dokument określa podstawowe zasady przetwarzania i zabezpieczenia danych osobowych w Stowarzyszeniu rodzin STX BP1 z siedzibą w Żelechowie.

II. Podstawowe pojęcia

§ 1

Ilekroć w niniejszym dokumencie jest mowa o:

1) **Administratorze** – należy przez to rozumieć **Stowarzyszenie rodzin STX BP1 z siedzibą w Żelechowie**, ul. Wilczyska 53, 08-430 Żelechów, decydujące o celach i sposobach przetwarzania danych osobowych;
2) **Danych osobowych** – należy przez to rozumieć informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (**osobie, której dane dotyczą**). Osobą możliwą do zidentyfikowania jest osoba, 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) **Danych wrażliwych** – należy przez to rozumieć dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, biometryczne, dotyczące zdrowia, seksualności lub orientacji seksualnej osoby, której dane dotyczą;
4) **Naruszeniu ochrony danych osobowych** – należy przez to rozumieć naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
5) **Odbiorcy danych** – należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Odbiorcą danych nie są organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z obowiązującymi przepisami prawa;
6) **Organie nadzorczym** lub **PUODO** – należy przez to rozumieć Prezesa Urzędu

Ochrony Danych Osobowych;

7) **Podmiocie przetwarzającym** – należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora na podstawie umowy o powierzenie przetwarzania danych;
8) **Polityce bezpieczeństwa** – należy przez to rozumieć niniejszą Politykę bezpieczeństwa Stowarzyszenia rodzin STX BP1 z siedzibą w Żelechowie;
9) **Współpracowniku –** należy przez to rozumieć pracownika, osobę zatrudnioną na dowolnej innej podstawie prawnej (na podstawie umowy cywilnoprawnej), współpracownika (współpraca B2B), praktykanta, stażystę, wolontariusza oraz wszelkie inne osoby stale współpracujące z Administratorem i należące do struktury organizacyjnej Administratora, jak również samego Administratora w zakresie, w jakim wykonuje poszczególne czynności z zakresu przetwarzania danych osobowych;
10) **Przetwarzaniu danych osobowych** – należy przez to rozumieć operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
11) **Upoważnionym Współpracowniku** – należy przez to rozumieć Współpracownika posiadającego pisemne upoważnienie do przetwarzania danych osobowych nadane przez Administratora;
12) **Użytkowniku** – należy przez to rozumieć użytkownika Systemu informatycznego;
13) **Zabezpieczeniu danych w systemie informatycznym** – należy przez to rozumieć wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem lub utratą;
14) **Zgodzie osoby, której dane dotyczą** – należy przez to rozumieć dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
15) **Źródła publiczne** – utworzone na podstawie przepisów obowiązującego prawa rejestry, ewidencje lub bazy, posiadające charakter jawny i powszechnie dostępny, udostępnione za pośrednictwem sieci Internet, w szczególności CEiDG, KRS, rejestr REGON, rejestr podatników VAT.

III. Uwagi ogólne

§ 2

1. Przepisy i standardy dotyczące ochrony danych osobowych podlegają dynamicznym zmianom. Administrator zobowiązuje się dokonywać okresowo przeglądu i aktualizacji Polityki bezpieczeństwa pod kątem zgodności stanu deklarowanego ze stanem faktycznym.
2. Każdy Współpracownik jest zobowiązany do zapoznania się z Polityką bezpieczeństwa oraz do jej przestrzegania. Współpracownicy, którzy zostali zapoznani z Polityką

bezpieczeństwa, potwierdzają ten fakt poprzez podpisanie oświadczenia, którego wzór stanowi **Załącznik nr 1** do Polityki bezpieczeństwa.

3. Wdrożenie Polityki bezpieczeństwa odbywa się poprzez:
   1) zapoznanie Współpracowników z treścią Polityki bezpieczeństwa oraz zobowiązanie do jej przestrzegania;
   2) systematyczne sprawdzanie znajomości wiedzy zasad określonych w Polityce bezpieczeństwa;
   3) szkolenia z zakresu ochrony danych osobowych.
4. Aktualna wersja Polityki bezpieczeństwa jest dostępna w siedzibie Administratora.
5. Wszelkie wątpliwości dotyczące sposobu interpretacji postanowień zawartych w Polityce bezpieczeństwa powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane te dotyczą.

IV. Wykaz budynków, pomieszczeń i systemów, tworzących obszar, w którym przetwarzane są dane osobowe

§ 3

1. Administrator przetwarza dane osobowe głównie w systemach informatycznym, korzystając z usług zewnętrznych firm hostingowych, dostawców usług poczty elektronicznej oraz podmiotów świadczących usługi zarządzania bazami danych.
2. Przetwarzanie danych osobowych poza obszarem przetwarzania, jest dopuszczalne za zgodą Administratora wyłącznie pod warunkiem, że dane osobowe zostały odpowiednio zabezpieczone.

V. Środki techniczne i organizacyjne służące należytemu zabezpieczeniu danych osobowych

V.1. Postanowienia ogólne

§ 4

1. Administrator stosuje środki organizacyjne i techniczne, mające na celu zapobieganie naruszeniom ochrony danych osobowych. Rozwiązania te uwzględniają charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych. Spośród stosowanych przez Administratora środków można wyróżnić:
   1) zabezpieczenia fizyczne pomieszczeń i wyposażenia;
   2) zabezpieczenia systemu informatycznego;
   3) zabezpieczenia osobowe (organizacyjne) określające obowiązki i zasady działania Administratora oraz Współpracowników.
2. Administrator ze szczególną dbałością i ostrożnością zabezpiecza dane wrażliwe, w tym dane dotyczące stanu zdrowia osób korzystających z pomocy Stowarzyszenia. Dostęp do tych informacji mają wyłącznie ci spośród Współpracowników, którym te dane są niezbędne do wykonywania obowiązków w Stowarzyszeniu.

§ 5

Administrator dąży do podnoszenia poziomu stosowanych zabezpieczeń poprzez:

1) szkolenia z zakresu ochrony danych osobowych;
2) przeprowadzanie audytów ochrony danych osobowych;
3) systematyczne sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
4) podejmowanie działań mających na celu eliminację ujawnionych naruszeń w zakresie ochrony danych osobowych;
5) monitorowanie zmian w zakresie zabezpieczania systemów informatycznych oraz wdrażanie nowych narzędzi, metod pracy lub sposobów zarządzania tym systemem.

V.2. Zabezpieczenia budynków i pomieszczeń

§ 6

1. Administrator wprowadza ogólne środki organizacyjne i techniczne służące zabezpieczeniu obszaru przetwarzania danych, w zależności od stwierdzonych potrzeb oraz w miarę możliwości technicznych i finansowych.
2. Administrator korzysta z pomieszczeń, w których są stosowane odpowiednie zabezpieczenia fizyczne.
3. Bezpośrednie zabezpieczenie obszaru przetwarzania danych jest realizowane przez Współpracowników, poprzez przestrzeganie następujących zasad:
   1) pomieszczenia obszaru przetwarzania danych zamyka się na czas nieobecności Współpracowników oraz po zakończonej pracy, w sposób uniemożliwiający dostęp osobom nieupoważnionym;
   2) szafki, w których są przechowywane dane osobowe są zamykane na klucz. Dostęp do klucza posiadają jedynie wybrani Upoważnieni Współpracownicy.
4. Dane osobowe znajdujące się w obszarze przetwarzania danych osobowych są chronione przed dostępem osób nieupoważnionych, obecnych w budynku Administratora poprzez realizacje następujących zasad:
   1) osoby nieupoważnione mogą przebywać w pomieszczeniach obszaru przetwarzania danych osobowych, a jedynie w obecności Upoważnionych Współpracowników;
   2) osoby z zewnątrz mogą przebywać tylko w wydzielonych do tego pomieszczeniach i obszarach;
   3) każdy Współpracownik jest zobowiązany zwracać uwagę na przebywanie w obszarze przetwarzania osób nieupoważnionych, które mogą stanowić potencjalne źródło niebezpieczeństwa dla danych osobowych, w szczególności osób zachowujących się nietypowo, np. zdenerwowanych, ubranych nieodpowiednio do pory dnia, roku lub pogody, przebywających bez wyraźnego celu lub potrzeby, posiadających przy sobie podejrzane bagaże lub przedmioty.

V.3. Zabezpieczenia dokumentów tradycyjnych

§ 7

1. Każdy Współpracownik ma obowiązek dbać o integralność, nienaruszalność, kompletność oraz poufność dokumentów tradycyjnych zawierających dane osobowe, do których Współpracownik ma dostęp w związku lub przy okazji

współpracy z Administratorem.

2. Współpracownik jest zobowiązany do przestrzegania następujących zasad zabezpieczania danych osobowych utrwalonych w dokumentach tradycyjnych:
   1) dokumenty tradycyjne zawierające dane osobowe należy przechowywać w przeznaczonych do tego szafkach zamykanych na klucz;
   2) dokumenty tradycyjne nie powinny być pozostawiane bez należytego dozoru w miejscach ogólnodostępnych, ciągach komunikacyjnych, holu, toaletach, pomieszczeniach socjalnych, i innych tego rodzaju pomieszczeniach;
   3) dokumentów tradycyjnych nie należy pozostawiać w miejscach, w których mogą być widoczne z zewnątrz (na fotelu w samochodzie, na parapetach);
   4) dokumenty zawierające dane osobowe nie mogą być przekazywane osobom nieupoważnionym, chyba że dokumenty te zostały należycie zabezpieczone przed dostępem osób nieupoważnionych;
   5) dokumenty archiwalne należy chronić w sposób analogiczny, jak tego samego rodzaju dokumenty bieżące (aktualne).

V.4. Zasady ochrony danych osobowych w systemie informatycznym

§ 8

1. Administrator oraz każdy Współpracownik ma obowiązek dbać o integralność, nienaruszalność, kompletność oraz poufność dokumentów i nośników elektronicznych, zawierających dane osobowe przetwarzane przez Administratora.
2. Dane osobowe w formie elektronicznej powinny być przetwarzane wyłącznie na urządzeniach i nośnikach przeznaczonych do tego przez Administratora.
3. Współpracownik może przetwarzać dane osobowe na własnych urządzeniach i nośnikach wyłącznie w zakresie i na podstawie uprzedniej zgody Administratora oraz pod warunkiem, że wykorzystywane urządzenia i nośniki zostały zaaprobowane przez Administratora pod kątem bezpieczeństwa przetwarzania danych osobowych.
4. W trakcie pracy przenośne nośniki zawierające dane osobowe należy przechowywać w miejscu niedostępnym dla osób nieupoważnionych, zaś po jej zakończeniu – w zamykanych na klucz szafach lub innych urządzeniach do przechowywania.
5. Nie należy pozostawiać na stanowisku pracy nośników informacji w czasie, gdy nie są używane.
6. Współpracownik korzystający z komputera przenośnego lub innego przenośnego nośnika informacji, na którym przechowywane są dane osobowe (np. pendrive, notes elektroniczny, dysk zewnętrzny, etc.), jest zobowiązany zachować szczególną ostrożność podczas przechowywania, użytkowania i transportu urządzenia poza obszar przetwarzania danych.
7. Na pulpicie komputera nie należy zapisywać folderów, plików lub skrótów plików zawierających dane osobowe, w szczególności dane wrażliwe.

§ 9

1. W przypadku wykonywania czynności związanych z przetwarzaniem danych osobowych w pomieszczeniach, w których przebywają osoby nieupoważnione, monitory urządzeń należy w miarę możliwości umieszczać w taki sposób, który uniemożliwia odczyt danych przez te osoby.
2. W przypadku, gdy nie jest możliwe umieszczenie monitora w sposób, o którym mowa

w ust. 1 powyżej, w czasie obecności w pomieszczeniu osób nieupoważnionych, należy zminimalizować pliki zawierające dane osobowe, uniemożliwiając w ten sposób zapoznanie się z danymi osobowymi przez te osoby.

3. Urządzenia elektroniczne zawierające dane osobowe nie mogą pozostawać bez kontroli Współpracownika. W przypadku czasowego opuszczenia stanowiska pracy w trakcie dnia pracy, Współpracownik jest zobowiązany zablokować komputer w sposób wymuszający ponowne zalogowanie.
4. Nie należy pozostawiać elektronicznych nośników danych osobowych w pomieszczeniach i miejscach, w których nie jest zapewniony należyty nadzór.
5. Przed zakończeniem pracy, Współpracownik jest zobowiązany wylogować z wykorzystywanych programów i aplikacji oraz wyłączyć komputer.
6. Urządzenia i nośniki zawierające dane osobowe powinny być transportowane w sposób zapewniający bezpieczeństwo danych osobowych, w tym w przystosowanych do tego pokrowcach lub torbach. Nośniki i sprzęt należy przewozić w taki sposób, który nie zdradza zawartości bagażu.
7. Urządzenia i nośniki nie powinny być powierzane osobom nieupoważnionym lub pozostawiane bez dozoru oraz bez należytego fizycznego zabezpieczenia.
8. Urządzenia i nośniki powinny być zabezpieczone przed dostępem osób nieupoważnionych poprzez stosowanie haseł dostępu spełniających wymagania określone w § 13 poniżej.

§ 10

1. Administrator odbiera upoważnienie do działania w systemie informatycznym na wniosek Współpracownika albo z własnej inicjatywy. Odebranie upoważnienia następuje w przypadku, gdy jest to konieczne w celu zapewnienia bezpieczeństwa danych, w razie zmiany zakresu obowiązków Współpracownika lub zakończenia współpracy ze Współpracownikiem.
2. Jeżeli jest to możliwe i nie wpłynie negatywnie na poprawne działanie systemu informatycznego lub utratę jego zasobów, w przypadku odebrania upoważnienia do przetwarzania danych osobowych w systemie informatycznym, identyfikator Współpracownika, który utracił upoważnienie jest wyrejestrowywany z systemu informatycznego.
3. Dostęp do systemu informatycznego z tzw. poziomu administratora systemu jest ograniczony do Administratora lub osoby przez niego upoważnionej.
4. W uzasadnionych przypadkach (np. konserwacja, nadzór autorski systemu informatycznego, programu, aplikacji, usunięcie błędu oprogramowania, naprawa baz lub zasobów danych itp.), dostęp do systemu informatycznego mogą uzyskać osoby z zewnętrz, z którymi Administrator zawarł umowę współpracy z odpowiednią klauzulą poufności oraz umowę powierzenia przetwarzania danych osobowych. Dostęp do systemu informatycznego, w przypadku opisanym powyżej, odbywa się na warunkach i w zakresie określonym w tych umowach.
5. Przepisy niniejszego paragrafu stosuje się, o ile wiążące Administratora zasady korzystania z poszczególnych programów informatycznych lub aplikacji nie określają w sposób odmienny procedur nadawania uprawnień.

§ 11

1. Współpracownik ma prawo do wykonywania w systemie informatycznym tylko tych

czynności, do których uzyskał uprawnienie.
2. Współpracownik ponosi odpowiedzialność za wszelkie czynności wykonywane w systemie informatycznym przy użyciu swojego identyfikatora oraz hasła.
3. Umyślne przekroczenie przyznanych uprawnień może być potraktowane jako poważne naruszenie warunków umowy, którą Współpracownik zawarł z Administratorem.
4. Współpracownik jest zobowiązany do zachowania w tajemnicy nadanych mu identyfikatorów (loginów) oraz haseł, także po ustaniu zatrudnienia lub współpracy z Administratorem. Administrator poucza Współpracownika o zakresie jego uprawnień oraz konsekwencjach nieprzestrzegania zasad, o których mowa powyżej.
5. Współpracownik może logować się do aplikacji i programów służących do przetwarzania danych osobowych Administratora przy użyciu prywatnych urządzeń wyłącznie za zgodą Administratora i po zapewnieniu bezpieczeństwa przetwarzania na tych urządzeniach.

§ 12

1. Dostęp do konta w systemie informatycznym (dostęp do komputera) powinien być zabezpieczony hasłem, które należy wpisać po uruchomieniu komputera lub po 5 minutach bezczynności. Współpracownik nie jest uprawniony usunięcia tego zabezpieczenia ani do zmiany czasu bezczynności, po upływie którego konieczne jest ponowne wpisanie hasła.
2. Hasła do systemu informatycznego powinny być regularnie zmieniane, nie rzadziej niż co 3 miesiące.
3. Administrator dąży do zapewnienia właściwości systemu informatycznego polegającej na okresowym wymuszaniu zmiany haseł. W sieciowym systemie informatycznym należy stosować mechanizmy wymuszające okresową zmianę wszelkich haseł dostępu.
4. Współpracownik odpowiada za systematyczną i terminową zmianę haseł. Tylko pierwsze hasło do systemu informatycznego i hasło do programu lub aplikacji nadaje Administrator lub osoba przez niego upoważniona i przekazuje je Współpracownikowi w sposób poufny. Po zalogowaniu się do systemu informatycznego, programu lub aplikacji Współpracownik powinien zmienić hasło na własne, zachowując odpowiednią strukturę oraz warunki tworzenia hasła, o których powyżej. Współpracownik nie może zlecić zmiany hasła innej osobie.
5. Hasło podlega niezwłocznej zmianie w przypadku odkrycia lub podejrzenia odkrycia przez osobę nieupoważnioną, w tym również przez innego Współpracownika.
6. W przypadku, gdy Współpracownik zapomni hasła, Administrator lub osoba przez niego upoważniona przydziela hasło czasowe, które Współpracownik powinien zmienić na nowe przy pierwszym uwierzytelnieniu w systemie informatycznym, programie lub aplikacji.
7. Hasła nie powinny być zapisywane lub przekazywane Współpracownikowi w postaci umożliwiającej zapoznanie się z ich treścią przez osoby nieupoważnione lub przez innego użytkownika. Hasła utrzymuje się w tajemnicy również po upływie ich ważności.
8. Współpracownik nie może udostępniać żadnego hasła innemu Współpracownikowi lub jakiejkolwiek innej osobie, chyba że Administrator lub osoba przez niego upoważniona na to zezwoli. Ujawnione w ten sposób hasło podlega zmianie w najszybszym możliwym terminie.
9. Jeżeli w systemie informatycznym istnieje właściwość umożliwiająca zapamiętanie

identyfikatora lub loginu oraz hasła, Współpracownik nie powinien korzystać z tej opcji. Powyższe nie dotyczy identyfikatora (loginu) Współpracownika i jego hasła zapisywanego w programach i aplikacjach, jeżeli system informatyczny został zabezpieczony hasłem na poziomie systemu operacyjnego.

§ 13

1. Hasła do systemu informatycznego, aplikacji lub urządzenia (nośnika) powinny składać się z co najmniej 9 znaków oraz zawierać co najmniej 1 małą i wielką literę, znak specjalny oraz cyfrę. Hasło nie może stanowić powtórzenia wcześniej użytego hasła.
2. Hasła powinny być skonstruowane w taki sposób, aby utrudnić identyfikację Współpracownika oraz dostęp do danych osobowych. W strukturze hasła nie powinny być używane imiona, nazwiska, przezwiska, pseudonimy, inicjały, znaki, litery, cyfry następujące po sobie na klawiaturze, daty, numery rejestracyjne samochodów, nr telefonów, nazwy programów lub aplikacji, powszechnie znane skróty i inne kombinacje znaków kojarzących się bezpośrednio ze Współpracownikiem lub Administratorem, albo mogących w inny sposób doprowadzić do łatwego ich rozszyfrowania przez osoby nieupoważnione.
3. Hasła powinny być łatwe do zapamiętania oraz szybkie do wprowadzenia, by uniemożliwić ich podejrzenie przez osoby nieupoważnione.

§ 14

1. Na komputerach i urządzeniach mobilnych Administratora może być instalowane wyłącznie oprogramowanie pochodzące z legalnego źródła. Zmiany w systemie informatycznym lub instalacja nowego oprogramowania jest dokonywana wyłącznie przez Administratora.
2. Niedopuszczalne jest wprowadzanie przez Współpracownika zmian w systemie informatycznym Administratora oraz instalowanie nielegalnych lub pochodzących z niepewnego źródła programów lub aplikacji.
3. Współpracownik nie jest uprawniony do udostępniania osobom trzecim programów lub aplikacji będących własnością Administratora lub użytkowanych przez niego na podstawie umowy licencyjnej.
4. Współpracownik jest zobowiązany używać aplikacji lub programów zainstalowanych na urządzeniach Administratora z poszanowaniem praw autorskich i praw pokrewnych.
5. Administrator przeprowadza systematyczne kontrole legalności oprogramowania programów i aplikacji zainstalowanych na poszczególnych urządzeniach wchodzących w skład systemu informatycznego oraz na urządzeniach prywatnych wykorzystywanych przez Współpracowników.

§ 15

1. W przypadku konieczności naprawy lub konserwacji urządzeń służących do przetwarzania danych osobowych, przed przekazaniem odpowiednim podmiotom, urządzenia należy zabezpieczyć przed nieuprawnionym dostępem lub utratą danych osobowych.
2. Z urządzeń służących do przetwarzania danych osobowych, przeznaczonych do wymiany lub likwidacji, należy przenieść dane osobowe, a następnie usunąć je z urządzenia, w sposób uniemożliwiający ich odzyskanie lub gwarantujący pełną

anonimizację. W przypadku gdy nie jest możliwe usunięcie lub anonimizacja danych osobowych, należy urządzenie uszkodzić w sposób dostatecznie uniemożliwiający odczytanie danych.

§ 16

1. Korzystanie przez Współpracownika ze służbowego konta poczty elektronicznej dozwolone jest wyłącznie w celu wykonywania warunków współpracy.
2. Korzystając ze służbowego konta poczty elektronicznej Współpracownik powinien dbać o bezpieczeństwo przesyłanych danych, w szczególności poprzez:
   1) zwracanie należytej uwagę na prawidłowe adresy odbiorców, zwłaszcza w przypadku korzystania z mechanizmu automatycznego uzupełniania adresu;
   2) korzystanie z opcji „ukryta kopia" w przypadku konieczności wysłania wiadomości do wielu niezwiązanych ze sobą osób, niebędących uczestnikami wspólnej konwersacji;
   3) unikanie załączania do wiadomości plików o dużych rozmiarach;
   4) zabezpieczanie hasłem wszystkich przesyłanych plików zawierających dane osobowe, zwłaszcza plików zawierających dane wrażliwe osób korzystających z pomocy Stowarzyszenia. Hasło powinno zostać przesłane w odrębnej wiadomości e-mail lub podane adresatowi w wiadomości sms. Hasło powinno spełniać warunki określone w § 13 powyżej;
   5) unikanie przesyłania danych osobowych (zwłaszcza danych wrażliwych) za pomocą komunikatorów internetowych typu Facebook (Messenger), Instagram, WhatsApp, etc.;
   6) niezwłoczne zgłaszanie Administratorowi wszelkich przypadków nieprawidłowego wykorzystania poczty elektronicznej, w tym na omyłkowe przesłanie wiadomości do niewłaściwego adresata.
3. Współpracownik powinien zwracać szczególną uwagę na wiadomości elektroniczne pochodzące od nieznanych nadawców, dotyczące opłacenia faktur, windykacji, komunikaty z serwisów aukcyjnych, wiadomości zawierające prośbę o podanie danych osobowych lub danych do logowania, wiadomości zawierających błędy w nazwie, adresie lub treści.
4. W przypadku otrzymania przez Współpracownika, na służbowy adres poczty elektronicznej, podejrzanej korespondencji, Współpracownik jest zobowiązany:
   1) poinformować o tym fakcie Administratora;
   2) nie otwierać załączników, przed uzyskaniem zgody Administratora;
   3) nie uruchamiać linków zawartych w takich wiadomościach;
   4) nie odpisywać na takie wiadomości, bez uzyskania pewności, że dotyczą one spraw służbowych.
5. Współpracownik może wykorzystywać służbowe urządzenia z dostępem do sieci Internet wyłącznie do celów związanych z realizacją obowiązków służbowych. Współpracownik nie może wykorzystywać tych urządzeń do:
   1) przeglądania, wykorzystywania lub ściągania materiałów płatnych;
   2) przeglądania, wykorzystywania lub ściągania materiałów o treściach prawnie zakazanych, naruszających dobre obyczaje lub uznawanych za obraźliwe;
   3) uzyskiwania dostępu do informacji z naruszaniem praw osób trzecich (w tym prawa autorskiego);
   4) wyrażania osobistych opinii w sposób umożliwiający potraktowanie ich jako opinii Administratora;

5) zakłócania normalnej pracy innych urządzeń Administratora;
6) naruszenia dobrego imienia Administratora;
7) korzystania z dostępnych w Internecie gier i oprogramowania rozrywkowego.

6. Po zakończeniu współpracy z Administratorem Współpracownik jest zobowiązany:
   1) usunąć z pamięci wykorzystywanych przez siebie urządzeń, będących własnością Administratora, wszelkich prywatnych danych i informacji;
   2) zwrócić Administratorowi wszystkie wykorzystywane przez siebie, a należące do Administratora urządzenia i nośniki, zachowując na nich wszelkie zapisane na nich informacje i materiały służbowe.
7. Po zakończeniu współpracy ze Współpracownikiem, używane przez niego urządzenia (w tym urządzenia prywatne) są czyszczone z danych osobowych należących do Administratora (po stworzeniu kopii zapasowej danych, których przechowywanie jest niezbędne z uwagi na obowiązek prawny lub prawnie uzasadniony interes Administratora).

V.5. Retencja danych. Usuwanie danych, niszczenie dokumentów tradycyjnych oraz nośników elektronicznych

§ 17

1. Administrator na bieżąco monitoruje okres przechowywania danych osobowych oraz usuwa dane osobowe po upływie tego okresu lub po odpadnięciu celu, dla którego dane mogą być przetwarzane.
2. Dokumenty tradycyjne oraz nośniki informacji zawierające dane osobowe przeznaczone do usunięcia, powinny być uprzednio zniszczone w sposób uniemożliwiający odczytanie danych (np. przy pomocy niszczarki lub poprzez przekazanie zewnętrznemu podmiotowi zajmującemu się zawodowo niszczeniem dokumentów i nośników).
3. Niezamierzone zniszczenie danych osobowych należy zgłosić Administratorowi. W szczególnie uzasadnionych przypadkach należy sporządzić raport z naruszenia ochrony danych osobowych, zgodnie z Załącznikiem nr 8 do Polityki bezpieczeństwa.

V.6. Zabezpieczenie systemu informatycznego i kontrola antywirusowa

§ 18

1. System informatyczny, w tym w szczególności wchodzące w jego skład komputery i urządzenia mobilne powinno zabezpieczyć się przed:
   1) nieuprawnionym dostępem;
   2) utratą danych spowodowaną działaniem nieautoryzowanego oprogramowania (np. wirusów, robaków, trojanów) oraz przechwyceniem (uszkodzeniem danych lub ich zafałszowaniem);
   3) uszkodzeniem kodu aplikacji, umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu;
   4) przechwyceniem danych podczas transmisji w przypadku rozproszonego przetwarzania danych z wykorzystaniem sieci Internet;
   5) aplikacjami prywatnymi użytkowników;
   6) awarią zasilania lub zakłóceniami w sieci zasilającej, awarią systemu

spowodowaną błędem lub wadliwym działaniem programu, aplikacji lub działaniem Użytkownika.

2. W celu ochrony systemu informatycznego przed działaniem szkodliwego oprogramowania i naruszeniem ochrony danych osobowych Administrator stosuje:
   1) ochronę antywirusową w aktualnej wersji;
   2) zaporę sieciową w aktualnej wersji;
   3) autoryzację użytkowników, przy zachowaniu haseł dostępu o odpowiednim poziomie skomplikowania;
   4) stosowanie szyfrowanej transmisji danych.
3. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, Administrator podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:
   1) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego;
   2) odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane;
   3) samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z podmiotami zewnętrznymi.

V.7. Szkolenie wstępne i okresowe

§ 19

1. Przed dopuszczeniem do przetwarzania danych, Współpracownik odbywa szkolenie w zakresie obowiązujących u Administratora zasad ochrony danych osobowych oraz podstawowych przepisów dotyczących ochrony danych osobowych.
2. W zależności od bieżących potrzeb Współpracownicy podlegają okresowym szkoleniom z zakresu ochrony danych osobowych. Szkolenia te są przeprowadzane w szczególności w sytuacji:
   1) istotnej zmiany przepisów dotyczących ochrony danych osobowych,
   2) zmiany obowiązujących u Administratora zasad ochrony danych osobowych,
   3) wystąpienia u Administratora istotnego naruszenia ochrony danych osobowych.

VI. Nadawanie uprawnień do przetwarzania danych osobowych

§ 20

1. Administrator nadaje upoważnienia do przetwarzania danych osobowych stosownie do zakresu danych osobowych, do których Współpracownik powinien mieć dostęp, w celu należytego wykonywania swoich obowiązków.
2. Upoważnienie do przetwarzania danych oraz odwołanie upoważnienia powinny posiadać formę pisemną. Wzór upoważnienia stanowi **Załącznik nr 2**, natomiast wzór odwołania upoważnienia stanowi **Załączniki nr 3** do Polityki bezpieczeństwa.

VII. Procedury dotyczące przetwarzania danych osobowych

VII.1. Podstawy przetwarzania danych osobowych

§ 21

1. Administrator, a w jego imieniu każdy Współpracownik przetwarza dane osobowe wyłącznie, jeśli istnieje ku temu podstawa prawna, zgodnie z art. 6 ust. 1 lub 9 ust. 2 RODO.
2. Dane zwykłe mogą być przetwarzane wyłącznie jeśli:
   1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie jej danych osobowych w określonym celu;
   2) przetwarzanie jest niezbędne do wykonania umowy (w tym jej rozliczenia), której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
   3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze (w tym w zakresie przekazywania danych osobowych organom administracji publicznej);
   4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
   5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
   6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, w szczególności do celów marketingowych, dochodzenia i obrony roszczeń.
3. Dane wrażliwe, w tym dane dotyczące stanu zdrowia, mogą być przetwarzane wyłącznie jeśli:
   1) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych, chyba że z odrębnych przepisów wynika zakaz uzyskiwania zgody w takim celu;
   2) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem lub porozumieniem zbiorowym prawa pracy, przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
   3) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
   4) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
   5) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
   6) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony przed roszczeniami;
   7) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem

publicznym, na podstawie obowiązującego prawa;

8) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie obowiązującego prawa lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem zapewnienia odpowiednich warunków i zabezpieczeń;
9) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie obowiązującego prawa;
10) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, na podstawie obowiązującego prawa.

VII.2. Zasady przetwarzania danych osobowych

§ 22

1. Administrator, a w jego imieniu każdy Współpracownik przetwarza dane osobowe z poszanowaniem zasad:
   1) zgodności z prawem, rzetelności i przejrzystości – działania związane z przetwarzaniem danych powinny być zgodne z prawem, a także dokonywane w sposób rzetelny i jawny dla osób, których dane dotyczą;
   2) ograniczenia celu – jeśli dane zostały zebrane z określonym przeznaczeniem, tylko w tym celu mogą być przetwarzane. W przypadku konieczności zmiany tej podstawy, należy niezwłocznie poinformować o tym osobę, której dane dotyczą;
   3) minimalizacji danych (adekwatności) – dane osobowe mogą być przetwarzane tylko w takim zakresie, jaki jest niezbędny do realizacji określonego celu przetwarzania. Dane osobowe nie powinny być zbierane „na zapas" lub „na wszelki wypadek";
   4) prawidłowości – należy dążyć do tego, by zebrane dane były merytorycznie poprawne. w przypadku wykrycia błędu, należy sprostować omyłki i usunąć nieprawidłowości;
   5) ograniczenia czasowego – dane osobowe mogą być przetwarzane tylko przez czas wynikający z obowiązujących przepisów (jeśli taki czas został określony), a jeśli w przypadku braku stosownych przepisów prawa – przez czas niezbędny do realizacji celu, dla którego dane zostały zebrane;
   6) poufności – dane należy chronić przed dostępem osób nieupoważnionych;
   7) rozliczalności – przetwarzanie powinno być zorganizowane w taki sposób, aby móc wykazać jego zgodność z prawem, np. poprzez dokumentowanie zdarzeń związanych z przetwarzaniem danych osobowych.

VIII. Opis zasad i sposobów realizacji praw osób, których dane dotyczą

§ 23

1. Zgodnie z Rozdziałem III RODO, Administrator zapewnia realizację praw osób, których dane dotyczą.
2. Administrator umożliwia podmiotom danych osobowych zgłaszanie żądań dotyczących realizacji ich praw w dowolnej formie, w tym elektronicznej.
3. Każdy Współpracownik, który w ramach wykonywania obowiązków otrzymał zgłoszenie dotyczące realizacji praw podmiotów danych osobowych, jest zobowiązany niezwłocznie przekazać Administratorowi informację o dokonanym zgłoszeniu lub, jeżeli posiada takie upoważnienie, w porozumieniu z Administratorem zrealizować żądanie.

VIII.1. Prawo do informacji

§ 24

Podczas pozyskiwania danych osobowych od osoby, której dane dotyczą, Administrator wykonuje względem tej osoby obowiązek informacyjny, o których mowa w art. 13 ust. 1 RODO. W związku z tym Administrator. informuje o:

1) swojej nazwie oraz danych kontaktowych;
2) celach przetwarzania danych osobowych oraz podstawie prawnej przetwarzania;
3) prawnie uzasadnionych interesach realizowanych przez Administratora, jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO;
4) odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
5) zamiarze przekazania danych do państwa trzeciego lub organizacji międzynarodowej;
6) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu;
7) prawie do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
8) jeżeli przetwarzanie odbywa się na podstawie zgody – o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
9) prawie wniesienia skargi do organu nadzorczego;
10) obowiązkowym charakterze przetwarzania danych osobowych, w tym:
    a) czy podanie danych osobowych jest wymogiem ustawowym lub warunkiem zawarcia umowy;
    b) czy osoba, której dane dotyczą, jest zobowiązana do podania danych osobowych;
    c) jakie są ewentualne konsekwencje niepodania danych osobowych;
11) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.

§ 25

W przypadku, gdy Administrator pozyskuje dane osobowe z innego źródła, niż od osoby, której dane dotyczą, w szczególności w przypadku pobierania danych ze

Źródeł publicznych, Administrator wykonuje względem osoby, której dane dotyczą obowiązek informacyjny, o których mowa w art. 14 ust. 1 RODO. W tym celu poza informacjami wymienionym w § 27, Administrator informuje o:

1) źródle pochodzenia danych osobowych, w tym czy pochodzą one Źródeł publicznych;
2) kategoriach danych osobowych, które są przetwarzane przez Administratora.

§ 26

1. Administrator podaje informacje, o których mowa w § 26 i 27 w odpowiednim terminie:
   1) w odniesieniu do danych pozyskiwanych od osoby, której dane dotyczą - podczas pozyskiwania;
   2) w odniesieniu do danych pozyskiwanych z innego źródła niż od osoby, której dane dotyczą:
      a) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca;
      b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji;
      c) jeżeli Administrator planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.
2. Konieczność wykonania obowiązku informacyjnego nie dotyczy sytuacji, gdy i w zakresie, w jakim (i) osoba, której dane dotyczą posiada już te informacje lub (ii) informacje te muszą pozostać poufne zgodnie z obowiązującym prawem.

§ 27

1. W celu wykonywania obowiązku informacyjnego Administrator stosuje opracowane wzory klauzul informacyjnych.
2. Realizacja obowiązku informacyjnego względem klientów i kontrahentów Administratora może odbywać się również poprzez odesłanie do Polityki Prywatności dostępnej na stronie internetowej Administratora.

VIII.2. Prawo dostępu do danych osobowych

§ 28

Na żądanie osoby, której dane dotyczą, Administrator (i) niezwłocznie potwierdza, czy przetwarza dane osobowe dotyczące tej osoby, (ii) umożliwia osobie, której dane dotyczą dostęp do przetwarzanych danych oraz (iii) przekazuje informacje o:

1) celach przetwarzania danych osobowych;
2) kategoriach danych osobowych tej osoby, które przetwarza Administrator;
3) odbiorcach lub kategoriach odbiorców, którym dane zostały lub zostaną ujawnione, w tym o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
4) planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, kryteriach ustalania tego okresu;
5) prawie do żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych oraz do wniesienia sprzeciwu wobec przetwarzania;
6) prawie wniesienia skargi do organu nadzorczego;

7) źródle pochodzenia danych osobowych, jeżeli nie zostały zebrane od osoby, której dane dotyczą;
8) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu,
9) odpowiednich zabezpieczeniach, związanych z przekazaniem danych do państwa trzeciego lub organizacji międzynarodowej.

§ 29

Administrator dostarcza osobie, której dane dotyczą, na jej żądanie, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, Administrator może pobrać opłatę. Opłata nie może być jednak wyższa niż koszt poniesiony na wykonanie kopii i przekazanie nośnika. Administrator może przekazać kopię danych drogą elektroniczną, jeśli osoba, której dane dotyczą się o to zwraca.

VIII.3. Prawo do sprostowania danych osobowych

§ 30

1. Niezwłocznie po wykryciu jakichkolwiek nieprawidłowości, nieścisłości lub omyłek pisarskich w przetwarzanych danych, Administrator poprawia te błędy. Administrator prostuje dane osobowe z własnej inicjatywy oraz na żądanie podmiotu danych.
2. W przypadku, gdy nie stoi temu na przeszkodzie cel przetwarzania, na żądanie osoby, której dane dotyczą, Administrator uzupełnia niekompletne dane osobowe.

§ 31

1. Współpracownik, który w ramach wykonywania swoich obowiązków wykrył jakiekolwiek nieprawidłowości, nieścisłości lub omyłki pisarskie w danych osobowych, jest zobowiązany powiadomić o tym Administratora albo poprawić te dane, o jest uprawniony do ingerowania w treść dokumentu, w którym dane zostały utrwalone.
2. Administrator niezwłocznie informuje odbiorców danych o dokonanym przez siebie sprostowaniu danych osobowych, chyba że jest to niemożliwe lub wymagałoby nadmiernego wysiłku. Administrator informuje osobę, której dane dotyczą, na jej żądanie o tych odbiorcach.

VIII.4. Prawo do bycia zapomnianym

§ 32

1. Na żądanie osoby, której dane dotyczą, Administrator niezwłocznie usuwa jej dane osobowe ze wszelkich nośników, serwerów i sieci, w których były utrwalone.
2. Żądanie usunięcia danych osobowych może być zrealizowane w przypadku, gdy:
   1) dane osobowe nie są już niezbędne Administratorowi do celów, w których zostały zebrane lub w inny sposób przetwarzane;
   2) osoba, której dane dotyczą, cofnęła zgodę, na której opierało się przetwarzanie;
   3) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;
   4) dane osobowe były przetwarzane niezgodnie z prawem;
   5) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku

prawnego przewidzianego w przez prawo;
6) dane zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

§ 33

1. Jeśli doszło do upublicznienia danych, Administrator informuje odbiorców danych, że osoba, której dane dotyczą, żąda, by administratorzy usunęli wszelkie łącza do danych osobowych tej osoby, kopie tych danych osobowych lub ich replikacje.
2. Administrator nie jest zobowiązany do realizacji obowiązku, o którym mowa w ust. 1, jeśli przy uwzględnieniu dostępnych mu technologii lub kosztów realizacji, poinformowanie nie jest możliwe albo gdy przetwarzanie danych jest obowiązkiem prawnym. Administrator informuje osobę, której dane dotyczą, na jej żądanie o tych odbiorcach.

VIII.5. Prawo do ograniczenia przetwarzania danych osobowych

§ 34

1. Na żądanie osoby, której dane dotyczą Administrator ogranicza przetwarzanie danych osobowych, poprzez zmniejszenie liczby kategorii przetwarzanych danych lub celów, dla których dane są przetwarzane.
2. Żądanie ograniczenia przetwarzania danych może być uwzględnione, jeśli:
   1) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – ograniczenie może zostać wprowadzone na okres pozwalający Administratorowi sprawdzić prawidłowość tych danych;
   2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
   3) Administrator nie potrzebuje już danych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony przed roszczeniami;
   4) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – ograniczenie może zostać wprowadzone do czasu stwierdzenia, czy prawnie uzasadnione podstawy występujące po stronie Administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

§ 35

1. Administrator może w dalszym ciągu przetwarzać dane osobowe, w odniesieniu do których doszło do ograniczenia, wyłącznie poprzez ich przechowywanie. Administrator może przetwarzać dane w pozostałym zakresie wyłącznie za zgodą osoby, której dane dotyczą, (i) w celu ustalenia, dochodzenia lub obrony przed roszczeniami albo (iii) w celu ochrony praw innej osoby fizycznej lub prawnej. O dalszym przetwarzaniu Administrator niezwłocznie informuje osobę, której dane dotyczą i która żądała ograniczenia.
2. Administrator niezwłocznie informuje odbiorców danych o dokonanym przez siebie ograniczeniu, chyba że jest to niemożliwe lub wymagałoby nadmiernego wysiłku. Administrator informuje osobę, której dane dotyczą, na jej żądanie o tych odbiorcach.

VIII.6. Prawo do przenoszenia danych osobowych

§ 36

1. Na żądanie osoby, której dane dotyczą, Administrator przekazuje jej w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego (np. w formacie PDF, pliku Excel) dane osobowe dotyczące tej osoby, które ta osoba dostarczyła Administratorowi.
2. O ile jest to technicznie możliwie, na żądanie osoby, której dane dotyczą, Administrator przesyła dane, o których mowa w ust. 1 innemu wskazanemu przez tę osobę administratorowi.
3. Żądanie, o których mowa w ust. 1 i 2 powyżej mogą zostać zrealizowane, jeżeli:
   1) przetwarzanie danych osobowych odbywa się na podstawie zgody;
   2) przetwarzanie danych osobowych odbywa się w sposób zautomatyzowany.
4. Na żądanie osoby, której dane dotyczą Administrator usuwa dane dotyczące tej osoby niezwłocznie po przeniesieniu (zgodnie z prawem do bycia zapomnianym).

VIII.7. Prawo do sprzeciwu wobec przetwarzania

§ 37

1. Sprzeciw wobec przetwarzania może zostać uwzględniony przez Administratora, jeśli dane osobowe, których dotyczy sprzeciw są wykorzystywane do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora, w tym do celów komercyjnych, marketingu bezpośredniego oraz profilowania.
2. Po otrzymaniu sprzeciwu wobec przetwarzania danych osobowych dla celów marketingu bezpośredniego, Administrator niezwłocznie zaprzestaje przetwarzania danych osobowych w tym celu.
3. Po otrzymaniu sprzeciwu wobec przetwarzania danych osobowych w celu realizacji innego prawnie uzasadnionego interesu Administratora niż wskazany w ust. 3, Administrator może w dalszym ciągu przetwarzać dane osobowe, o ile istnieją (i) ważne prawnie uzasadnione podstaw do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą, lub (ii) podstawy do ustalenia, dochodzenia lub obrony przed roszczeniami.

IX. Zagrożenia i naruszenia ochrony danych osobowych

§ 38

1. Administrator oraz Współpracownicy są zobowiązani zapobiegać zagrożeniom ochrony danych osobowych.
2. Spośród istniejących u Administratora zagrożeń ochrony danych wyróżnia się:
   1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu);
   2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, Administratora, Współpracowników, awarie sprzętowe, błędy oprogramowania);
   3) zewnętrzne lub wewnętrzne zamierzone, świadome i celowe działania nakierowane na wywołanie uszkodzenia infrastruktury technicznej, zakłócenia

ciągłości pracy lub ujawnienia danych osobowych osobom nieuprawnionym. Mogą one polegać w szczególności na:

a) uzyskaniu nieuprawnionego dostępu do systemu informatycznego z zewnątrz (włamaniu do systemu),
b) nieuprawnionym dostępie do systemu z jego wnętrza,
c) nieuprawnionym przekazie danych,
d) pogorszeniu jakości sprzętu i oprogramowania,
e) bezpośrednim zagrożeniu materialnych składników systemu.

§ 39

1. Administrator uznaje za naruszenie lub uzasadnione podejrzenie naruszenia bezpieczeństwa danych osobowych w szczególności następujące przypadki:
   1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, itp.;
   2) niewłaściwe parametry środowiska, jak np.: nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
   3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych;
   4) pojawienie się komunikatu alarmowego z tej części systemu informatycznego, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
   5) odstępstwa wskazujące na zakłócenia systemu informatycznego lub inną niepożądaną modyfikację w systemie;
   6) próby naruszenia integralności systemu informatycznego lub bazy danych;
   7) stwierdzone próby modyfikacji danych osobowych lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
   8) niedopuszczalna manipulacja danymi osobowymi w systemie informatycznym;
   9) ujawnienie danych osobowych osobom nieupoważnionym, w tym poprzez omyłkowe przesłanie danych osobowych do niewłaściwego adresata;
   10) niewynikające z przypadku odstępstwa od zasad bezpieczeństwa pracy w systemie informatycznym, wskazujące na przełamanie lub zaniechanie ochrony danych osobowych, np.: praca na urządzeniu osoby, która nie posiada upoważnienia do obsługi tego urządzenia lub przetwarzania zapisanych na nim danych, sygnał o uporczywym nieautoryzowanym logowaniu;
   11) istnienie nieautoryzowanych kont dostępu do danych;
   12) zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia;
   13) skasowanie lub skopiowanie w sposób niedozwolony danych osobowych;
   14) rażące naruszenie procedur bezpieczeństwa informacji.
2. Za naruszenie ochrony danych osobowych Administrator uznaje również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych, jak również poprzez przechowywane danych osobowych w formie niezabezpieczonej na nośnikach tradycyjnych, dyskach twardych, pendrive, dyskach zewnętrznych, kartach pamięci.

X. Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 40

1. W przypadku stwierdzenia naruszenia ochrony danych każdy Współpracownik jest zobowiązany niezwłocznie powiadomić o tym fakcie Administratora.
2. W umowach o powierzenie przetwarzania danych osobowych, Administrator określa, że Podmiot przetwarzający jest zobowiązany powiadomić Administratora o naruszeniu ochrony danych lub o uzasadnionym podejrzeniu takiego naruszenia niezwłocznie, nie później jednak niż w ciągu 48 godzin od stwierdzenia naruszenia lub od wystąpienia podejrzenia naruszenia.
3. Do czasu przybycia Administratora na miejsce naruszenia Współpracownik powinien:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania, zminimalizowania lub uniknięcia wystąpienia niepożądanych skutków zaistniałego naruszenia;
   2) jeśli to możliwe, przystąpić do ustalenia przyczyn oraz sprawców naruszenia;
   3) udokumentować wstępnie zaistniałe naruszenie;
   4) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia.
4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych, Administrator:
   1) zapoznaje się z zaistniałą sytuacją i decyduje o dalszym postępowaniu, mając na uwadze ewentualne dalsze zagrożenia;
   2) może żądać dokładnej relacji z zaistniałego naruszenia ochrony danych osobowych od Współpracownika powiadamiającego, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
   3) nawiązuje bezpośredni kontakt – jeżeli zachodzi taka potrzeba – z osobami lub podmiotami zewnętrznymi posiadającymi wiedzę specjalistyczną, w celach niezbędnych do usunięcia lub zminimalizowania skutków naruszenia.
5. Po wyczerpaniu niezbędnych środków doraźnych związanych z zaistniałym naruszeniem, Administrator zasięga niezbędnych opinii i ustala zasady postępowania naprawczego.
6. Administrator dokumentuje zaistniały przypadek naruszenia ochrony danych osobowych oraz sporządza raport dotyczący naruszenia według wzoru stanowiącego **Załącznik nr 6** do Polityki bezpieczeństwa.

§ 41

1. Administrator niezwłocznie po uzyskaniu informacji o naruszeniu ochrony danych decyduje, czy naruszenie mogło skutkować ryzykiem naruszenia praw i wolności osób fizycznych i tym samym, czy zachodzi obowiązek zgłoszenia naruszenia do PUODO.
2. Przy ocenie charakteru naruszenia Administrator bierze pod uwagę możliwość powstania:
   1) uszczerbku fizycznego,
   2) szkód majątkowych u osób fizycznych (straty finansowej);
   3) szkód niemajątkowych u osób fizycznych, takich jak:
      a) utrata kontroli nad własnymi danymi osobowymi,
      b) ograniczenie praw,
      c) dyskryminacja,
      d) kradzież lub sfałszowanie tożsamości,
      e) nieuprawnione odwrócenie pseudonimizacji (nieuprawnione odszyfrowanie zaszyfrowanych danych),
      f) naruszenie dobrego imienia,
      g) naruszenie poufności danych osobowych chronionych tajemnicą zawodową;
   4) wszelkich innych znacznych szkód gospodarczych lub społecznych.

3. W przypadku, gdy analiza prowadzi do wniosku, że naruszenie mogło skutkować ryzykiem dla praw i wolności osób fizycznych, Administrator niezwłocznie, nie później jednak niż w ciągu 72 godzin od momentu stwierdzenia naruszenia dokonuje zgłoszenia naruszenia do PUODO.
4. Zgłoszenie powinno nastąpić w przyjętym przez PUODO formacie dla zgłoszeń naruszenia ochrony danych osobowych.
5. W przypadku, gdy przeprowadzona przez Administratora analiza prowadzi do wniosku, że naruszenie nie mogło skutkować ryzykiem naruszenia praw i wolności osób fizycznych, Administrator dokumentuje wyniki tej analizy w raporcie stanowiącym Załącznik nr 8.

XI. Postępowanie z danymi osobowymi w przypadku alarmu przeciwpożarowego lub innego

§ 42

1. Po ogłoszeniu alarmu każdy Współpracownik przerywa pracę i - w miarę możliwości, o ile nie zagraża to jego bezpieczeństwu - przed opuszczeniem obszaru przetwarzania danych:
   1) dokonuje wylogowania z używanych programów (aplikacji) oraz systemu informatycznego,
   2) blokuje lub - w miarę możliwości - wyłącza komputer,
   3) dokonuje niezbędnego zabezpieczenia danych osobowych przetwarzanych w systemie informatycznym i dokumentach tradycyjnych, tak, aby uniemożliwić dostęp do danych osobowych osób nieupoważnionych. W sytuacji opisanej powyżej za osoby nieupoważnione nie uważa się osób prowadzących akcję ratunkową lub ewakuacyjną.
2. W miarę możliwości, bezpośrednio po akcji ratunkowej lub ewakuacyjnej, Współpracownik sporządza notatkę lub odpowiedni raport zawierający informacje o miejscu i sposobie zabezpieczenia lub składowania urządzeń, nośników lub dokumentów tradycyjnych zawierających dane osobowe. Współpracownik przekazuje Administratorowi notatkę lub raport bezpośrednio po ustaniu zagrożenia.

XII. Procedury i środki sprawdzania zgodności przetwarzania danych osobowych z obowiązującymi przepisami

§ 43

1. Administrator przeprowadza okresowe sprawdzanie zgodności przetwarzania danych osobowych z przepisami dotyczącymi ochrony danych osobowych, w tym RODO.
2. Przedmiotem sprawdzenia powinny być w szczególności:
   1) zabezpieczenia fizyczne;
   2) zabezpieczenia osobowe (organizacyjne);
   3) zabezpieczenia systemu informatycznego.
3. Administrator archiwizuje dokumenty dotyczące sprawdzenia zgodności.

XIII. Zasady prowadzenia rejestru czynności przetwarzania danych

§ 44

1. Na podstawie art. 30 RODO Administrator prowadzi Rejestr Czynności Przetwarzania danych osobowych.
2. W sytuacji, gdy Administrator występuje w roli Podmiotu przetwarzającego, prowadzi on Rejestr Kategorii Czynności Przetwarzania dokonywanych w imieniu administratora.
3. Rejestry, o których mowa ust. 1 i 2 powyżej, są prowadzone w formie elektronicznej, według wzoru określonego w **Załączniku nr 4 i 5** do Polityki bezpieczeństwa.
4. Rejestry, o których mowa ust. 1 i 2 powyżej, są przeznaczone do użytku wewnętrznego i udostępniane osobom trzecim tylko na uzasadnione żądanie.

XIV. Zasady postępowania przy udostępnianiu i powierzeniu przetwarzania danych osobowych

XIV.1. Udostępnienie danych osobowych

§ 45

1. Administrator udostępnia dane osobowe na uzasadniony wniosek. Wniosek zawiera:
   1) informacje umożliwiające wyszukanie żądanych danych osobowych w posiadanych przez Administratora zbiorach danych;
   2) wskazanie zakresu żądanych danych osobowych;
   3) określenie celu, dla którego dane mają być udostępnione, a następnie wykorzystane.
2. Wystąpienie z wnioskiem o udostępnienie danych osobowych nie jest wymagane, jeśli Administratorowi jest znany cel, dla którego dane osobowe zostaną wykorzystane i cel ten jest zgodny z obowiązującym prawem.
3. Dane osobowe mogą być wykorzystane wyłącznie zgodnie z celem, dla którego zostały udostępnione.

§ 46

Podmiot, który występuje do Administratora z żądaniem udostępnienia danych osobowych powinien każdorazowo wskazać podstawę prawną i faktyczną przetwarzania danych. Administrator dokonuje analizy wskazanej podstawy przetwarzania danych i w przypadku stwierdzenia braku legitymacji odmawia na piśmie udostępnienia danych. Kopię pisma pozostawia się w dokumentacji ochrony danych Administratora.

XIV.2. Powierzenie przetwarzania danych osobowych

§ 47

1. Administrator zawiera umowę o powierzenie przetwarzania danych osobowych w przypadku, gdy zleca podmiotowi trzeciemu (innemu przedsiębiorcy) świadczenie usług, o ile realizacja tych usług wymaga przetwarzania danych osobowych w imieniu Administratora, w szczególności w związku z outsourcingiem usług kadrowych,

księgowych, informatycznych.

2. Administrator korzysta wyłącznie z usług podmiotów przetwarzających, którzy zapewniają gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Przed zawarciem umowy o powierzenie przetwarzania Administrator przeprowadza analizę dopuszczalności powierzenia danych określonemu Podmiotowi przetwarzającemu.
3. W przypadku, gdy na podstawie analizy, o której mowa w ust. 2 powyżej, Administrator stwierdza, że Podmiot przetwarzający zapewnia gwarancje bezpiecznego przetwarzania danych, Administrator zawiera umowę o powierzenie przetwarzania danych osobowych spełniającą wymagania określone w art. 28 RODO.
4. W przypadku uzasadnionego podejrzenia, że Podmiot przetwarzający nie wykonuje należycie wynikających z umowy oraz obowiązujących przepisów prawa obowiązków w zakresie przetwarzania powierzonych mu danych osobowych, Administrator dokonuje kontroli przestrzegania przez Podmiot przetwarzający jego obowiązków. W przypadku potwierdzenia naruszenia obowiązków Podmiotu przetwarzającego Administrator rozwiązuje z Podmiotem przetwarzającym umowę o świadczenie usług oraz umowę o powierzenie przetwarzania danych osobowych.

XV. Postanowienia końcowe

§ 48

1. Polityka bezpieczeństwa jest dokumentem wewnętrznym Administratora i nie podlega ujawnieniu, ani udostępnieniu osobom trzecim, chyba że obowiązek taki wynika z obowiązujących przepisów prawa lub odrębnych ustaleń stron.
2. Polityka bezpieczeństwa ma moc obowiązującą od dnia ……

Spis załączników:

1. Wzór oświadczenia o zapoznaniu się z Polityką bezpieczeństwa
2. Wzór upoważnienia do przetwarzania danych osobowych
3. Wzór odwołania upoważnienia do przetwarzania danych osobowych
4. Wzór Rejestru Czynności Przetwarzania Danych Osobowych
5. Wzór Rejestru Kategorii Czynności Przetwarzania dokonywanych w imieniu administratora
6. Wzór Raportu z naruszenia ochrony danych osobowych