POLITYKA BEZPIECZEŃSTWA

REMSTAT PIOTR POCHWATKA, ANDRZEJ SZCZEŚNIAK SPÓŁKA JAWNA

§1

1. Remstat Piotr Pochwatka, Andrzej Szcześniak Spółka jawna **[„Remstat”]** wprowadza Politykę Bezpieczeństwa oraz Instrukcję zarządzania systemem informatycznym określające sposób prowadzenia, zakres i sposób przetwarzania danych osobowych, środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.

2. Polityka Bezpieczeństwa jest zbiorem zasad regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych przetwarzanych przez Remstat.

3. Polityka Bezpieczeństwa zawiera:

   a) Wykaz budynków, pomieszczeń, części pomieszczeń, tworzący obszar w którym przetwarzane są dane osobowe – Załącznik nr 1,

   b) Wykaz zbioru danych osobowych ze wskazaniem programów zastosowanych do przetwarzania tych danych – Załącznik nr 2,

   c) Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania z nimi – Załącznik nr 3,

   d) Sposób przepływu danych osobowych pomiędzy poszczególnymi systemami – Załącznik nr 4,

   e) Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych – Załącznik nr 5.

4. Celem wprowadzenia niniejszego dokumentu jest określenie spójnych, precyzyjnych i zgodnych z obowiązującym prawem przepisów, reguł i procedur, według których Remstat buduje, zarządza oraz udostępnia zasoby i systemy informacyjne, informatyczne i dokumentację, określa sposób i środki ochrony tych danych, obowiązki użytkowników w procesie obiegu i ochrony informacji oraz postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych.

5. Podstawę prawną niniejszego dokumentu stanowią następujące akty prawne:

   a) ustawa z dnia 29 sierpnia 1997 roku (tj. Dz.U. z 2016 r. poz. 922) o ochronie danych osobowych – dalej „Ustawa”,

   b) rozporządzenie z dnia 29 kwietnia 2004 roku (Dz. U. Nr 100, poz. 1024) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych – dalej „Rozporządzenie”.

§2

Ilekroć w Polityce Bezpieczeństwa mowa jest o:

1) Administratorze Danych Osobowych **(ADO)** – należy przez to rozumieć Remstat Piotr Pochwatka, Andrzej Szcześniak Spółka jawna w zakresie, w jakim decyduje o celach i środkach przetwarzania danych osobowych oraz jako podmiot, któremu powierzono przetwarzanie danych osobowych w drodze umowy zawartej na piśmie przetwarzając dane osobowe wyłącznie w zakresie i celu przewidzianym umową.

2) Administratorze Systemu Informatycznego **(ASI)** – należy przez to rozumieć specjalistę ds. zarządzania systemem informatycznym działającego na podstawie upoważnienia udzielonego przez ADO.

3) Danych osobowych – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (osoby, 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).

4) Przetwarzaniu danych osobowych – należy przez to rozumieć jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

5) Systemie informatycznym – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

6) Zbiorze danych – należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

7) Użytkownik – osoba posiadająca upoważnienie nadane przez ADO i upoważniona do przetwarzania danych osobowych w zakresie i czasie wskazanym w upoważnieniu.

§3

1. Przetwarzanie danych osobowych przez ADO odbywa się w siedzibie Remstat. Wykaz pomieszczeń został szczegółowo wskazany w **Załączniku nr 1** do Polityki Bezpieczeństwa.
2. Do przetwarzania danych osobowych upoważnione są osoby, które uzyskały imienne upoważnienie od ADO do przetwarzania danych osobowych w określonym w upoważnieniu zbiorze danych.
3. Wzór upoważnienia, o którym mowa w ustępie poprzedzającym stanowi **Załącznik nr 6** do Polityki Bezpieczeństwa.
4. Upoważnienie do przetwarzania danych osobowych wydawane jest w dwóch egzemplarzach, po jednym dla:
   1) pracownika lub osoby współpracującej na podstawie umowy cywilnoprawnej oraz
   2) ADO.
5. Uprawnienie do nadawania upoważnień do przetwarzania danych osobowych przysługuje każdemu ADO.

6. ADO prowadzi ewidencję upoważnień do przetwarzania danych osobowych w formie elektronicznej lub papierowej, według wzoru stanowiącego **Załącznik nr 7** do Polityki Bezpieczeństwa.
7. Ewidencja osób upoważnionych do przetwarzania danych osobowych, o której mowa w ustępie poprzedzającym podlega aktualizacji w przypadku zmian kadrowych, w wyniku których zmienia się skład osób upoważnionych do przetwarzania danych osobowych.

§4

1. Polityka Bezpieczeństwa ma zastosowanie do zbiorów danych osobowych określonych w wykazie stanowiącym **Załącznik nr 3** do Polityki Bezpieczeństwa.
2. Polityka Bezpieczeństwa ma zastosowanie do wszystkich pracowników oraz osób współpracujących na podstawie umów cywilnoprawnych z Remstat.
3. Pracownicy oraz osoby współpracujące z Remstat na podstawie umów cywilnoprawnych, zobowiązani są do współdziałania z ADO na etapie tworzenia umów, regulaminów lub aktów wewnętrznych, w których jest mowa o przetwarzaniu danych osobowych.
4. Dane osobowe przetwarzane przez Remstat mogą być wykorzystywane wyłącznie do celów, dla których zostały pozyskane.
5. W zbiorach danych posiadanych przez Remstat znajdują się zbiory zwolnione z obowiązku rejestracji na mocy przepisu art. 43 ust. 1 Ustawy.
6. Dane osobowe przetwarzane są w zbiorach danych:
   a) tradycyjnych, w szczególności w kartotekach, skorowidzach, wykazach i w zbiorach ewidencyjnych,
   b) w systemach informatycznych.

§5

1. Systemy informatyczne wraz z infrastrukturą, służące do przetwarzania danych osobowych Remstat powinny spełniać wymogi obowiązujących aktów prawnych, regulujących zasady bezpiecznego przetwarzania danych osobowych z uwzględnieniem środków bezpieczeństwa na poziomie wysokim, określonym w Rozporządzeniu.
2. Wszystkie dane w formie elektronicznej, przechowywane są na serwerze firmowym.
3. Dostęp do danych, o których mowa w ustępie poprzedzającym możliwy jest na podstawie indywidualnych haseł dostępu. Dostęp do danych udzielany jest przez ADO zgodnie z potrzebami.
4. Za prawidłowe funkcjonowanie serwera odpowiedzialny jest ADO lub w przypadku powołania – ASI.
5. Dostęp do serwerowni ma wyłącznie ADO, lub w przypadku powołania – ASI.
6. Archiwizacja danych realizowana jest w dwóch formach:
   1) raz dziennie za pomocą mechanizmu zachowującego wersje plików z danego dnia, przechowującego wersję plików do …….. dni wstecz,
   2) raz w miesiącu archiwizacja na zewnętrzny dysk szyfrowany hasłem przechowywany do dwóch miesięcy.
7. Zasady pracy z wykorzystaniem systemów, sprzętu i oprogramowania informatycznego w Remstat określa i wdraża ADO, w przypadku powołania – ADO dokonuje opisanych wyżej czynności w porozumieniu z ASI.
8. Serwery danych Remstat są zabezpieczone w sposób zapewniający poufność, integralność i rozliczalność, za pomocą środków technicznych będących standardami przemysłowymi przy wykorzystaniu mechanizmów uwierzytelniania i autoryzacji, filtrowania (firewall), systemu prezencji włamań (IPS) oraz szyfrowania.

§6

1. Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. Opuszczenie pomieszczenia, w których znajdują się zbiory danych osobowych musi być poprzedzone zabezpieczeniem zbioru danych, w tym w szczególności poprzez zablokowanie komputera oraz zamknięcia na klucz szaf i szafek, w których przechowywane są zbiory danych.
2. Wszystkie dane w formie papierowej przechowywane są w szafkach zamykanych na klucz.
3. Każdy pracownik posiada swoją szafkę, w której przechowuje dokumenty prowadzonych przez niego spraw i projektów.
4. Na koniec dnia każdy pracownik zamyka swoją szafkę z dokumentami na klucz.
5. Klucz do szafki jest wydawany przez ADO bądź osobę przez niego upoważnioną.

§7

1. Mając na celu ochronę danych osobowych oraz ich zabezpieczenie przed utratą, ujawnieniem osobom nieuprawnionym bądź innymi niepożądanymi działaniami, każdy pracownik lub osoba współpracująca na podstawie umowy cywilnoprawnej jest zobowiązany stosować odpowiednie środki zabezpieczające dostęp do komputera, nośników elektronicznych oraz dokumentów w formie papierowej znajdujących się w posiadaniu takiej osoby.
2. Pracownik Remstat oraz osoba współpracująca z Remstat na podstawie umowy cywilnoprawnej, po zakończeniu pracy zobowiązana jest do zniszczenia, w sposób uniemożliwiający zidentyfikowanie danych osobowych, zbędnych dokumentów papierowych oraz uzyskanych z systemów informatycznych, zawierających dane osobowe powstałe w trakcie ich przetwarzania.
3. Ponadto zabrania się:
   a) wyrzucania dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia,
   b) pozostawiania dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach,
   c) pozostawiania kluczy w drzwiach, szafach, biurkach, zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe,
   d) pozostawiania dokumentów na biurku po zakończonej pracy, pozostawiania otwartych dokumentów na ekranie monitora bez blokady konsoli,
   e) ignorowania nieznanych osób z zewnątrz poruszających się w obszarze przetwarzania danych osobowych,
   f) przekazywania informacji będących danymi osobowymi osobom nieupoważnionym,
   g) ignorowania zapisów Polityki Bezpieczeństwa.

§8

1. W umowach zawieranych przez Remstat podczas realizacji których mogą być przetwarzane dane osobowe, winny znajdować się postanowienia zobowiązujące podmioty zewnętrzne i bezpośrednich wykonawców do ochrony danych osobowych przetwarzanych przez Remstat.

2. W umowach zawieranych przez Remstat podczas realizacji których mogą być przetwarzane dane osobowe, winny znajdować się oświadczenia o zgodzie na przetwarzanie danych osobowych pozyskiwanych bezpośrednio od osób, których dane dotyczą lub postanowienia zezwalające na przetwarzanie danych osobowych pozyskiwanych przez Remstat z innych źródeł.

3. W przypadku pozyskiwania danych osobowych bezpośrednio od osoby, których te dane dotyczą ADO jest obowiązany poinformować tę osobę o:

   1) adresie swojej siedziby i pełnej nazwie,

   2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,

   3) prawie dostępu do treści swoich danych oraz ich poprawiania,

   4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

4. W przypadku pozyskiwania danych osobowych nie od osoby, której one dotyczą, ADO jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:

   1) adresie swojej siedziby i pełnej nazwie,

   2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,

   3) źródle danych,

   4) prawie dostępu do treści swoich danych oraz ich poprawiania,

   5) uprawnieniach wynikających z art.32 ust.1 pkt 7) i 8) Ustawy (tj. m.in. prawie złożenia sprzeciwu wobec przetwarzania danych lub wobec przekazywania ich innym podmiotom oraz żądania zaprzestania przetwarzania danych ze względu na szczególną sytuację osoby, której dane są przetwarzane).

5. Przebywanie osób wykonujących czynności na rzecz Remstat na podstawie umów cywilnoprawnych, oraz pracowników podmiotów zewnętrznych, w pomieszczeniach służących do przetwarzania danych osobowych, po godzinach urzędowania, powinno być uregulowane umowami zawieranymi z tymi podmiotami albo osobami oraz powinno podlegać nadzorowi pracownika Remstat lub osoby współpracującej z Remstat na podstawie umowy cywilnoprawnej, która jest odpowiedzialna za realizację umowy z tym podmiotem.

§9

1. Siedziba Remstat oraz obszary przetwarzania danych osobowych, o których mowa w § 3 ust. 1 Polityki Bezpieczeństwa wymagają stałego zabezpieczenia przez techniczne elementy bezpieczeństwa.

2. Obszary przetwarzania danych osobowych nie mogą być dostępne dla osób nieuprawnionych. Dopuszczalne odstępstwo od tej reguły możliwe jest wyłącznie dla pomieszczeń, w których przyjmowani są interesanci. Jeżeli pomieszczenia te wyposażone są w urządzenia z dostępem do systemów baz danych lub w tradycyjne kartoteki, należy w nich zastosować szczególne środki ostrożności, w tym:

   a) Interesanci powinni wchodzić pojedynczo i pozostawać w pomieszczeniu tylko w obecności pracownika Remstat lub osoby współpracującej z Remstat na podstawie umowy cywilnoprawnej,

b) nie należy pozostawiać żadnych nośników danych nie zabezpieczonych przed dostępem osób nieuprawnionych,

c) monitory komputerów powinny być usytuowane tak, aby uniemożliwić wgląd osobom nieuprawnionym,

d) wszystkie urządzenia powinny być usytuowane tak, aby znajdowały się z dala od przestrzeni, po której poruszają się osoby nieuprawnione.

3. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych poprzez nadanie każdemu użytkownikowi Identyfikatora. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;
b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

4. Do uwierzytelniania użytkowników używa się hasła, które składa się co najmniej z 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne (**„Identyfikator użytkownika”**).
5. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
6. Dostęp do danych będą miały wyłącznie osoby, których zakres obowiązków wymaga uzyskiwania danych – w zakresie pozostającym w związku z wykonywanymi przez te osoby obowiązkami. Dostęp do danych może mieć miejsce jedynie po podpisaniu przez Użytkownika oświadczenia o zachowaniu poszczególnych danych w tajemnicy.
8. Osoba użytkująca laptopa zawierającego dane osobowe, zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w Załączniku nr 1 do Polityki Bezpieczeństwa, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

9. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

1) likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

3) naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez ADO.

§10

1. Za nadzór nad bezpieczeństwem danych osobowych Remstat odpowiada ADO.
2. Za naruszenie zasad ochrony danych osobowych uważa się w szczególności:
a) nieupoważniony dostęp, modyfikację, kopiowanie lub zniszczenie/usunięcie danych osobowych, zarówno w systemie informatycznym, jak i na nośnikach papierowych i elektronicznych,
b) udostępnianie danych osobowych nieuprawnionym podmiotom lub osobom,
c) nieautoryzowany dostęp do danych przez połączenie sieciowe,
d) dostęp do pomieszczeń, w których przetwarza się dane osobowe dla osób nieuprawnionych,

e) niedopełnienie obowiązku ochrony danych osobowych przez umożliwienie dostępu do danych (np. pozostawienie kopii danych, niezablokowanie dostępu do systemu, brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi przebywającymi w pomieszczeniach gdzie przetwarza się dane osobowe),
f) wykrycie niezabezpieczonego kanału dystrybucji danych osobowych,
g) nielegalne bądź nieświadome ujawnienie danych osobowych,
h) pozyskiwanie danych osobowych z nielegalnych źródeł,
i) przetwarzanie danych osobowych niezgodne z uprawnionym celem i zakresem,
j) stwierdzenie obecności wirusów komputerowych lub innych programów godzących w integralność systemu informatycznego,
k) ujawnienie indywidualnych haseł dostępu do systemu.

3. W przypadku stwierdzenia naruszeń zabezpieczeń danych osobowych, każdy Użytkownik jest zobowiązany niezwłocznie zgłosić ten fakt ADO.
4. ADO lub upoważniona przez niego osoba podejmie wszelkie, niezbędne czynności mające na celu:
   a) minimalizację negatywnych skutków naruszenia,
   b) wyjaśnienie okoliczności naruszenia zabezpieczeń oraz lokalizuje źródło naruszeń,
   c) usunięcie stwierdzonych nieprawidłowości,
   d) umożliwienie dalszego, bezpiecznego przetwarzania danych osobowych.
5. Każdy Użytkownik zobowiązany jest podjąć niezbędne czynności, w tym złożenie stosownych wyjaśnień, w związku ze stwierdzonym naruszeniem bezpieczeństwa danych osobowych.
6. Odmowa Użytkownika podjęcia współpracy, o której mowa w ustępie poprzedzającym będzie stanowiła naruszenie obowiązków pracowniczych, a w przypadku współpracowników – postanowień wiążącej strony umowy.

§11

1. Dane osobowe mogą być udostępnione osobom i podmiotom z mocy przepisów prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.

2. ADO odmawia udostępnienia danych jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

3. Powierzenie danych może nastąpić w drodze pisemnej umowy, w której osoba przyjmująca dane zobowiązuje się do przestrzegania obowiązujących przepisów ustawy o ochronie danych osobowych. Umowa powinna zawierać informacje o podstawie prawnej powierzenia danych, celu i sposobie ich przetwarzania.

§12

1. Polityka Bezpieczeństwa zostaje udostępniona w formie papierowej do wglądu wszystkich pracowników Remstat.

2. W każdym przypadku zatrudnienia nowego pracownika bądź osoby współpracującej z Remstat na podstawie umowy cywilnoprawnej, osoba taka zostaje zapoznana z zasadami bezpieczeństwa zawartymi w niniejszym dokumencie.

Załączniki:

1. Załącznik nr 1 - Wykaz adresów budynków i pomieszczeń, w których przetwarzane są dane osobowe.
2. Załącznik nr 2 - Wykaz zbioru danych osobowych ze wskazaniem programów zastosowanych do przetwarzania tych danych.
3. Załącznik nr 3 - Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania z nimi.
4. Załącznik nr 4 - Sposób przepływu danych osobowych pomiędzy poszczególnymi systemami.
5. Załącznik nr 5 - Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.
6. Załącznik nr 6 – Wzór upoważnień do przetwarzania danych osobowych.
7. Załącznik nr 7 – Wzór ewidencji upoważnień.

.....
Piotr Pochwatka

REMSTAT
P. Pochwatka, A . Szcześniak Sp. J.
80-209 Chwaszczyno, ul. Rewerenda 17B
Tel. 58 553 69 32
NIP 584-266-62-74 Regon 220717710