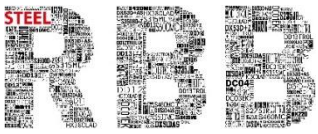
DATA	WYDANIE	NUMER	DOKUMENT OGÓLNODOSTĘPNY	
2018-05-25	1	RBB-PBD	**Polityka Bezpieczeństwa Danych Osobowych**	

	Data	Jednostka organizacyjna	Imię i nazwisko
Opracował:	2018-05-25	FP	Andrzej Świdurski
Zweryfikował:	2018-05-25	D	Maciej Frąckowiak
Zatwierdził:	2018-05-25	O	Joanna Borusiak-Liwinska Włodzimierz Borusiak

Wstęp

Realizując konstytucyjne prawo każdej osoby do ochrony życia prywatnego oraz postanowienia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) w celu zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ww. rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, wprowadza się następujący zestaw procedur.

Rozdział 1

Postanowienia ogólne

1. Ilekroć w dokumencie jest mowa o:
   1) **rozporządzeniu** – rozumie się przez to rozporządzenie 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);
   2) **danych osobowych** – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to 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) **zbiorze danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
   4) **przetwarzaniu danych** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich 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;
   5) **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
   6) **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
   7) **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
   8) **administratorze danych** – rozumie się przez to **STEEL RBB Sp. z o.o. Sp. K.** z siedzibą w Jarocinie przy ul. Wojska Polskiego 83, 63-200 Jarocin;

9) **zgodzie osoby, której dane dotyczą** – oznacza to 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;

10) **odbiorcy danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

11) **państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;

12) **środkach technicznych i organizacyjnych** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;

13) **ograniczeniu przetwarzania** – należy przez to rozumieć oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

14) **osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to osobę, która została upoważniona do przetwarzania danych osobowych przez administratora danych;

15) **pseudonimizacji** – oznacza to przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

16) **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;

17) **identyfikatorze** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

18) **podmiocie przetwarzającym** – oznacza to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

19) **naruszeniu ochrony danych osobowych** – oznacza to 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.

2. Administrator danych, świadomy wagi zagrożeń prywatności, w tym zwłaszcza zagrożeń bezpieczeństwa danych osobowych przetwarzanych w związku z wykonywaniem zadań, deklaruje podejmowanie wszelkich możliwych działań koniecznych do minimalizowania ryzyka w celu zapobiegania zagrożeniom, m.in. takim jak:
    1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie, działania antyterrorystyczne, niepożądana ingerencja ekipy remontowej, zgubienie lub kradzież nośnika/urządzenia, dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji, korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy;
    2) niewłaściwe parametry środowiska, zakłócające pracę urządzeń komputerowych np. nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne;
    3) awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne naruszenia ochrony danych osobowych, niewłaściwe działanie serwisantów, w tym pozostawienie serwisantów bez nadzoru, a także przyzwolenie na naprawę sprzętu zawierającego dane poza siedzibą administratora danych i inne o podobnym charakterze;
    4) podejmowanie pracy w systemie z przełamaniem lub zaniechaniem stosowania procedur ochrony danych, np. praca osoby, która nie jest upoważniona do przetwarzania, próby stosowania nie swojego hasła i identyfikatora przez osoby upoważnione;
    5) celowe lub przypadkowe rozproszenie danych w Internecie z ominięciem zabezpieczeń systemu lub wykorzystaniem błędów systemu informatycznego administratora danych;
    6) ataki z Internetu, nieuprawnione uzyskanie dostępu do informacji, nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń, złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych, uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)

7) naruszenia zasad i procedur określonych w dokumentacji z zakresu ochrony danych osobowych przez osoby upoważnione do ich przetwarzania, związane z nieprzestrzeganiem procedur w tym zakresie, w tym zwłaszcza:

   - niezgodne z procedurami np. zakończenie pracy lub opuszczenie stanowiska pracy, nieprawidłowe wyłączenie komputera, niezablokowanie wyświetlenia treści pracy na ekranie komputera przed tymczasowym opuszczeniem stanowiska pracy, pozostawienie po zakończeniu pracy nieschowanych do zamykanych na klucz szaf dokumentów zawierających dane osobowe, niezamknięcie na klucz pokoju po jego opuszczeniu, nieoddanie klucza do sekretariatu, itp.,
   - naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie,
   - ujawnienie osobom nieupoważnionym systemu zabezpieczeń ochrony danych i dokumentów z nim związanych stosowanych u administratora danych,
   - ujawnienie osobom nieupoważnionym danych przetwarzanych przez administratora danych, w tym również nieumyślne ujawnienie danych osobom postronnym, przebywającym bez nadzoru lub niedostatecznie nadzorowanym w pomieszczeniach administratora danych,
   - brak wykonywania stosownych kopii zapasowych,
   - przetwarzanie danych osobowych w celach prywatnych,
   - wprowadzanie zmian do systemu informatycznego administratora danych i instalowanie programów bez zgody administratora danych,
   - nieprawidłowa anonimizacja danych osobowych w dokumencie;
   - nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora;
   - niezamierzona publikacja;
   - dane osobowe wysłane do niewłaściwego odbiorcy;
   - ujawnienie danych niewłaściwej osoby;
   - ustne ujawnienie danych osobowych.

3. Wdrożenie niniejszej Polityki Ochrony Danych ma na celu zabezpieczenie przetwarzanych przez niego danych osobowych, w tym danych przetwarzanych w systemie informatycznym administratora danych i poza nim, poprzez wykonanie obowiązków wynikających z ogólnego rozporządzenia o ochronie danych, ustaw i aktów wykonawczych.
4. Niniejszy dokument opisuje zbiór procedur i zasad dotyczący przetwarzania danych osobowych oraz sposób ich zabezpieczenia.
5. Niniejsza polityka dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach, dokumentacji papierowej, jak i w systemach informatycznych.
6. Procedury i zasady określone w niniejszej Polityce stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i pozostałych wykonujących świadczenie w ramach innych umów.

Rozdział 2

Administrator danych

Administrator danych w szczególności:

1. uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane;
2. prowadzi rejestr czynności przetwarzania;
3. wyznacza Inspektora Ochrony Danych (IOD);
4. upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi ich obowiązków;
5. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

Rozdział 3

Inspektor ochrony danych

Inspektor ochrony danych realizuje zadania wynikające z rozporządzenia w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych oraz powierzonych obowiązków, w tym zwłaszcza:

1. informuje administratora, podmiot przetwarzający oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy rozporządzenia oraz innych obowiązujących przepisów o ochronie danych i doradza im w tej sprawie;
2. monitoruje przestrzeganie rozporządzenia oraz innych obowiązujących przepisów o ochronie danych, polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3. udziela na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 rozporządzenia;
4. współpracuje z organem nadzorczym;
5. pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 rozporządzenia, oraz w stosownych przypadkach prowadzi konsultacje we wszelkich innych sprawach.

Rozdział 4

Osoba upoważniona do przetwarzania danych osobowych

1. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

a) może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków;
b) osoba upoważniona do przetwarzania danych osobowych musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania; przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u administratora danych lub świadczenia usługi w oparciu o inną umowę, a także po ustaniu stosunku pracy lub innej;
c) osoba upoważniona do przetwarzania danych osobowych zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej polityki oraz stosuje określone przez administratora procedury oraz wytyczne mające na celu zgodne z prawem przetwarzanie danych;
d) osoba upoważniona do przetwarzania danych osobowych korzysta z systemu informatycznego administratora danych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;
e) osoba upoważniona do przetwarzania danych osobowych zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym w sposób wskazany w niniejszej Polityce i załącznikach do niej;
f) zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie;
g) rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;

2. Z uwagi na dbałość o bezpieczeństwo danych wdraża się następujące zasady przetwarzania danych przez użytkownika. Użytkownik przestrzega, aby:
   a) ekrany komputerowe były ustawione tak, aby osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza aby nie były ustawione naprzeciwko wejścia do pomieszczenia;
   b) wszelkie dokumenty, nośniki danych i sprzęt nie był pozostawiany w miejscach publicznych poza siedzibą administratora danych, np. w hotelach, samolotach, itp.;
   c) nie podłączano do komputerów dysków przenośnych w celu dokonywania kopii zapasowych na użytek prywatny;
   d) nie używano powtórnie dokumentów zadrukowanych jednostronnie (danymi osobowymi lub informacjami niejawnymi);
   e) inne osoby upoważnione do przetwarzania danych osobowych powstrzymywane były od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu;
   f) inne osoby upoważnione do przetwarzania danych osobowych przestrzegały swoich uprawnień w systemie, tj. właściwie korzystały z baz danych, używały tylko własnego identyfikatora i hasła;
   g) stosować się do zaleceń inspektora ochrony danych;
   h) opuszczając stanowisko pracy aktywizować wygaszacz ekranu lub zablokować stację roboczą w inny sposób;
   i) nie wynosić na jakichkolwiek nośnikach zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej;
   j) zachować w tajemnicy udostępnione jej dane osobowe, nawet przed najbliższymi;
   k) niszczyć w niszczarce lub chować do szaf zamykanych na klucz wszelkie wydruki zawierające dane osobowe przed opuszczeniem miejsca pracy;
   l) umieszczać klucze do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;
   m) zamykać okna w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;

n) zamykać drzwi na klucz po zakończeniu pracy w danym dniu i upewniać się, że w budynku nie pozostają osoby trzecie nieuprawnione do przebywania w siedzibie administratora danych.

Rozdział 5

Środki techniczne i organizacyjne

1. W celu ochrony danych spełniono wymogi, o których mowa w rozporządzeniu, w szczególności:
   a) przeprowadzono ocenę skutków dla ochrony danych zgodnie z załącznikiem nr 1,
   b) przeprowadzono analizę ryzyka w stosunku do zasobów biorących udział w poszczególnych procesach zgodnie z załącznikiem nr 2,
   c) do przetwarzania danych zostały dopuszczone wyłącznie osoby upoważnione przez administratora danych;
   d) zawarto umowy powierzenia przetwarzania danych zgodnie z załącznikiem nr 3;
   e) została opracowana i wdrożona niniejsza polityka ochrony danych;
2. W celu ochrony danych stosuje się zasady bezpieczeństwa osobowego, w tym w szczególności:
   a) ryzyko utraty bezpieczeństwa danych przetwarzanych przez administratora danych pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych jest minimalizowane przez podpisanie umów powierzenia przetwarzania danych osobowych;
   b) ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp o danych osobowych (np. osoby sprzątające pomieszczenia administratora danych) jest minimalizowane przez zobowiązanie ich do zachowania tajemnicy na podstawie odrębnych, pisemnych oświadczeń.
   c) przeprowadza się szkolenia dla osób, które mają zostać upoważnione do przetwarzania danych osobowych;
   d) przeprowadza się szkolenia wewnętrzne dla wszystkich osób upoważnionych do przetwarzania danych osobowych w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych;
   e) administrator danych prowadzi nadzór nad stosowaniem polityki „czystego biurka”;
   f) administrator danych prowadzi nadzór nad stosowaniem polityki kluczy.
3. W celu ochrony danych osobowych stosuje się następujące środki ochrony fizycznej danych osobowych:
   a) dostęp fizyczny do biura zabezpieczony jest poprzez istnienie barier architektoniczno-budowlanych, takich jak płot, zamykana brama przed budynkiem, drzwi antywłamaniowe;
   b) dostęp fizyczny do biura jest zabezpieczony poprzez drzwi zamykane na klucz oraz zabezpieczenie kartą magnetyczną;
   c) drzwi do pomieszczeń, w których przetwarzane są zbiory danych osobowych są w czasie nieobecności pracowników zabezpieczone zamkiem;
   d) biuro jest zabezpieczone poprzez zewnętrzny monitoring wizyjny, nadzór nad monitoringiem sprawują kierownicy działów i pracowników ochrony;
   e) dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych jest w czasie nieobecności pracowników nadzorowany przez agencję ochrony – grupę interwencyjną; z firmą ochroniarską zawarto umowę, która zakłada gotowość przyjechania patrolu interwencyjnego;
   f) zbiory danych osobowych w formie papierowej przechowywane są w drewnianych szafach zamykanych na klucz;
   g) dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych, objęty jest systemem kontroli dostępu, a dostęp do danych ma jedynie upoważnione osoby;
   h) pomieszczenia, w których przetwarzane są zbiory danych osobowych, zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy;
   i) zastosowano nadzór nad stosowaniem polityki „czystego biurka”;
   j) personel sprzątający jest zatrudniony na umowę o pracę, od personelu uzyskano odpowiednie zobowiązania dotyczące zachowania poufności danych;
   k) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
4. W celu ochrony danych osobowych stosuje się następujące środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej.
   a) zastosowano odrębny identyfikator dla każdego użytkownika w systemie informatycznym,
   b) dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej/komputerze przenośnym możliwy jest wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia,
   c) doszło do ograniczenia dostępu użytkownika do konkretnych zasobów – dostęp według uprawnień;
   d) uwierzytelnienie do systemu wymaga podania loginu;
   e) minimalny poziom złożoności haseł powinien obejmować kombinację minimum ośmiu znaków, małych i dużych liter, znaków specjalnych lub cyfr;
   f) hasło jest zmieniane co 30 dni;
   g) stosowane są wygaszacze ekranów, hasła wygaszaczy i odpowiednie ustawienie monitorów w sposób wykluczający wgląd przez osoby trzecie;

h) wprowadzono zabezpieczenie wewnętrzne sieci komputerowej przez odseparowanie od sieci publicznej poprzez użycie systemu Firewall (sprzętowy Stormshield, dodatkowo programowy ESET dotyczący komputerów przenośnych);
i) zastosowano skuteczne oprogramowanie antywirusowe, które jest aktualizowane (zarządzany w sposób centralny ESET);
j) zastosowano dodatkowe zabezpieczenia w postaci oprogramowania do zarządzania siecią Axence nVision;
k) wykonywane są kopie zapasowe dla zasobów przechowywanych na komputerach (poczta i dokumenty);
l) serwerowania jest zlokalizowana w odrębnym, klimatyzowanym zamykanym Pomieszczeniu. W pokoju tym mogą przebywać wyłącznie Zarząd Spółki administratora, Administrator Systemu Informatycznego, inne osoby upoważnione do przetwarzania tylko w ich towarzystwie, a osoby postronne w ogóle nie mają dostępu;
m) bieżąca konserwacja sprzętu wykorzystywanego przez administratora danych do przetwarzania danych prowadzona jest przez wewnętrzny personel informatyczny. Wszelkie naprawy wymagające interwencji firmy zewnętrznej realizowane są po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych, określającej kary umowne za naruszenie bezpieczeństwa danych.
n) administrator danych dopuszcza konserwowanie i naprawę sprzętu poza siedzibą administratora danych jedynie po trwałym usunięciu danych osobowych. Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych, a urządzenia uszkodzone mogą być przekazywane w celu utylizacji (jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony administratora) właściwym podmiotom, z którymi także zawiera się umowy powierzenia przetwarzania danych osobowych.
o) wszystkie awarie, działania konserwacyjne i naprawy systemu informatycznego są opisywane w stosownych protokołach, podpisywanych przez osoby w tych działaniach uczestniczące, a także przez wyznaczonego inspektora ochrony danych.

5. **Administrator wdrożył Politykę Bezpieczeństwa Teleinformatycznego** (aktualna wersja z dnia 15.01.2018), która stanowi doprecyzowanie niniejszej Polityki Ochrony Danych w zakresie przetwarzania danych osobowych w systemie teleinformatycznym Administratora. W celu ochrony danych osobowych stosuje się środki ochrony w ramach narzędzi programowych i baz danych opisane dokładnie w Polityce Bezpieczeństwa Teleinformatycznego.
6. W zakresie korzystania z ogólnej infrastruktury teleinformatycznej wprowadzono następujące zasady:
   a) użytkownik nie może samodzielnie odinstalować oprogramowania antywirusowego lub Firewall;
   b) użytkownik nie może samodzielnie dezaktywować skanera antywirusowego;
   c) użytkownik nie może samodzielnie instalować oprogramowania na swoim komputerze.
   d) dla zasobów danych osobowych przechowywanych na komputerach są wykonywane kopie zapasowe; kopie zapasowe są wykonywane na dysk zewnętrzny i VPN; kopie zapasowe są przechowane poza siedzibą Administratora; dostęp do kopii zapasowych posiada informatyk;
   e) Administrator nie stosuje nośników danych typu pendrive; dane osobowe nie są przetrzymywane na urządzeniach mobilnych;
7. W celu ochrony danych osobowych stosuje się następujące środki organizacyjne:
   a) monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane;
   b) kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco (Urządzenie NAS replikacja w serwerowni zapasowej);
   c) dostęp do kopii posiada Zarząd Spółki administratora oraz Administrator Systemu Informatycznego;
   d) przyrostowe kopie wykonywane są w zależności od ważności codziennie lub cotygodniowo na nośnik Ferro Beckup System, urządzenie NAS;
   e) uszkodzone nośniki z danymi osobowymi przed ich wyrzuceniem niszczy się fizycznie w sposób uniemożliwiający odtworzenie zawartości danych pod nadzorem inspektora ochrony danych;
   f) po wykorzystaniu wydruki zawierające dane osobowe niszczy się codziennie przed zakończeniem pracy w niszczarce; w miarę możliwości nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę administratora danych;
   g) zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronne zadrukowanych kart, jeśli zawierają one dane osobowe lub inne rodzaje informacji niejawnych.

Rozdział 6

Procedura DPIA

(Data Protection Impact Assessment)

1. Ocenę skutków dla ochrony danych osobowych (DPIA) przeprowadza każdorazowo administrator danych z wykorzystaniem załącznika nr 1.
2. DPIA jest przeprowadzana przy każdorazowej istotnej zmianie procesu przetwarzania danych osobowych, np. zmiana dostawcy usług, zmiana sposobu przetwarzania danych, wymiana zasobów biorących udział w procesie.

3. DPIA jest przeprowadzana wraz z analizą ryzyka nie rzadziej niż raz w roku w stosunku do procesów, które w wyniku poprzednio przeprowadzonego DPIA wykazały wysokie ryzyko dla praw i wolności osób, których dane dotyczą.

Rozdział 7

Procedura analizy ryzyka i plan postępowania z ryzykiem

1. Analizę ryzyka dla zasobów biorących udział w procesach przeprowadza administrator danych samodzielnie z wykorzystaniem załącznika nr 2.
2. Analiza ryzyka jest przeprowadzana nie rzadziej niż raz w roku i stanowi podstawę do aktualizacji sposobu postępowania z ryzykiem.
3. Na podstawie wyników przeprowadzonej analizy ryzyka, wskazani przez administratora danych właściciele procesów lub administrator danych samodzielnie wdrażają sposoby postępowania z ryzykiem.
4. Każdorazowo administrator danych wybiera sposób postępowania z ryzykiem i określa, które ryzyka i w jakiej kolejności będą rozpatrywane jako pierwsze.
5. Administrator danych nie może zlekceważyć ryzyk, których wartość przekracza 6 punktów zgodnie z załącznikiem nr 2 lub ryzyka w stosunku do zasobu, biorącego udział w procesie wysokiego ryzyka zgodnie z wynikiem DPIA zgodnie z załącznikiem nr 1.

Rozdział 8

Procedura współpracy z zatrudnionym personelem, upoważnionym współpracownikiem

1. Kontrola dostępu do systemu:
   a) Poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem udzielonego upoważnienia. Administrator danych przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem.
   b) W celu zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła, stosowania się do zaleceń administratora danych, inspektora ochrony danych, postanowień niniejszej Polityki.
   c) Upoważniony pracownik lub współpracownik zobowiązany jest do zachowania w tajemnicy swojego loginu i hasła do systemu informatycznego. Wzór polecenia przetwarzania danych osobowych jest Załącznikiem nr 5 do niniejszej Polityki.
2. Upoważniony pracownik lub współpracownik zobowiązany jest do zachowania w tajemnicy wszelkich informacji pozyskanych w związku z przetwarzaniem danych osobowych.
3. Upoważniony pracownik lub współpracownik zobowiązany jest do stosownego zabezpieczenia pomieszczenia, w którym przetwarzane są dane osobowe, za każdym razem, kiedy pomieszczenie to opuszcza.
4. Zabrania się podłączania do urządzeń stanowiących część systemu informatycznego służącego do przetwarzania danych nośników danych, które nie zostały przeznaczone do tego celu i które nie zostały sprawdzone pod kątem bezpieczeństwa przy zastosowaniu odpowiednich programów.
5. Upoważniony pracownik lub współpracownik zobowiązany jest do przetwarzania danych w sposób nie zagrażający ich bezpieczeństwu, w szczególności poprzez stosowanie się do zaleceń niniejszej Polityki.
6. Upoważniony pracownik lub współpracownik ponosi odpowiedzialność za nieuprawnione udostępnienie loginu lub hasła innym osobom, a także za niezabezpieczenie pomieszczenia przeznaczonego do przetwarzania danych osobowych.
7. Ujawnienie przez pracownika informacji dotyczących przetwarzanych danych osobowych stanowi poważne naruszenie obowiązków pracowniczych i może stanowić podstawę do rozwiązania umowy o pracę bez wypowiedzenia, a dla współpracownika rozwiązania umowy o współpracę.

Rozdział 9

Procedura współpracy z podmiotami zewnętrznymi

1. Każdorazowe skorzystanie z usług podmiotu przetwarzającego jest poprzedzone zawarciem umowy powierzenia przetwarzania danych osobowych zgodnie z załącznikiem nr 3.
2. Nie rzadziej niż raz w roku oraz każdorazowo przed zawarciem umowy powierzenia przetwarzania danych osobowych administrator danych weryfikuje zgodność z rozporządzeniem wszystkich podmiotów przetwarzających, z których usług korzysta lub ma zamiar skorzystać z wykorzystaniem listy kontrolnej.

Rozdział 10

Przeglądy polityka ochrony danych i kontroli systemu

i procedura domyślnej ochrony danych

1. Polityka ochrony danych powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych inspektor ochrony danych wskazuje administratorowi potrzebę aktualizacji polityki stosownie do potrzeb.
2. W przypadku zmian w budowie systemu informatycznego, zmian organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osób, czy też zmian w obowiązującym prawie administrator wdraża procedurę domyślnej ochrony danych.
3. Administrator danych w przypadku zamiaru rozpoczęcia przetwarzania danych osobowych w nowym procesie przeprowadza DPIA w stosunku do tego procesu.
4. W każdym przypadku tworzenia nowych usług administrator danych uwzględnia prawa osób, których dane dotyczą, na każdym kluczowym etapie jego projektowania i wdrażania.

Rozdział 11

Procedura zarządzania incydentami

1. W każdym przypadku naruszenia ochrony danych osobowych administrator danych weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
2. Administrator danych w przypadku stwierdzenia, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu 72 godz. od identyfikacji naruszenia.
3. Administrator danych zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia wobec nich naruszeń skutkujących ryzykiem naruszenia ich praw lub wolności, chyba że zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka wystąpienia ww. naruszenia.
4. Administrator danych dokumentuje naruszenia, które skutkują naruszeniem praw i wolności osób fizycznych.
5. Postępowanie w zakresie naruszenia ochrony danych osobowych określa załącznik nr 6.

Rozdział 12

Procedura realizacji praw osób

1. Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w rozporządzeniu administrator danych rozpatruje indywidualnie.
2. W zależności od ich ustawowych uprawnień w tym zakresie, administrator danych niezwłocznie realizuje następujące prawa osób, których dane dotyczą:
    a) prawo dostępu do danych,
    b) prawo do sprostowania danych,
    c) prawo do usunięcia danych,
    d) prawo do przenoszenia danych,
    e) prawo do sprzeciwu wobec przetwarzania danych,
3. W przypadku realizacji prawa do sprostowania, usunięcia i ograniczenia przetwarzania danych administrator danych niezwłocznie informuje odbiorców danych, którym udostępnił on przedmiotowe dane, chyba że jest to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
4. Administrator danych odmawia realizacji praw osób, których dane dotyczą, jeżeli możliwość taka wynika z przepisów rozporządzenia, jednak każda odmowa realizacji praw osób, których dane dotyczą, wymaga uzasadnienia z podaniem podstawy prawnej wynikającej z rozporządzenia.

Rozdział 13

Procedura odbierania zgód oraz informowania osób

1. W każdym przypadku pobierania danych bezpośrednio od osoby, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą, zgodnie z załącznikiem nr 4.
2. W każdym przypadku pobierania danych z innych źródeł niż osoba, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą, niezwłocznie, jednak nie później niż przy pierwszym kontakcie z osobą, której dane dotyczą, zgodnie z załącznikiem nr 4.
3. W każdym przypadku odbierania zgody od osoby, której dane dotyczą, korzysta się z klauzul zgody zgodnie z załącznikiem nr 4.

Rozdział 14

Postanowienia końcowe

1. Wszelkie zasady opisane w niniejszym dokumencie są przestrzegane przez osoby upoważnione do przetwarzania danych osobowych ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą.
2. Dokument niniejszy obowiązuje od dnia jego zatwierdzenia przez administratora danych.

Załączniki:

– *Arkusz DPIA (załącznik nr 1),*

– *Arkusz analizy ryzyka (załącznik nr 2),*

– *Umowa powierzenia przetwarzania danych osobowych (załącznik nr 3)*

– *Przykładowe klauzule (załącznik nr 4),*

- Polecenie przetwarzania danych osobowych (załącznik nr 5)

- Procedura w sytuacji naruszenia ochrony danych osobowych (załącznik nr 6),

- Zobowiązanie pracownika/współpracownika do zachowania poufności danych osobowych (załącznik nr 7)