POLITYKA OCHRONY DANYCH
Fabryka Narzędzi Specjalnych FERMOT S.A.

1. Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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. Niniejsza Polityka zawiera:
   a) opracowanie zasad ochrony danych osobowych obowiązujących w przedsiębiorstwie Administratora;
   b) odwołania do załączników doprecyzowujących procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych.
3. Zasady ochrony informacji określa niniejszy dokument wraz z Instrukcją.
4. Zasady zarządzania systemami informatycznymi określa Instrukcja.

§ 1 Definicje

1. **Dane Osobowe** – oznaczają wszelkie 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
2. **Dane wrażliwe** oznaczają Dane Osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.
3. **Eksport danych** oznacza przekazanie Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej.
4. **Instrukcja** – Instrukcja Zarządzania Systemem Informatycznym.
5. **IOD** lub **Inspektor** oznacza Inspektora Ochrony Danych Osobowych
6. **Osoba Fizyczna** oznacza osobę, której dane dotyczą.
7. **Procesor** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza Dane Osobowe w imieniu Administratora.
8. **Polityka Bezpieczeństwa** oznacza niniejszą dokumentację wraz z załącznikami.
9. **Profilowanie** oznacza dowolną formę zautomatyzowanego Przetwarzania Danych Osobowych, które polega na wykorzystaniu Danych Osobowych do oceny niektórych czynników osobowych Osoby Fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej Osoby Fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
10. **Przetwarzanie** oznacza 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. **RODO** oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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)
12. **Rejestr Przetwarzania** oznacza rejestr czynności Przetwarzania, o którym mowa w artykule 30 RODO.
13. **System Informatyczny** - (system) - sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną Administratora.
14. **Zbiór** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

§ 2 Ochrona danych osobowych w przedsiębiorstwie Administratora

1. Zasady ochrony danych. Administrator Przetwarza Dane Osobowe z poszanowaniem następujących zasad:
   a) **Zgodności z prawem, rzetelności i przejrzystości** – co oznacza, że Dane Osobowe Przetwarzane są przez Administratora zgodnie z prawem, rzetelnie i w sposób przejrzysty dla Osoby Fizycznej;
   b) **Ograniczenia celu** - co oznacza, że Administrator zbiera Dane Osobowe w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie Przetwarza ich dalej w sposób niezgodny z tymi celami;
   c) **Minimalizacji danych** - co oznacza, że Administrator zbiera Dane Osobowe w sposób adekwatny, stosowny oraz w sposób ograniczony do tego, co niezbędne do celów, w których Dane Osobowe są Przetwarzane;
   d) **Prawidłowości** – co oznacza dbałość Administratora o prawidłowość Danych Osobowych. Administrator dba o uaktualnienie Danych Osobowych, oraz odejmuje rozsądne działania, aby Dane Osobowe, które są nieprawidłowe w świetle celów ich Przetwarzania, zostały niezwłocznie usunięte;
   e) **Ograniczenia przechowywania** – co oznacza, że przechowywanie Danych Osobowych przez Administratora w formie umożliwiającej identyfikację Osoby Fizycznej przez okres nie dłużej niż jest to niezbędne co celów, w których Dane Osobowe te są Przetwarzane;
   f) **Integralności i poufności** – co oznacza że Administrator Przetwarza Dane Osobowe w sposób zapewniający odpowiednie bezpieczeństwo Danych Osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem Przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem za pomocą stosowanych w przedsiębiorstwie odpowiednich środków technicznych i organizacyjnych;
   g) **Rozliczalności** – co oznacza, że Administrator jest odpowiedzialny za przestrzeganie powyższych zasad, jak również jest w stanie wykazać ich przestrzeganie.
2. **System ochrony danych**. System ochrony Danych Osobowych w przedsiębiorstwie Administratora składa się z następujących elementów:

a) **Inwentaryzacja danych**. Administrator dokonuje zgodnie z zasadami opisanym w Polityce identyfikacji zasobów Danych Osobowych oraz identyfikacji sposobów wykorzystania danych, w tym:
   a. przypadków Przetwarzania danych wrażliwych;
   b. profilowania;
   c. współadministrowania danymi.

b) **Rejestr**. Administrator opracowuje, prowadzi i utrzymuje Rejestr Przetwarzania. Wzór Rejestru Przetwarzania stanowi Załącznik nr 1 do Polityki Bezpieczeństwa – „Wzór Rejestru Czynności Przetwarzania Danych". Rejestr Przetwarzania jest narzędziem rozliczania zgodności z ochroną danych. Administrator prowadzi Rejestr Przetwarzania w formie elektronicznej;

c) **Podstawy prawne**. Administrator zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania Danych Osobowych, zgodnie z postanowieniami §4 Polityki Bezpieczeństwa i rejestruje je w Rejestrze Przetwarzania, w tym:
   a. utrzymuje system zarządzania zgodami na Przetwarzanie Danych Osobowych i komunikację na odległość;
   b. inwentaryzuje przypadki, gdy Administrator przetwarza Dane Osobowe na podstawie prawnie uzasadnionego interesu Administratora.

d) **Obsługa praw jednostki**. Administrator spełnia obowiązki informacyjne względem Osób Fizycznych, których dane przetwarza, zgodnie z postanowieniami niniejszej Polityki Bezpieczeństwa, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, zgodnie z §6 Polityki Bezpieczeństwa w tym:
   a. **Obowiązki informacyjne**. Administrator przekazuje Osobom Fizycznym podczas pozyskiwania Danych Osobowych wymagane informacje zgodnie z Artykułem 13 RODO albo w przypadku pozyskania Danych Osobowych w sposób niż od osoby, której dane dotyczą zgodnie z Artykułem 14 RODO oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków, zgodnie z §7 Polityki Bezpieczeństwa;
   b. **Możliwość wykonania żądań**. Administrator weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich Procesorów, zgodnie z §8 Polityki Bezpieczeństwa.

e) **Obsługa żądań**. Administrator zapewnia odpowiednie nakłady, aby żądania Osób Fizycznych były realizowane w terminach i w sposób wymagany przez RODO i dokumentowane, zgodnie z §8 Polityki Bezpieczeństwa;

f) **Zawiadamianie o naruszeniach**. Administrator stosuje procedury, zgodnie z Załącznikiem nr 6 (Procedura postępowania w przypadku naruszenia bezpieczeństwa Systemu Informatycznego), pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony Danych Osobowych, zgodnie z §11 ust. 4 Polityki Bezpieczeństwa. Zawiadomienie Administrator dokonuje zgodnie ze wzorem zgłoszenia w sprawie naruszenia Danych Osobowych, którego wzór stanowi Załącznik nr 2;

g) **Minimalizacja**. Administrator posiada zasady i metody zarządzania minimalizacją (privacy by default), zgodnie z §10 Polityki Bezpieczeństwa, a w tym:
   a. zasady zarządzania adekwatnością Danych Osobowych;
   b. zasady reglamentacji i zarządzania dostępem do Danych Osobowych;
   c. zasady zarządzania okresem przechowywania Danych Osobowych i weryfikacji dalszej przydatności.

h) **Bezpieczeństwo**. Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, zgodnie z §11 Polityki Bezpieczeństwa, w tym:
   a. przeprowadza analizy ryzyka dla czynności przetwarzania Danych Osobowych lub ich kategorii;
   b. przeprowadza oceny skutków dla ochrony Danych Osobowych tam, gdzie ryzyko naruszenia praw i wolności Osób Fizycznych jest wysokie;
   c. dostosowuje środki ochrony Danych Osobowych do ustalonego ryzyka;
   d. posiada system zarządzania bezpieczeństwem informacji;
   e. stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony Danych Osobowych Urzędowi Ochrony Danych − zarządza incydentami.

i) **Procesorzy**. Administrator powierza Przetwarzanie Danych Osobowych na rzecz Administratora, według wymogów i warunków przetwarzania na podstawie umowy powierzenia;

j) **Eksport danych**. Administrator weryfikuje, czy nie przekazuje Danych Osobowych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych;

k) **Privacy by design**. Administrator zarządza zmianami mającymi wpływ na prywatność. Uruchomienie nowych projektów i inwestycji u Administratora uwzględnia konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu;

l) **Przetwarzanie transgraniczne**. Administrator posiada zasady weryfikacji, kiedy zachodzą przypadki Przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

§ 3 Inwentaryzacja

1. Dane wrażliwe. Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać dane wrażliwe oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania danych wrażliwych. W przypadku zidentyfikowania przypadków przetwarzania danych wrażliwych, Administrator postępuje zgodnie z przyjętymi zasadami w tym zakresie, opisanymi w Załączniku nr 8 – zasady postępowania przy przetwarzaniu danych wrażliwych.
2. Dane niezidentyfikowane. Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.
3. Profilowanie. Administrator identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji, Administrator postępuje zgodnie z przyjętymi zasadami w tym zakresie, opisanymi w Załączniku nr 9 – Zasady postępowania w przypadku zautomatyzowanego podejmowania decyzji.
4. Współadministrowanie. Administrator identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami, opisanymi zgodnie z załącznikiem nr 10 – Zasady współadministrowania danymi.

§ 4 Rejestr Przetwarzania

1. RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
2. Administrator prowadzi Rejestr Przetwarzania, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.
3. Rejestr Przetwarzania jest jednym z podstawowych narzędzi umożliwiających Administratorowi rozliczanie większości obowiązków ochrony danych.
4. W Rejestrze Przetwarzania, dla każdej czynności przetwarzania danych, którą Administrator uznał za odrębną dla potrzeb Rejestru Przetwarzania, Administrator odnotowuje co najmniej:
   a) nazwę czynności;
   b) cel przetwarzania;
   c) opis kategorii osób;
   d) opis kategorii danych;
   e) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Administratora, jeśli podstawą jest uzasadniony interes;
   f) sposób zbierania danych;
   g) opis kategorii odbiorców danych (w tym Procesorów);
   h) informację o przekazaniu poza EU/EOG;
   i) ogólny opis technicznych i organizacyjnych środków ochrony danych.
5. Wzór Rejestru Przetwarzania zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Administrator rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru Przetwarzania ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.

§ 5 Podstawy przetwarzania

1. Administrator dokumentuje w Rejestrze Przetwarzania podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
2. Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Administratora) Administrator dookreśla podstawę w czytelny sposób, gdy jest to potrzebne. Np. dla zgody wskazując na jej zakres, gdy podstawą jest prawo – wskazując na konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując na kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń.
3. Administrator wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

§ 6 Sposób obsługi praw jednostki i obowiązków informacyjnych

1. Administrator dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
2. Administrator ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej Administratora informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu z Administratorem.
3. Administrator dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.
4. Administrator wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
5. W celu realizacji praw jednostki Administrator zapewnia mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Administratora, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,
6. Administrator dokumentuje obsługę zawiadomień i żądań osób, zgodnie ze wzorem stanowiącym załącznik nr 4 do Polityki

§ 7 Obowiązki informacyjne

1. Administrator określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
2. Administrator informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
3. Administrator informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
4. Administrator informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.
5. Administrator informuje osobę o planowanej zmianie celu przetwarzania danych.
6. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania.
7. Administrator informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
8. Administrator informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
9. Administrator bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

§ 8 Prawa Osób Fizycznych

1. Administrator przestrzega, aby prawa Osób Fizycznych były realizowane zgodnie z obowiązującym przepisami prawa, dając tym samym gwarancję ochrony praw i wolności Osób Fizycznych.
2. Administrator zapewnia realizację praw Osób Fizycznych poprzez stosowanie odpowiednich procedur opisanych w załączniku nr 7 do Polityki Bezpieczeństwa, w tym:

a) prawo dostępu – uzyskania informacji od Administratora czy przetwarza on dane osoby której dane dotyczą;
b) prawo do sprostowania;
c) prawo do usunięcia danych;
d) prawo do ograniczenia przetwarzania;
e) prawo do przenoszenia danych;
f) prawo do sprzeciwu w zakresie przetwarzania danych osobowych oraz;
g) prawo do sprzeciwu w przypadku zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach (w tym profilowanie).

3. **Nieprzetwarzanie**. Administrator informuje Osobę Fizyczną o tym, że nie przetwarza Danych Osobowych jej dotyczących, jeśli taka Osoba Fizyczna zgłosiła żądanie dotyczące jej praw.
4. **Odmowa**. Administrator informuje Osobę Fizyczną, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
5. **Dostęp do danych**. Na żądanie Osoby Fizycznej dotyczące dostępu do jej Danych Osobowych, Administrator informuje Osobę Fizyczną, czy przetwarza jej Dane Osobowe oraz informuje Osobę Fizyczną o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela Osobie Fizycznej dostępu do Danych Osobowych jej dotyczących. Dostęp do Danych Osobowych może być zrealizowany przez wydanie kopii Danych Osobowych, z zastrzeżeniem, że kopii Danych Osobowych wydanej w wykonaniu prawa dostępu do Danych Osobowych Administrator nie uzna za pierwszą nieodpłatną kopię Danych Osobowych dla potrzeb opłat za kopie Danych Osobowych.
6. **Kopie danych**. Na żądanie Administrator wydaje Osobie Fizycznej kopię Danych Osobowych jej dotyczących i odnotowuje fakt wydania pierwszej kopii Danych Osobowych. Administrator wprowadza i utrzymuje cennik kopii Danych Osobowych, zgodnie z którym pobiera opłaty za kolejne kopie Danych Osobowych. Cena kopii Danych Osobowych skalkulowana jest w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii Danych Osobowych.
7. **Sprostowanie danych**. Administrator dokonuje sprostowania nieprawidłowych Danych Osobowych na żądanie Osoby Fizycznej. Administrator ma prawo odmówić sprostowania Danych Osobowych, chyba że Osoba Fizyczna w rozsądny sposób wykaże nieprawidłowości Danych Osobowych, których sprostowania się domaga. Administrator informuje o sprostowaniu Danych Osobowych, każdego odbiorcę, któremu ujawniono Dane Osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje Osobę Fizyczną, której Dane Osobowe dotyczą, o tych odbiorcach, jeżeli Osoba Fizyczna, której Dane Osobowe dotyczą, tego zażąda.
8. **Uzupełnienie danych**. Administrator uzupełnia i aktualizuje Dane Osobowe na żądanie Osoby Fizycznej. Administrator ma prawo odmówić uzupełnienia Danych Osobowych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania Danych Osobowych (Administrator nie przetwarza danych, które są mu zbędne). Administrator może polegać na oświadczeniu Osoby Fizycznej, co do uzupełnianych Danych Osobowych, chyba że będzie to niewystarczające w świetle przyjętych przez Administratora procedur (np. co do pozyskiwania takich Danych Osobowych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
9. **Usunięcie danych**. Na żądanie Osoby Fizycznej, Administrator usuwa Dane Osobowe,

gdy:

a) Dane Osobowe nie są niezbędne do celów, w których zostały zebrane ani Przetwarzane w innych celach;
b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej Przetwarzania;
c) Osoba Fizyczna wniosła skuteczny sprzeciw względem Przetwarzania tych Danych Osobowych;
d) Dane Osobowe były Przetwarzane niezgodnie z prawem;
e) konieczność usunięcia wynika z obowiązku prawnego.

Administrator określa sposób obsługi prawa do usunięcia Danych Osobowych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony Danych Osobowych, w tym bezpieczeństwa.

Jeżeli Dane Osobowe podlegające usunięciu zostały upublicznione przez Administratora, Administrator podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te Dane Osobowe, o potrzebie usunięcia Danych Osobowych i dostępu do nich.

W przypadku usunięcia Danych Osobowych Administrator informuje Osobę Fizyczną o odbiorcach Danych Osobowych, na żądanie tej osoby.

10. **Ograniczenie przetwarzania**. Administrator dokonuje ograniczenia przetwarzania Danych Osobowych na żądanie Osoby Fizycznej, gdy:
    a) Osoba Fizyczna kwestionuje prawidłowość Danych Osobowych – na okres pozwalający sprawdzić ich prawidłowość;
    b) Przetwarzanie jest niezgodne z prawem, a Osoba Fizyczna, której Dane Osobowe dotyczą, sprzeciwia się usunięciu Danych Osobowych, żądając w zamian ograniczenia ich wykorzystywania;
    c) Administrator nie potrzebuje już Danych Osobowych, ale są one potrzebne Osobie Fizycznej, do ustalenia, dochodzenia lub obrony roszczeń;
    d) Osoba Fizyczna wniosła sprzeciw względem Przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

§ 9 W trakcie ograniczenia przetwarzania Administrator przechowuje Dane Osobowe, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody Osoby Fizycznej, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

Administrator informuje Osobę Fizyczną przed uchyleniem ograniczenia Przetwarzania.

W przypadku ograniczenia przetwarzania danych Administrator informuje Osobę Fizyczną o odbiorcach danych, na żądanie tej Osoby Fizycznej.

1. **Przenoszenie danych**. Na żądanie osoby Administrator wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego (csv, który jest formatem powszechnie używanym) lub przekazuje innemu podmiotowi, jeśli jest to możliwe, Dane Osobowe dotyczące tej osoby, które dostarczyła ona Administratorowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Administratora.

2. **Sprzeciw w szczególnej sytuacji**. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej Danych Osobowych, a Dane Osobowe Przetwarzane są przez Administratora w oparciu o uzasadniony interes lub powierzono Administratorowi zadanie w interesie publicznym, Administrator uwzględni sprzeciw, o ile nie zachodzą po stronie Administratora ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
3. **Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych**. Jeżeli Administrator prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Administrator uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.
4. **Sprzeciw względem marketingu bezpośredniego**. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Administratora na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Administrator uwzględni sprzeciw i zaprzestanie takiego przetwarzania.
5. **Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu**. Jeżeli Administrator przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę, Administrator zapewnia możliwość odwołania się do interwencji i decyzji osoby po stronie Administratora, chyba że taka automatyczna decyzja:
   a) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Administratorem lub;
   b) jest wprost dozwolona przepisami prawa lub;
   c) opiera się o wyraźną zgodę odwołującej osoby.

§ 10 Minimalizacja

1. Administrator dba o minimalizację Przetwarzania Danych Osobowych pod kątem:
   a) adekwatności Danych Osobowych do celów (ilości danych i zakresu przetwarzania);
   b) dostępu do Danych Osobowych;
   c) czasu przechowywania Danych Osobowych.
2. **Minimalizacja zakresu**. Administrator zweryfikował zakres pozyskiwanych Danych Osobowych, zakres ich przetwarzania i ilość przetwarzanych Danych Osobowych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.
3. Administrator dokonuje okresowego przeglądu ilości przetwarzanych Danych Osobowych i zakresu ich przetwarzania nie rzadziej niż raz na rok.
4. Administrator przeprowadza weryfikację zmian co do ilości i zakresu Przetwarzania Danych Osobowych w ramach zarządzania zmianą (privacy by design).
5. **Minimalizacja dostępu**. Administrator stosuje ograniczenia dostępu do Danych Osobowych:
   a) prawne (zobowiązania do poufności, zakresy upoważnień);
   b) fizyczne (strefy dostępu, zamykanie pomieszczeń);
   c) logiczne (ograniczenia uprawnień do systemów przetwarzających Dane Osobowe

i zasobów sieciowych, w których rezydują Dane Osobowe).

6. Administrator stosuje kontrolę dostępu fizycznego.
7. Administrator dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach Procesorów.
8. Administrator dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.
9. Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są poniżej w treści Polityki.
10. **Minimalizacja czasu**. Administrator wdraża mechanizmy kontroli cyklu życia danych osobowych u Administratora, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze Przetwarzania.
11. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów produkcyjnych Administratora, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Administratora.

§ 11 Bezpieczeństwo

1. Administrator zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Administratora.
2. **Analizy ryzyka i adekwatności środków bezpieczeństwa**. Administrator przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:
   a) Administrator zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych;
   b) Administrator kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają;
   c) Administrator przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Administrator analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia;
   d) Administrator ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Administrator ustala przydatność i stosuje takie środki i podejście jak:
      a. pseudonimizacja;
      b. szyfrowanie Danych Osobowych;
      c. inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
      d. środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności Danych Osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

3. **Oceny skutków dla ochrony danych**. Administrator dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.
4. **Środki bezpieczeństwa**. Administrator stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.
5. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa i są bliżej opisane zarówno w treści niniejszej Polityki jak i w Instrukcji Zarządzania Systemem Informatycznym.
6. **Zgłaszanie naruszeń**. Administrator stosuje procedury, zgodnie z załącznikiem nr 5 - Procedura postępowania w przypadku naruszenia bezpieczeństwa przetwarzania, pozwalające na identyfikację i ocenę czy doszło do naruszenia ochrony danych, w przypadku ujawnienia naruszenia danych osobowych na podstawie wzoru stanowiącego załącznik nr 2 (wzór zgłoszenia w sprawie naruszenia danych osobowych), zgłasza zidentyfikowane naruszenie Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.
7. Administrator prowadzi również rejestr naruszeń zgodnie ze wzorem stanowiącym Załącznik nr 3 do Polityki.

§ 12 Procesorzy

1. Administrator powierza Przetwarzanie Danych Osobowych jedynie podmiotom dającym wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Administratorze.
2. Administrator przyjął minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące Załącznik nr 5 do Polityki – Wzór umowy powierzenia przetwarzania danych.

§ 13 Eksport Danych

1. Administrator rejestruje w Rejestrze Przetwarzania przypadki eksportu Danych Osobowych, czyli przekazywania Danych Osobowych poza Europejski Obszar Gospodarczy (Unia Europejska, Islandia, Lichtenstein i Norwegia).
2. W celu uniknięcia sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych (shadow IT), Administrator okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.

§ 14 Projektowanie Prywatności

1. Administrator zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.
2. W tym celu prowadzenie projektów i inwestycji przez Administratora odwołuje się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

§ 15 Wykaz Zbiorów Danych Osobowych

1. W niniejszym paragrafie znajdują się Zbiory Danych Osobowych Przetwarzane przez Administratora:
2. **Kandydaci do pracy**

   Zbiór prowadzony w formie papierowej oraz z użyciem systemów informatycznych.

   Systemy informatyczne, przy pomocy których przetwarzane są dane osobowe:

   a) Panel internetowy poczty elektronicznej;

   Miejsca, w których Przetwarzane są Dane Osobowe

   a) ul. Sobieskiego 71, 96-100 Skierniewice

   W zbiorze gromadzone są następujące kategorie Danych Osobowych:

   a) adres e-mail;

   b) adres korespondencyjny (ulica, miasto, kod pocztowy);

   c) doświadczenie zawodowe i historia zatrudnienia;

   d) imię;

   e) nazwisko;

   f) numer telefonu;

   g) umiejętności;

   h) wykształcenie, kursy i szkolenia;

   Zbiór Danych Osobowych zawiera Dane Osobowe kandydatów do pracy. Dane są pozyskiwane bezpośrednio od osób, których dotyczą. Kandydaci do pracy przesyłają aplikacje drogą elektroniczną na wskazany adres e-mail albo za pośrednictwem Poczty Polskiej albo przynoszą aplikację osobiście do siedziby Administratora Danych Osobowych.

   Przepływ Danych Osobowych

   Dane osobowe gromadzone są w formie papierowej oraz systemie poczty elektronicznej i nie następuje ich przepływ do innych systemów informatycznych. Dane Osobowe są wprowadzane ręcznie do Systemu Informatycznego instytucji bankowej bzwbk.pl.

   Dane Osobowe są powierzane następującym podmiotom:

   a) BIURO RACHUNKOWE "DUET" DOROTA DAŃCZAK, ul. dr. Stanisława Rybickiego 8, 96-100 Skierniewice, REGON: 750203283, NIP: 8361053200. Dane Osobowe są powierzane w celu świadczenia na rzecz Administratora Danych Osobowych usług kadrowo-księgowych, rozliczeń finansowych oraz rozliczeń podatkowych.

   Dane Osobowe są udostępniane następującym podmiotom:

   a) BANK ZACHODNI WBK S.A., ul. Rynek 9/11, 50-950 Wrocław, REGON: 930041341, NIP: 8960005673. Dane Osobowe są udostępniane w celu świadczenia usług bankowych.

   Dane osobowe pozyskiwane są z następujących źródeł

   a) Zgoda w formie papierowej

b) Zgoda wysłana poprzez e-mail

3. **Klienci firmy**

Zbiór prowadzony w formie papierowej oraz z użyciem systemów informatycznych.

Systemy informatyczne, przy pomocy których przetwarzane są dane osobowe:

a) Gratyfikant GT;

b) Panel Administracyjny dhl.com.pl;

c) Panel Administracyjny jasfbg.com.pl;

d) Panel Administracyjny Strony Internetowej;

e) Panel Administracyjny webklient.dpd.com.pl;

f) Panel bankowości elektronicznej bzwbk.pl;

g) Panel internetowy poczty elektronicznej;

h) Plan-de-CAMpagne;

Miejsca, w których Przetwarzane są Dane Osobowe

a) ul. Sobieskiego 71, 96-100 Skierniewice

W zbiorze gromadzone są następujące kategorie Danych Osobowych:

a) adres e-mail;

b) adres korespondencyjny (ulica, miasto, kod pocztowy);

c) adres zamieszkania lub pobytu (ulica, miasto, kod pocztowy);

d) firma przedsiębiorcy;

e) imię;

f) nazwisko;

g) NIP;

h) numer telefonu;

W zbiorze przetwarzane są dane osobowe klientów firmy.

Przepływ Danych Osobowych

Dane Osobowe są wprowadzane ręcznie do Systemu Informatycznego instytucji bankowej bzwbk.pl. Dane osobowe tj. imię i nazwisko, adres dostawy oraz numer telefonu wprowadzane są ręcznie przez Osobę Upoważnioną do systemu informatycznego jasfbg.com.pl. Dane osobowe tj. imię i nazwisko, adres dostawy oraz numer telefonu wprowadzane są ręcznie przez Osobę Upoważnioną do systemu informatycznego webklient.dpd.com.pl. Dane osobowe tj. imię i nazwisko, adres dostawy oraz numer telefonu wprowadzane są ręcznie przez Osobę Upoważnioną do systemu informatycznego dhl.com.pl.

Dane Osobowe są powierzane następującym podmiotom:

a) TRANSPORT CIĘŻAROWY ZBIGNIEW SOSNOWSKI, ul. Strusia 15, 85-447 Bydgoszcz, REGON: 090536182, NIP: 9670050660. Dane Osobowe są powierzane w celu świadczenia usługi dostawy paczki lub korespondencji.

b) PPH "STAN MAX" S.C. KRYSTYNA STANIAK, JACEK STANIAK, ul. Warszawska 41, 96-332 Radziwiłłów, REGON: 016255325, NIP: 8361149259.

Dane Osobowe są powierzane w celu świadczenia usługi dostawy paczki lub korespondencji.

c) JAS-FBG S.A., ul. Kolejowa 17, 40-706 Katowice, REGON: 271069438, NIP: 6330003565. Dane Osobowe są udostępniane w celu świadczenia usługi dostawy przesyłki lub korespondencji.
d) BARTOSZ DYBOWSKI DYBI-TRANS, ul. Konwaliowa 37, 96-100 Skierniewice, REGON: 100321238, NIP: 8361791642. Dane Osobowe są powierzane w celu świadczenia usługi dostawy paczki lub korespondencji.
e) DPD Polska Sp. z o.o., ul. Mineralna 15, 02-274 Warszawa, REGON: 012026421, NIP: 5260204110. Dane Osobowe są udostępniane w celu świadczenia usługi dostawy paczki lub korespondencji.
f) DHL Express (Poland) sp. z o.o., ul. Osmańska 2, 02 - 823 Warszawa, REGON: 012005407, NIP: 5270022391. Dane Osobowe są udostępniane w celu świadczenia usługi dostawy przesyłki lub korespondencji.
g) BIURO RACHUNKOWE "DUET" DOROTA DAŃCZAK, ul. dr. Stanisława Rybickiego 8, 96-100 Skierniewice, REGON: 750203283, NIP: 8361053200. Dane Osobowe są powierzane w celu świadczenia na rzecz Administratora Danych Osobowych usług kadrowo-księgowych, rozliczeń finansowych oraz rozliczeń podatkowych.

Dane Osobowe są udostępniane następującym podmiotom:

a) BANK ZACHODNI WBK S.A., ul. Rynek 9/11, 50-950 Wrocław, REGON: 930041341, NIP: 8960005673. Dane Osobowe są udostępniane w celu świadczenia usług bankowych.

Dane osobowe pozyskiwane są z następujących źródeł

a) Zamówienia przez stronę WWW

4. **Kontrahenci firmy**

Zbiór prowadzony w formie papierowej oraz z użyciem systemów informatycznych.

Systemy informatyczne, przy pomocy których przetwarzane są dane osobowe:

a) Panel bankowości elektronicznej bzwbk.pl;
b) Panel internetowy poczty elektronicznej;

Miejsca, w których Przetwarzane są Dane Osobowe

a) ul. Sobieskiego 71, 96-100 Skierniewice

W zbiorze gromadzone są następujące kategorie Danych Osobowych:

a) adres e-mail;
b) adres korespondencyjny (ulica, miasto, kod pocztowy);
c) adres zamieszkania lub pobytu (ulica, miasto, kod pocztowy);
d) firma przedsiębiorcy;
e) imię;
f) nazwisko;
g) NIP;
h) numer telefonu;

i) REGON;

W zbiorze przetwarzane są dane osobowe kontrahentów firmy.

Przepływ Danych Osobowych

Dokumenty zawierające Dane Osobowe tj. umowy i faktury są przesyłane za pośrednictwem poczty elektronicznej. Dokumenty są przesyłane pocztą elektroniczną do firmy świadczącej usługi księgowe, z którą współpracuje Administrator Danych Osobowych w celu wykonywania obowiązku ustawowego w zakresie rozliczeń podatkowo księgowych. W zakresie rozliczeń finansowych Dane Osobowe są wprowadzane w systemie bankowym w celu wykonania płatności przez Administratora Danych Osobowych faktury na rzecz kontrahenta. Dane Osobowe są wprowadzane ręcznie do Systemu Informatycznego instytucji bankowej bzwbk.pl.

Dane Osobowe są powierzane następującym podmiotom:

a) BIURO RACHUNKOWE "DUET" DOROTA DAŃCZAK, ul. dr. Stanisława Rybickiego 8, 96-100 Skierniewice, REGON: 750203283, NIP: 8361053200. Dane Osobowe są powierzane w celu świadczenia na rzecz Administratora Danych Osobowych usług kadrowo-księgowych, rozliczeń finansowych oraz rozliczeń podatkowych.

Dane Osobowe są udostępniane następującym podmiotom:

a) BANK ZACHODNI WBK S.A., ul. Rynek 9/11, 50-950 Wrocław, REGON: 930041341, NIP: 8960005673. Dane Osobowe są udostępniane w celu świadczenia usług bankowych.

Dane osobowe pozyskiwane są z następujących źródeł

a) Zawarcie umowy w formie papierowej
b) Zawarcie umowy w formie elektronicznej
c) Zawarcie umowy cywilno-prawnej

5. **Pracownicy i współpracownicy**

Zbiór prowadzony w formie papierowej oraz z użyciem systemów informatycznych.

Systemy informatyczne, przy pomocy których przetwarzane są dane osobowe:

a) Gratyfikant GT;
b) Panel Administracyjny Strony Internetowej;
c) Panel bankowości elektronicznej bzwbk.pl;
d) Panel internetowy poczty elektronicznej;
e) Plan-de-CAMpagne;
f) Płatnik;

Miejsca, w których Przetwarzane są Dane Osobowe

a) ul. Sobieskiego 71, 96-100 Skierniewice

W zbiorze gromadzone są następujące kategorie Danych Osobowych:

a) adres korespondencyjny (ulica, miasto, kod pocztowy);
b) adres zamieszkania lub pobytu (ulica, miasto, kod pocztowy);
c) doświadczenie zawodowe i historia zatrudnienia;

d) firma przedsiębiorcy;

e) imię;

f) nazwisko;

g) NIP;

h) PESEL;

i) stanowisko pracy;

j) umiejętności;

k) wykształcenie, kursy i szkolenia;

l) zawód;

Zbiór prowadzony jest w Systemie Informatycznym. Zawiera Dane Osobowe pracowników i współpracowników.

Przepływ Danych Osobowych

Dane Osobowe są wprowadzane ręcznie do Systemu Informatycznego instytucji bankowej bzwbk.pl.

Dane Osobowe są powierzane następującym podmiotom:

a) BIURO RACHUNKOWE "DUET" DOROTA DAŃCZAK, ul. dr. Stanisława Rybickiego 8, 96-100 Skierniewice, REGON: 750203283, NIP: 8361053200. Dane Osobowe są powierzane w celu świadczenia na rzecz Administratora Danych Osobowych usług kadrowo-księgowych, rozliczeń finansowych oraz rozliczeń podatkowych.

Dane Osobowe są udostępniane następującym podmiotom:

a) BANK ZACHODNI WBK S.A., ul. Rynek 9/11, 50-950 Wrocław, REGON: 930041341, NIP: 8960005673. Dane Osobowe są udostępniane w celu świadczenia usług bankowych.

Dane osobowe pozyskiwane są z następujących źródeł

a) Zawacie umowy o pracę

b) Zawarcie umowy cywilno-prawnej

§ 16 Szkolenia

1. Administrator Danych Osobowych jest odpowiedzialny za zapewnianie zapoznania osób upoważnionych do Przetwarzania z przepisami o ochronie danych osobowych, w szczególności poprzez organizację szkoleń w tym zakresie. Każda osoba upoważniona do Przetwarzania danych ma obowiązek uczestniczenia w tych szkoleniach.
2. Szkolenie powinno w szczególności dotyczyć:
   a) obowiązujących przepisów prawa ochrony danych osobowych;
   b) procedur stosowanych przez Administratora Danych Osobowych w celu Przetwarzania zgodnego z prawem.

§ 17 Zabezpieczenia Fizyczne Pomieszczeń

1. W niniejszym rozdziale znajduje się opis środków technicznych podjętych przez Administratora Danych Osobowych w celu zapewnienia poufności, integralności i rozliczalności Przetwarzanych Danych Osobowych.
2. Fizyczne lokalizacje i miejsca w których Przetwarzane są Dane Osobowe.

a) ul. Sobieskiego 71, 96-100 Skierniewice
Pomieszczenia biurowe na pierwszym piętrze - biuro Technologów, Kierownika Wydziału Mechanicznego, Wiceprezesa WM, Prezesa, Wiceprezesa WN, Logistyki, Utrzymania Ruchu, BHP, Kadr, Sekretariat.

Dodatkowe zabezpieczenia:

-
-

.

3. Dokumenty papierowe zawierające Dane Osobowe przeznaczone do zniszczenia, niszczone są przy użyciu niszczarek, które znajdują się na standardowym wyposażeniu pomieszczeń, w których przetwarzane są dane osobowe lub są dostępne w holu. Użyte urządzenia służące do niszczenia zapewniają odpowiedni poziom fragmentacji dokumentów, uniemożliwiając ich odtworzenie.

§ 18 Postanowienia Końcowe

1. Niniejsza Polityka Bezpieczeństwa wchodzi w życie w dniu 16.05.2018 r.
2. Załączniki do Polityki Bezpieczeństwa:
   a) Załącznik nr. 1 - Rejestr czynności przetwarzania danych osobowych;
   b) Załącznik nr. 2 - Wzór zgłoszenia naruszenia;
   c) Załącznik nr. 3 - Wzór rejestru naruszeń;
   d) Załącznik nr. 4 - Wzór rejestru zawiadomień i żądań osób których dane dotyczą;
   e) Załącznik nr. 5 - Wzór umowy powierzenia danych osobowych;
   f) Załącznik nr. 6 - Procedura postępowania w przypadku naruszenia bezpieczeństwa Systemu Informatycznego;
   g) Załącznik nr. 7 - Wykaz procedur praw osób których dane dotyczą;
   h) Załącznik nr. 8 - Zasady postępowania przy przetwarzaniu danych wrażliwych;
   i) Załącznik nr. 9 - Zasady postępowania w przypadku zautomatyzowanego podejmowania decyzji;
   j) Załącznik nr. 10 - Zasady współadministrowania danymi.