CashBill

21.05.2018 r.

Polityka Ochrony Danych Osobowych

Polityka Ochrony Danych Osobowych CashBill S.A. z siedzibą w Katowicach z dnia 21 maja 2018 r.

+48 32 438 45 00 || kontakt@cashbill.pl
CashBill Spółka Akcyjna ul. Sobieskiego 2, 40-082 Katowice
NIP: 629-241-08-01, REGON: 241048572, KRS: 0000323297, Kapitał zakładowy: 5 000 000 zł

Spis treści

Uwzględniając obowiązki wynikające z art. 25 oraz art. 32 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) (Dz.Urz. UE L 119, s. 1), celem zapewnienia, że Dane osobowe w Spółce Cashbill Spółka Akcyjna są przetwarzane i zabezpieczone zgodnie z postanowieniami prawa poprzez wdrożenia odpowiednich środków technicznych i organizacyjnych zaprojektowanych w celu skutecznej realizacji zasad ochrony danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń; a CashBill Spółka Akcyjna z siedzibą w Katowicach zapewnia, że domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

1 Postanowienia wstępne

1.1. Polityka określa zasady przetwarzania oraz zabezpieczania Danych osobowych w Przedsiębiorstwie celem zapewnienia zbieżności Przetwarzania z wymaganiami RODO oraz przepisami bezwzględnie obowiązującego prawa polskiego w zakresie przetwarzania danych osobowych. Polityka stanowi zbiór oraz podstawę wdrażanych w Przedsiębiorstwie wymogów, procedur oraz zasad ochrony danych osobowych. Polityka zawiera:

i) zawiera opis zasad ochrony danych obowiązujących w Przedsiębiorstwie;

ii) zbiór procedur, instrukcji i regulacji szczegółowych dotyczących przetwarzania Danych osobowych w Przedsiębiorstwie, dotyczących poszczególnych obszarów z zakresu ochrony danych osobowych; stanowiących załączniki do Polityki.

1.2. Polityka obowiązuje wszystkich Pracowników oraz współpracowników Przedsiębiorstwa. Za przestrzeganie i utrzymanie postanowień Polityki odpowiedzialni są:

i) Przedsiębiorstwo;

ii) komórki organizacyjne utworzone w Przedsiębiorstwie, w których przetwarzane są Dane osobowe;

iii) Pracownicy.

1.3. Dla skutecznej realizacji Polityki, uwzględniając zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia Przedsiębiorstwo zapewnia:

i) wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających zgodność przetwarzania Danych osobowych z wymogami prawa oraz niezbędne zabezpieczenie przetwarzanych danych osobowych;

ii) zabezpieczenie zasobów systemów informatycznych, infrastruktury technicznej, sprzętu i osprzętu przed zniszczeniem, uszkodzeniem lub kradzieżą;

iii) uniemożliwienie dostępu do Danych osobowych zawartych w systemach informatycznych oraz przechowywyanych w formie papierowej osobom do tego nieupoważnionym;

iv) stałe monitorowanie zgodności przetwarzania Danych osobowych z wymogami prawa oraz poddawanie środków, o których mowa w ust. powyżej ciągłym przeglądom oraz uaktualnianiu;

v) kontrolę i nadzór nad przetwarzaniem Danych osobowych.

1.4. Nadzór nad przestrzeganiem postanowień Polityki zapewnia Zarząd Przedsiębiorstwa. Nadzór, o którym mowa w zdaniu poprzedzającym zmierza w szczególności, ale nie wyłącznie do zapewnienia, że czynności związane z przetwarzaniem Danych osobowych w Przedsiębiorstwie są zgodne z wymogami prawa oraz postanowieniami Polityki.

1.5. Przedsiębiorstwo zapewnia zgodność postępowania kontrahentów Przedsiębiorstwa, w tym w szczególności Podmiotów Przetwarzających z postanowieniami Polityki w odpowiednim zakresie we wszystkich sytuacjach, w których dochodzi do przekazania tym podmiotom Danych osobowych do przetwarzania, w tym przechowywania.

1.6. Polityka jest przechowywana i udostępniana w wersji papierowej oraz elektronicznej w siedzibie Przedsiębiorstwa.

1.7. Politykę udostępnia się:

i) obligatoryjnie wszystkim osobom upoważnionym do przetwarzania Danych osobowych w Przedsiębiorstwie, celem zapewnienia osobom upoważnionym należytej wiedzy oraz informacji na temat zasad i wymogów dotyczących przetwarzania Danych Osobowych w Przedsiębiorstwie;

ii) osobom zainteresowanym, w szczególności osobom fizycznym, których dane dotyczą – na ich wniosek.

2 Słownik pojęć

2.1. Ilekroć w niniejszej Polityce zostaną wykorzystane poniższe definicje lub zwroty, należy nadawać im następujące znaczenie:

i) Administrator Systemu Informatycznego – oznacza osobę odpowiedzialną za nadzór i bezpieczeństwo nad systemami informatycznymi użytkowanymi w Przedsiębiorstwie oraz infrastrukturą IT;

ii) Dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, takie 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; o których mowa w art. 4 pkt 1 RODO;

iii) Dane wrażliwe – oznaczają Dane Osobowe, o których mowa w art. 9 RODO;

iv) Dokumenty z danymi osobowymi – oznaczają wszelkie dokumenty, w których zawarte są dane osobowe, z wyjątkiem wizytówek, kalendarzy i notatników prowadzonych w formie papierowej lub elektronicznej;

v) Kierownik jednostki organizacyjnej – oznacza osobę koordynującą pracą Pracowników w poszczególnych jednostkach organizacyjnych utworzonych w Przedsiębiorstwie;

vi) Login – oznacza ciąg znaków literowych, cyfrowych lub innych, identyfikujący Użytkownika do Przetwarzania Danych osobowych w systemie informatycznym;

vii) Nośniki danych – oznaczają wszelkie nośniki, na których są zapisane informacje w postaci elektronicznej, w szczególności: dyski CD–ROM, DVD–ROM, BluRay, dyski, pamięć USB i inne pamięci przenośne, karty magnetyczne oraz dokumenty papierowe zawierające dane osobowe;

viii) Odbiorca - oznacza 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;

ix) Osoba upoważniona – oznacza osobę upoważnioną przez Przedsiębiorstwo do przetwarzania Danych osobowych w danym zakresie;

x) Podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Przedsiębiorstwa;

xi) Polityka – oznacza niniejszą Politykę Ochrony Danych Osobowych Cashbill S.A. z siedzibą w Katowicach z dnia 21 maja 2018 r. wraz ze wszystkimi ewentualnymi Załącznikami;

xii) Pracownicy – oznaczają zarówno osoby zatrudnione w Przedsiębiorstwie na podstawie stosunku pracy, jak również osoby fizyczne współpracujące z Przedsiębiorstwem na podstawie Umowy cywilnoprawnej;

xiii) Przedsiębiorstwo (Administrator Danych Osobowych) – oznacza spółkę CashBill S.A., ul. Jana III Sobieskiego 2, 40-082 Katowice, wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy Katowice-Wschód w Katowicach VIII Wydział Gospodarczy KRS pod numerem 0000323297, NIP: 6292410801;

xiv) 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, o których mowa w art. 4 pkt 2 RODO;

xv) Rejestr - oznacza Rejestr Czynności Przetwarzania Danych Osobowych Przedsiębiorstwa;

xvi) 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) (Dz.Urz. UE L 119, s. 1);

xvii) Sieć lokalna – oznacza połączenie systemów informatycznych Przedsiębiorstwa wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych;

xviii) Sieć rozległa – należy przez to rozumień sieć publiczną (telekomunikacyjną) w rozumieniu ustawy z dnia 16 lipca 2004 r., Prawo telekomunikacyjne (Dz.U. 2004 nr 171 poz. 1800);

xix) System – oznacza System ochrony Danych osobowych w Przedsiębiorstwie, o którym mowa w § 5 Polityki;

xx) System informatyczny – oznacza zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania Danych osobowych;

xxi) Urządzenie mobilne – oznaczają komórkowe telefony przenośne, tablety oraz inne urządzenia przenośne, które za pomocą posiadanych właściwości przeznaczone są lub mogą służyć do Przetwarzania Danych osobowych;

xxii) Uwierzytelnienie – oznacza działanie, którego celem jest weryfikacja deklarowanej tożsamości Użytkownika;

xxiii) Użytkownik – oznacza osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania Danych umieszczonych w systemach, oprogramowaniu, zasobach sieciowych, plikach i folderach zapisanych na komputerach, serwerach, Nośnikach danych i innych urządzeniach elektronicznych;

xxiv) Zbiór danych – oznacza każdy uporządkowany zestaw Danych osobowych, dostępny według określonych kryteriów.

3 Dane osobowe

3.1. Przedsiębiorstwo przetwarza Dane osobowe gromadzone w zbiorach danych. Zbiory danych przetwarzane w Przedsiębiorstwie określa Załącznik nr 1 do Polityki.

3.2. Uaktualnienie lub poszerzenie listy Zbiorów danych następuje po uprzednim przeprowadzeniu analizy skutków oraz ryzyk przetwarzania Danych osobowych dla praw i wolności osób fizycznych objętych zbiorem.

3.3. Przedsiębiorstwo nie podejmuje czynności Przetwarzania, które mogłyby wiązać się z istotnym ryzykiem naruszenia praw i wolności osób, których Dane osobowe dotyczą. W przypadku planowania podjęcia czynności, o których mowa w zdaniu poprzedzającym Przedsiębiorstwo obligatoryjnie przeprowadza uprzednią ocenę skutków przetwarzania, o których mowa w art. 35 RODO.

3.4. Dane osobowe domyślnie Przetwarzane są na obszarze obejmującym pomieszczenia znajdujące się w siedzibie Przedsiębiorstwa przy ul. Jana III Sobieskiego 2, 40-082 Katowice. Dodatkowy obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne i inne Urządzenia mobilne oraz Nośniki danych znajdujące się poza obszarem wskazanym w zdaniu poprzedzającym.

4 Podstawy ochrony Danych osobowych w Przedsiębiorstwie

4.1. Przedsiębiorstwo zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości Przetwarzanych danych.

4.2. Osoby upoważnione oraz wszystkie inne osoby, którym udostępnia się Dane osobowe Przetwarzane w Przedsiębiorstwie zobowiązane są do Przetwarzania Danych osobowych zgodnie z wymogami prawa oraz zgodnie z postanowieniami Polityki, jak również innych wewnętrznych aktów prawnych Przedsiębiorstwa lub procedur wewnętrznych związanych z Przetwarzaniem Danych Osobowych.

4.3. Przy zatrudnianiu Pracowników oraz w toku zatrudnienia Przedsiębiorstwo zapewnia, że:

i) Pracownicy przed przystąpieniem do wykonywania obowiązków służbowych otrzymują należytą wiedzę w zakresie zasad Przetwarzania i ochrony Danych osobowych w Przedsiębiorstwie;

ii) każdy z Pracowników zostaje upoważniony na piśmie do Przetwarzania Danych Osobowych w niezbędnym zakresie, zgodnie z wzorem stanowiącym Załączniki nr 2 do Polityki;

iii) każdy z Pracowników zostaje zobowiązany do zachowania poufności i integralności Danych osobowych, zgodnie z wzorem stanowiącym Załącznik nr 3 do Polityki, przy czym Pracownicy zobowiązani są w szczególności, ale nie wyłącznie do:

(a) ścisłego przestrzegania zakresu upoważnienia;

(b) przestrzegania wymogów prawa oraz postanowień Polityki w zakresie przetwarzania;

(c) zachowania w tajemnicy Danych osobowych;

(d) zachowania poufności i integralności w zakresie Danych osobowych;

(e) niezwłocznego zgłaszania Przedsiębiorstwu wszelkich incydentów związanych z naruszeniem bezpieczeństwa Danych osobowych.

4.4. Przedsiębiorstwo zapewnia, aby Dane osobowe Przetwarzane w Przedsiębiorstwie były:

i) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;

ii) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;

iii) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;

iv) prawidłowe i w razie potrzeby uaktualniane; Przedsiębiorstwo zapewnia podejmowanie działań, mających na celu usuwanie lub sprostowanie Danych osobowych, które są nieprawidłowe w świetle celów ich przetwarzania ("prawidłowość");

v) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;

vi) przetwarzane 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 odpowiednich środków technicznych lub organizacyjnych.

4.5. Przy zapewnieniu Przetwarzania Danych osobowych zgodnie z zasadami wskazanymi w ust. powyżej Przedsiębiorstwo opiera Przetwarzanie na następujących podstawach:

i) Legalność – Przedsiębiorstwo dba o ochronę prywatności i przetwarza Dane osobowe zgodnie z wymogami prawa;

ii) Bezpieczeństwo – Przedsiębiorstwo zapewnia odpowiedni poziom bezpieczeństwa Danych osobowych podejmując stale działania w tym zakresie;

iii) Prawa Jednostki – Przedsiębiorstwo umożliwia osobom, których Dane osobowe są przetwarzane, wykonywanie swoich praw i prawa te realizuje;

iv) Rozliczalność – Przedsiębiorstwo zapewnia należyte udokumentowanie sposobu spełniania obowiązków w zakresie ochrony Danych osobowych.

5 System ochrony Danych osobowych

5.1. Przedsiębiorstwo zapewnia zgodność Przetwarzania Danych osobowych z wymogami prawa również poprzez zaprojektowanie, wprowadzenie i utrzymywanie Systemu. Na System składają się środki organizacyjne oraz środki techniczne ochrony, adekwatne do poziomu ryzyka zidentyfikowanego dla poszczególnych Zbiorów danych oraz kategorii danych. Na System składają się w szczególności następujące środki:

i) ograniczenie dostępu do pomieszczeń, w których przetwarzane są Dane osobowe, jedynie do Osób upoważnionych oraz zapewnienie, że inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do Przetwarzania Danych osobowych wyłącznie w towarzystwie Osoby upoważnionej;

ii) zamykanie pomieszczeń tworzących obszar, o którym mowa w ust. 3.4 Polityki na czas nieobecności Pracowników, w sposób uniemożliwiający dostęp do nich osobom trzecim;

iii) zapewnienie zabezpieczenia obszaru, o którym mowa w ust. 3.4 Polityki przed czynnikami losowymi, takimi jak pożar lub powódź;

iv) wykorzystywanie zamykanych szafek, szuflad, sejfów lub innych środków technicznych uniemożliwiających osobom niepowołanym dostęp do przechowywanych w nich Danych osobowych;

v) wdrożenie Polityki czystego biurka, która stanowi Załącznik nr 4 do Polityki;

vi) ograniczenie dostępu osób postronnych do pomieszczeń poprzez wdrożenie elektronicznego systemu kontroli dostępu do pomieszczeń;

vii) wdrożenie zasad zarządzania systemem informatycznym służącym do przetwarzania Danych osobowych;

viii) wdrożenie zasad monitorowania systemu zainstalowanego na komputerach i urządzeniach przenośnych;

ix) wdrożenie zasad dotyczących tworzenia kopii zapasowych;

x) wdrożenie zasad przechowywania i archiwizowania gromadzonej dokumentacji zawierającymi Dane osobowe;

xi) wdrożenie zasad archiwizowania i przechowywania dokumentacji zawierającej Dane osobowe;

xii) wdrożenie zasad przekazywania Danych osobowych w obrębie Przedsiębiorstwa'

xiii) zapewnienie skutecznego usuwania lub niszczenia dokumentów zawierających Dane osobowe, w sposób uniemożliwiający ich późniejsze odtworzenie;

xiv) zapewnienie bezpieczeństwa sprzętowego i informatycznego, obejmującego:

(a) ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz,

(b) zapewnienie aktualności stosowanego oprogramowania,

(c) zabezpieczenie sprzętu komputerowego wykorzystywanego w Przedsiębiorstwie przed złośliwym oprogramowaniem,

(d) zapewnienie stałego i częstotliwego sporządzania kopii zapasowych danych przechowywanych na komputerach, serwerze oraz w sieci Przedsiębiorstwa,

(e) ograniczenie dostępu do sprzętu komputerowego, serwera oraz sieci lokalnej poprzez stosowanie reguł Uwierzytelniania;

xv) przeprowadzanie analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;

xvi) realizację standardów weryfikacji i doboru Podmiotów przetwarzających, jak również warunków powierzenia Przetwarzania danych na rzecz poszczególnych Podmiotów przetwarzających;

xvii) monitorowanie zmian w zakresie procesów Przetwarzania Danych osobowych w Przedsiębiorstwie oraz na bieżąco zarządzanie zmianami mającymi wpływ na ochronę Danych osobowych w Przedsiębiorstwie.

6 Rejestr

6.1. Rejestr obejmuje kategorie czynności przetwarzania Danych osobowych w Przedsiębiorstwie. Za pośrednictwem Rejestru Przedsiębiorstwo dokumentuje czynności przetwarzania Danych Osobowych oraz inwentaryzuje i monitoruje sposób, w jaki wykorzystuje Dane osobowe. Rejestr stanowi Załącznik nr 6 do Polityki.

6.2. Za pośrednictwem Rejestru, w szczególności poprzez wskazanie w Rejestrze ogólnych środków ochrony Danych osobowych objętych wyodrębnioną czynnością przetwarzania, Przedsiębiorstwo dąży również do wykazania zgodności Przetwarzania Danych osobowych z wymogami prawa.

6.3. W Rejestrze, odrębnie dla każdej zidentyfikowanej kategorii czynności przetwarzania Danych osobowych, odnotowuje się co najmniej:

i) nazwę czynności;

ii) cel przetwarzania;

iii) opis kategorii osób, których Dane osobowe przetwarzane są w ramach danej czynności;

iv) opis kategorii Danych osobowych przetwarzanych w ramach danej czynności;

v) podstawę prawną przetwarzania wraz z wyszczególnieniem kategorii uzasadnionego interesu Przedsiębiorstwa, jeśli podstawą przetwarzania jest uzasadniony interes;

vi) opis kategorii Odbiorców danych, w tym Podmiotów przetwarzających,

vii) informację o ewentualnym przekazaniu Danych osobowych poza terytorium Unii Europejskiej lub Europejskiego Obszaru Gospodarczego;

viii) ogólny opis technicznych i organizacyjnych środków ochrony Danych osobowych, znajdujących zastosowanie do danej czynności.

6.4. W przypadku uaktualnienia lub poszerzenia kategorii czynności przetwarzania Danych Osobowych, Przedsiębiorstwo dokonuje niezwłocznego uaktualnienia Rejestru celem zapewnienia zgodności Rejestru ze stanem faktycznym oraz zakresem operacji przetwarzania Danych osobowych w Przedsiębiorstwie.

6.5. Postanowienia ust. powyżej nie wyłączają możliwości ujęcia w Rejestrze w miarę potrzeby informacji dodatkowych, zwiększających szczegółowość lub czytelność Rejestru lub ułatwiających zarządzanie zgodnością ochrony Danych osobowych z wymogami prawa oraz realizację zasady rozliczalności.

6.6. Przedsiębiorstwo dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania poprzez wskazanie ogólnej podstawy prawnej przetwarzania, takiej jak: zgoda, umowa, obowiązek prawny nałożony na Przedsiębiorstwo, uzasadniony cel Przedsiębiorstwa.

7 Realizacja obowiązków wobec osób, których dane osobowe dotyczą

7.1. Przedsiębiorstwo 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, i inne) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności, takich jak zgłoszenie sprzeciwu lub ograniczenie przetwarzania.

7.2. Przedsiębiorstwo dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których Dane osobowe przetwarza.

7.3. Przedsiębiorstw publikuje na stronie internetowej Przedsiębiorstwa oraz pozostawia do wglądu w siedzibie Przedsiębiorstwa:

i) Politykę;

ii) Informację o prawach osób, których dane dotyczą;

iii) Informację o zakresie przetwarzanych danych osobowych w poszczególnych celach;

iv) Metodach kontaktu z Przedsiębiorstwem w zakresie Danych osobowych;

7.4. W celu realizacji praw osoby, której Dane osobowe dotyczą Przedsiębiorstwo zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Przedsiębiorstwo, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.

7.5. Przedsiębiorstwo dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób, informując osobę, której dane dotyczą o:

i) przetwarzaniu jej Danych osobowych, przy pozyskiwaniu danych od tej osoby.

ii) przetwarzaniu jej Danych osobowych, przy pozyskiwaniu danych o tej osobie nie bezpośrednio od niej;

iii) planowanej zmianie celu przetwarzania danych;

iv) uchyleniu ograniczenia przetwarzania Danych osobowych przed uchyleniem ograniczenia przetwarzania;

v) sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych, chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe;

vi) uprawnieniu do złożenia sprzeciwu względem przetwarzania Danych osobowych najpóźniej przy pierwszym kontakcie z tą osobą.

7.6. Przedsiębiorca bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony Danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

7.7. Niezależnie od postanowień ust. powyżej, Przedsiębiorstwo określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe.

7.8. Na żądanie osoby dotyczące dostępu do jej danych, Przedsiębiorstwo informuje osobę, czy przetwarza jej Dane osobowe oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych.

7.9. Przedsiębiorca wydaje osobie, której Dane osobowe dotyczą kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.

7.10. Przedsiębiorstwo dokonuje sprostowania nieprawidłowych danych na żądanie osoby, której Dane osobowe dotyczą. Przedsiębiorstwo ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Przedsiębiorstwo informuje osobę o odbiorcach danych, na żądanie tej osoby.

7.11. Przedsiębiorstwo uzupełnia i aktualizuje dane na żądanie osoby, której Dane osobowe dotyczą. Przedsiębiorstwo ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Przedsiębiorstwo może polegać na

oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Przedsiębiorstwo procedur lub prawa albo zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

7.12. Z uwzględnieniem ust. poniżej, na żądanie osoby, Przedsiębiorstwo usuwa dane, gdy:

i) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,

ii) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,

iii) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,

iv) dane były przetwarzane niezgodnie z prawem,

v) konieczność usunięcia wynika z obowiązku prawnego,

vi) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

7.13. Przedsiębiorstwo przy usuwaniu Danych osobowych uwzględnia, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.

7.14. Jeżeli dane podlegające usunięciu zostały upublicznione przez Przedsiębiorstwo, wówczas Przedsiębiorstwo podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich. W przypadku usunięcia danych Przedsiębiorstwo informuje osobę o odbiorcach danych, na żądanie tej osoby.

7.15. Przedsiębiorstwo dokonuje ograniczenia Przetwarzania danych na żądanie osoby, gdy:

i) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,

ii) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu Danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,

iii) Przedsiębiorstwo nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,

iv) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Przedsiębiorstwa zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

7.16. W trakcie ograniczenia przetwarzania Przedsiębiorstwo przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, 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. Przedsiębiorstwo informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Przedsiębiorstwo informuje osobę o odbiorcach danych, na żądanie tej osoby.

7.17. Na żądanie osoby Przedsiębiorstwo wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Przedsiębiorstwu, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Przedsiębiorstwu.

7.18. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, o którym mowa w art. 21 RODO, a dane przetwarzane są przez Przedsiębiorstwo w oparciu o uzasadniony interes Przedsiębiorstwu lub o powierzone Przedsiębiorstwu zadanie w interesie publicznym, Przedsiębiorstwo zobowiązuje się uwzględnić sprzeciw, o ile nie zachodzą po stronie Przedsiębiorstwa ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

7.19. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Przedsiębiorstwo na potrzeby marketingu bezpośredniego, Przedsiębiorstwo uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

8 Minimalizacja danych

8.1. Przedsiębiorstwo wdraża procedury służące realizacji zasady minimalizacji przetwarzanych Danych osobowej pod względem:

i) adekwatności Danych osobowych do celów Przetwarzania, obejmujących ograniczenie ilości przetwarzanych Danych osobowych oraz zakresu przetwarzania do celu Przetwarzania;

ii) ograniczenia dostępu do Danych osobowych wyłącznie do Osób upoważnionych, dla których wykorzystanie Danych osobowych w określonym zakresie jest niezbędne dla prawidłowej realizacji obowiązków;

iii) ograniczenia czasu przechowywania Danych osobowych do okresu, dla którego przechowywanie Danych osobowych jest niezbędne ze względu na realizację celu Przetwarzania lub obowiązków nałożonych na Przedsiębiorstwo.

8.2. Przedsiębiorstwo dokonuje okresowego przeglądu ilości przetwarzanych danych, ich rodzaju i zakresu ich przetwarzania nie rzadziej niż raz na rok.

8.3. Przedsiębiorstwo stosuje ograniczenia dostępu do Danych osobowych poprzez:

i) zobowiązanie Pracowników do zachowania poufności, w tym w zakresie Danych osobowych;

ii) weryfikację kręgu wewnętrznych odbiorców Danych osobowych poprzez nadawanie poszczególnym Pracownikom szczegółowych upoważnień co do Przetwarzania Danych osobowych jedynie w zakresie, w jakim jest to niezbędne do wykonania obowiązków służbowych związanych z celami ujawnionymi osobie, której Dane dotyczą;

iii) wdrożenie środków technicznych ochrony Danych osobowych poprzez ograniczenie dostępu do systemów, oprogramowania oraz zasobów sieciowych, w tym serwerów,

skrzynek pocztowych i Danych osobowych przetwarzanych na komputerach, telefonach oraz innych Nośnikach danych, wykorzystywanych w procesie Przetwarzania Danych Osobowych;

iv) wdrożenie fizycznych środków technicznych ochrony Danych osobowych, wskazanych w ust. 5.1(iv) Polityki.

8.4. Przedsiębiorstwo dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających. Przedsiębiorstwo dokonuje okresowego przeglądu ustanowionych Użytkowników systemów, skrzynek pocztowych i oprogramowania oraz aktualizuje ich nie rzadziej niż raz na rok.

8.5. Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Przedsiębiorstwa.

8.6. Przedsiębiorstwo przetwarza Dane osobowe z uwzględnieniem kryteriów wskazanych w Rejestrze. Przedsiębiorstwo wdraża mechanizmy kontroli cyklu życia Danych osobowych w Przedsiębiorstwie, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.

8.7. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów, oprogramowania, komputerów i innych Nośników danych Przedsiębiorstwa, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Przedsiębiorstwo. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

9 Bezpieczeństwo Danych osobowych

9.1. Przedsiębiorstwo zobowiązuje wszystkie osoby, które w obrębie wykonywania obowiązków służbowych, uzyskają w jakimkolwiek zakresie dostęp do Danych osobowych przetwarzanych przez Przedsiębiorstwo do zapoznania się przed przystąpieniem do pracy z obowiązującymi zasadami ochrony Danych osobowych określonymi w Polityce.

9.2. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia Przedsiębiorstwo wdraża środki techniczne i organizacyjne zapewniające należyty stopień ochrony Danych osobowych, odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Przedsiębiorstwo.

9.3. Przedsiębiorstwo przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa Danych osobowych. W tym celu Przedsiębiorstwo:

i) kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają;

ii) przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Przedsiębiorstwo 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;

9.4. Przedsiębiorstwo wdraża 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.

9.5. Ustanowiony w Przedsiębiorstwie Administrator Systemów Informatycznych podejmuje działania w celu zapewnienia zgodnego z prawem przetwarzania Danych osobowych w systemach informatycznych użytkowanych przez Przedsiębiorstwo oraz zachowania najwyższego stopnia bezpieczeństwa Danych osobowych w systemach informatycznych. Do obowiązków Administratora Systemów Informatycznych należy:

i) stała kontrola i monitorowanie uprawnień Użytkowników;

ii) zapewnienie prawidłowej eksploatacji systemu informatycznego, zgodnej z ustalonymi celami przetwarzania Danych osobowych i zasadami zgodnego z prawem przetwarzania;

iii) sprawowanie nadzoru w zakresie wykonywania kopii zapasowych oraz kontrolowanie systemu kopii w obrębie ich dalszej przydatności do odtwarzania Danych osobowych w przypadku wystąpienia awarii systemów, oprogramowania i zasobów sieciowych;

iv) informowania Członków Zarządu Przedsiębiorstwa o wszystkich wykrytych nieprawidłowościach i incydentach naruszających lub zagrażających bezpieczeństwu Danych osobowych i systemu informatycznego;

v) podejmowanie działań mających na celu zapobieganie występowaniu awarii systemu, nieprawidłowości i incydentów naruszających lub zagrażających bezpieczeństwu Danych osobowych i systemu informatycznego;

vi) wykonywanie przeglądów, konserwacji oraz modyfikacji w zakresie wdrażania aktualizacji do systemu informatycznego i oprogramowania służących do przetwarzania Danych osobowych;

vii) sprawowanie stałej kontroli nad poziomem bezpieczeństwa systemu informatycznego w zakresie przetwarzania Danych osobowych,

viii) uwierzytelnianie Użytkowników, w szczególności poprzez nadawanie, zmianę zakresu, pozbawianie ich uprawnień w dostępie do systemu informatycznego, zasobów sieciowych, serwerów, obsługiwanych programów, zgodnie z zasadami zarządzania, o których mowa w § 10 Polityki;

ix) wykonywanie innych czynności i zadań związanych z Przetwarzaniem Danych osobowych za pomocą serwerów, zasobów sieciowych, systemu informatycznego i oprogramowania oraz zapewnieniem bezpieczeństwa Danych osobowych związanych z Przetwarzaniem.

9.6. Użytkownicy zobowiązani są do przestrzegania zasad ochrony Danych osobowych określonych w niniejszej Polityce oraz do prawidłowego wykonywania obowiązków w zakresie:

i) przetwarzania Danych osobowych zgodnie z ustalonymi i ujawnionymi osobie, której Dane osobowe dotyczą celami;

ii) uczestnictwa w szkoleniach z zakresu ochrony Danych osobowych organizowanych przez Przedsiębiorstwo;

iii) stosowania się do zaleceń, poleceń służbowych oraz komunikatów wydawanych przez przełożonych w zakresie sprawnego funkcjonowania Systemu;

iv) przestrzeganie zasad dotyczących zabezpieczenia Danych osobowych przewidzianych niniejszą Polityką wraz z Załącznikami, jak i niewymienionych w Polityce, ale wdrożonych w Przedsiębiorstwie;

v) dbałości o bezpieczną eksploatację systemu informatycznego i sieciowego użytkowanego przez Użytkownika, w tym: przestrzeganie zasad związanych ze zmianą hasła na komputerach i urządzeniach mobilnych, wyłączanie komputera każdorazowo po zakończeniu pracy i opuszczeniu stanowiska pracy, brak przesyłania Danych osobowych zgromadzonych na komputerach, na serwerach, skrzynkach mailowych i innych zasobach sieciowych do osób nieupoważnionych, wykazywanie ostrożności przy odbiorze poczty elektronicznej pochodzącej o nieznanych adresatów, których identyfikacja budzi wątpliwości;

vi) powstrzymania się od wynoszenia dokumentów z Danymi osobowymi poza siedzibę Spółki w jakiejkolwiek formie, z wyjątkiem osób do tego upoważnionych;

vii) przestrzegania zasad związanych z ochroną Danych osobowych przetwarzanych w związku z wykonywaniem obowiązków służbowych zawartych w wizytówkach i notatnikach oraz kalendarzach prowadzonych w formie pisemnej lub elektronicznej;

viii) braku samodzielnego dorabiania kluczy zapasowych umożliwiających dostęp do pomieszczeń na terenie Przedsiębiorstwa,

ix) braku dokonywania jakichkolwiek przeróbek w treści istniejących pieczęci zawierających Dane osobowe, a w szczególności dodawania lub usuwania znaków, wyrabiania we własnym zakresie dodatkowych lub nowych pieczęci, dokonywania okresowej lub stałej zmiany istniejących pieczęci między sobą;

x) ustawienia monitora komputerowego w sposób uniemożliwiający podgląd wyświetlanych Danych osobowych przez osoby nieupoważnione przebywające w pomieszczeniu biurowym.

10 Zasady zarządzania systemem informatycznym służącym do Przetwarzania danych

10.1. Administrator Systemu Informatycznego nadaje, rejestruje i odbiera uprawnienia do systemów informatycznych, oprogramowania, zasobów sieciowych i serwerów. W tym celu Administrator Systemu Informatycznego:

i) ustala jaki zakres uprawnień w dostępie do systemów, oprogramowania, zasobów sieciowych i serwerów powinien mieć konkretny Użytkownik według Załącznika nr 9;

ii) stale monitoruje zmiany w obrębie konieczności ograniczenia lub poszerzenia zakresu uprawnień konkretnych Użytkowników do systemów, oprogramowania, zasobów sieciowych i serwerów;

iii) odbiera uprawnienia w dostępie do systemów, oprogramowania, zasobów sieciowych i serwerów konkretnym Użytkownikom na wniosek Członków Zarządu lub kierowników poszczególnych jednostek organizacyjnych funkcjonujących w Przedsiębiorstwie.

10.2. Login Użytkownika:

i) do systemu i urządzeń mobilnych:

(a) skonstruowany musi być w sposób umożliwiający jego identyfikację i jednocześnie odróżniać się wystarczająco od Loginów pozostałych Użytkowników;

(b) nadawany jest dla każdego Użytkownika osobno, chyba że istnieje potrzeba utworzenia jednego loginu dla kliku Użytkowników systemu w obrębie jednej jednostki organizacyjnej;

(c) przydzielony jednemu Użytkownikowi nie może być ponownie nadany innemu Użytkownikowi;

(d) wymaga każdorazowego wpisania po wylogowaniu się automatycznym lub ręcznym, zakończeniu pracy komputera, czasowego uśpienia komputera po upływie dłuższym niż 15 minut bezczynności;

(e) nie może być zapamiętany na komputerze i innym urządzeniu mobilnym w sposób automatyczny.

ii) do serwera:

(a) skonstruowany musi być w sposób umożliwiający jego identyfikację i jednocześnie odróżniać się wystarczająco od Loginów pozostałych Użytkowników;

(b) nadawany jest dla każdego Użytkownika osobno;

(c) przydzielony jednemu Użytkownikowi nie może być ponownie nadany innemu Użytkownikowi;

(d) wymaga każdorazowego wpisania po wylogowaniu się automatycznym lub ręcznym, zakończeniu pracy komputera;

(e) nie może być zapamiętany na komputerze i innym urządzeniu mobilnym w sposób automatyczny;

(f) nadawany jest zgodnie z modułowym dostępem do Danych osobowych według Załącznika nr 9.

iii) do programów:

(a) skonstruowany musi być w sposób umożliwiający jego identyfikację i jednocześnie odróżniać się wystarczająco od Loginów pozostałych Użytkowników z uwzględnieniem zasad określonych specyfiką i właściwościami danego programu;

(b) nadawany jest dla każdego Użytkownika osobno;

(c) przydzielony jednemu Użytkownikowi nie może być ponownie nadany innemu Użytkownikowi;

(d) powinien być wpisywany każdorazowo po wylogowaniu się automatycznym lub ręcznym, zakończeniu pracy programu, z uwzględnieniem zasad określonych specyfiką i właściwościami danego programu;

(e) nie może być zapamiętany na komputerze i innym urządzeniu mobilnym w sposób automatyczny;

(f) nadawany jest zgodnie z modułowym dostępem do Danych osobowych według Załącznika nr 9 do Polityki.

10.3. Hasło:

i) do systemu, urządzeń mobilnych i serwera:

(a) powinno składać się z co najmniej 8 znaków oraz zawierać co najmniej jedną dużą literę i jedną cyfrę lub znak specjalny;

(b) nie powinno być wyrażeniem lub słowem powszechnie znanym lub możliwym do zidentyfikowania w łatwy sposób, tj. imię i nazwisko Użytkownika, data urodzenia Użytkownika, powszechnie znany pseudonim Użytkownika;

(c) powinno być zmieniane nie rzadziej niż po upływie 30 dni od dnia jego ustanowienia przez wszystkich Użytkowników;

(d) nie może być zapisane w miejscu łatwo dostępnym dla innych osób;

(e) nie może być zapamiętane na komputerze w sposób automatyczny;

(f) wymaga każdorazowego wpisania po wylogowaniu się automatycznym lub ręcznym, zakończeniu pracy komputera, czasowego uśpienia komputera po upływie dłuższym niż 15 minut bezczynności, chyba że możliwości techniczne nie pozwalają na ustanowienie wylogowania się po upływie okresu bezczynności;

(g) byłych Pracowników jest usuwane wraz z usuniętym loginem lub zmieniane w sposób uniemożliwiający byłemu Pracownikowi uzyskanie dostępu do systemu, urządzeń mobilnych i serwera.

ii) do skrzynki mailowej programów:

(a) powinno składać się z co najmniej 8 znaków oraz zawierać co najmniej jedną dużą literę i jedną cyfrę lub znak specjalny z uwzględnieniem zasad określonych specyfiką i właściwościami danego programu, chyba że program pocztowy wymaga ustawienia hasła o innej konstrukcji;

(b) nie powinno być wyrażeniem lub słowem powszechnie znanym lub możliwym do zidentyfikowania w łatwy sposób, tj. imię i nazwisko Użytkownika, data urodzenia Użytkownika, powszechnie znany pseudonim Użytkownika;

(c) powinno być zmieniane nie rzadziej niż po upływie 30 dni od dnia jego ustanowienia przez wszystkich Użytkowników, z uwzględnieniem zasad określonych specyfiką i właściwościami danego programu;

(d) nie może być zapisane w miejscu łatwo dostępnym dla innych osób;

(e) nie może być zapamiętane na komputerze w sposób automatyczny;

(f) wymaga każdorazowego wpisania po wylogowaniu się automatycznym lub ręcznym;

(g) byłych Pracowników jest usuwane wraz z usuniętą skrzynką mailową lub zmieniane w sposób uniemożliwiający byłemu Pracownikowi uzyskanie dostępu do skrzynki mailowej i programów.

10.4. Dostęp do oprogramowania zainstalowanego na komputerach możliwy jest jedynie z komputerów powierzonych Pracownikom w siedzibie Przedsiębiorstwa. W przypadku

korzystania ze skrzynki mailowej na urządzeniu prywatnym, Użytkownik zobowiązany jest do zastosowania zasad ochrony przewidzianych w Polityce do zabezpieczenia urządzenia prywatnego oraz ochrony bezpieczeństwa Danych osobowych.

10.5. Nośniki danych przechowywane i transportowane muszą być w sposób uniemożliwiający naruszenie Danych osobowych:

i) nośniki danych w siedzibie Przedsiębiorstwa, przechowywane są w pomieszczeniu, w którym znajduje się stanowisko pracy Pracownika, w zamykanych na klucz szafkach lub szufladach albo w sejfach, chyba że Przedsiębiorstwo zapewnia zabezpieczenie Nośników danych w inny sposób przy użyciu wszelkich dostępnych środków technicznych;

ii) nośniki danych wynoszone poza siedzibę Przedsiębiorstwa są zabezpieczone w sposób uniemożliwiający dostęp do nich osób nieupoważnionych poprzez ustanowienie hasła dostępu do Danych osobowych lub przechowywanie Nośników danych w miejscach, do których nie mają dostępu osoby nieupoważnione.

10.6. Pracownicy korzystający przy wypełnianiu obowiązków służbowych z Urządzeń mobilnych zobowiązani są do ochrony przed ich uszkodzeniem, zniszczeniem, kradzieżą i uzyskaniem dostępu przez osoby nieupoważnione, w tym domowników. Urządzenia mobilne, za pomocą których Przetwarzane są Dane osobowe zabezpieczone są poprzez ustanowienie hasła do systemu zgodnie z pkt 10.3 (i), zainstalowanie oprogramowania lub systemu szyfrującego Dane osobowe, jak również zastosowanie innych funkcji i zabezpieczeń programowych lub systemowych zainstalowanych na Urządzeniu przenośnym, m.in. odblokowanie systemu za pomocą weryfikacji linii papilarnych, face ID.

11 Zasady monitorowania systemu zainstalowanego na komputerach i Urządzeniach mobilnych.

11.1. Administratorem programów wskazanych w 10.4 Polityki jest Administrator Systemu Informatycznego.

11.2. Komputery, przy pomocy których Pracownicy wykonują czynności pracownicze podłączone są wyłącznie do wewnętrznej sieci komputerowej oddzielonej fizycznie od sieci publicznej przy pomocy bramy internetowej zabezpieczonej oprogramowaniem firewall.

11.3. Zasoby informatyczne Przedsiębiorstwa zabezpieczone są poprzez zainstalowane na wszystkich komputerach użytkowanych przez Członków Zarządu i Pracowników oprogramowanie antywirusowe, wspomagające ochronę przed wirusami, oprogramowaniem szpiegowskim, trojanami i rokitnikami. Serwer plików zabezpieczony jest programem antywirusowym.

11.4. Baza sygnatur wirusów aktualizowana jest codziennie pod warunkiem podłączenia komputerów i Urządzeń mobilnych do sieci Internet. Skany komputerów i Urządzeń mobilnych w celu wykrycia wirusów i oprogramowania złośliwego wykonywane są nie rzadziej niż raz w miesiącu.

11.5. Dostęp logiczny do sieci lokalnej zabezpieczony jest adresem IP oraz MAC - adresem karty sieciowej. Dostęp do sieci rozległej zabezpieczony jest Firewallem wraz z oprogramowaniem antywirusowym zainstalowanym na stacji roboczej.

11.6. Kopie awaryjne istotnych danych wykonywane są w cyklu dziennym na serwerze sieciowym podmiotu świadczącego usługi hostingowe na rzecz Przedsiębiorstwa.

11.7. W przypadku wykrycia przez zainstalowane na komputerach i Urządzeniach mobilnych oprogramowanie antywirusowe próby ingerencji oprogramowania złośliwego na urządzeniu, którego program antywirusowy nie jest w stanie usunąć, zniszczyć lub zneutralizować, Użytkownik zobowiązany jest do zakończenia pracy w systemie, wylogowania się z systemu jeśli jest to możliwe i niezwłocznego zgłoszenia zdarzenia Administratorowi Systemu Informatycznego.

11.8. Zakazane jest samowolne podłączanie do lokalnej sieci Przedsiębiorstwa jakichkolwiek urządzeń aktywnych typu: Router, Switch, Access Point.

11.9. Połączenie zdalne z zasobami Przedsiębiorstwa możliwe jest jedynie za pomocą VPN. Administrator Systemu Informatycznego udostępnia Loginy i Hasłaprzy użyciu

dedykowanego imiennego certyfikatu, za pomocą któregoych możliwe jest nawiązanie połączenia zdalnego z systemem Przedsiębiorstwa oraz sprawuje stałą kontrolę nad połączeniami zdalnymi do systemu i programów.

12 Zasady dotyczące tworzenia kopii zapasowych

12.1. W celu zabezpieczenia Danych osobowych przetwarzanych przez Przedsiębiorstwo przed ich utratą, wykonywane są kopie zapasowe oprogramowania. Dla bazy danych wykonywane są kopie zapasowe nie rzadziej niż raz w tygodniu i jest wykonywana metodą pełną.

12.2. Kopie zapasowe wykonywane i przechowywane są przez podmiot świadczący usługi hostingowe na rzecz Przedsiębiorstwa.

12.3. Dostęp do kopii zapasowych posiada tylko Administrator Systemu Informacji.

13 Zasady archiwizowania i przechowywania gromadzonej dokumentacji zawierającej Dane osobowe

13.1. W siedzibie Przedsiębiorstwa znajdują się pomieszczenia zaadoptowane na potrzeby archiwizowania dokumentów. Przedsiębiorstwo podejmuje działania zmierzające do ograniczenia osób postronnych do wskazanych pomieszczeń oraz stosuje elektroniczną kontrolę dostępu, uniemożliwiającą osobom postronnym dostęp do dokumentacji.

13.2. Pomieszczenia zaadoptowane na potrzeby archiwizowania dokumentacji są zabezpieczone przez nieuprawnionym dostępem osób nieupoważnionych poprzez m.in.:

i) zainstalowanie w drzwiach zamka elektronicznego aktywowanego za pośrednictwem kart dostępu oraz powierzaniu klucza tylko Pracownikom posiadającym upoważnienie do dostępu do właściwych pomieszczeń. Karty do pomieszczeń przechowywane są w miejscach niedostępnych dla osób nieupoważnionych;

ii) przechowywanie dokumentacji w szafach zamykanych na klucz oraz powierzenie klucza tylko Pracownikom upoważnienie do dostępu do dokumentacji. Klucze do szaf przechowywane są w miejscach niedostępnych dla osób nieupoważnionych;

iii) zakaz udostępniania kluczy osobom nie będącym Pracownikami Przedsiębiorstwa.

13.3. Archiwizacji podlegają dokumenty, które nie są używane w toku bieżącego funkcjonowania Przedsiębiorstwa. O przeniesieniu dokumentacji do pomieszczenia zaadoptowanego na potrzeby archiwum decyduje kierownicy poszczególnych jednostek organizacyjnych lub wyznaczenie przez Kierowników Pracownicy.

13.4. Dokumenty zawierające Dane osobowe w formie papierowej przechowywane są w teczkach, segregatorach lub koszulkach, lub w inny sposób przyjęty przez Kierownika jednostki organizacyjnej i segregowane w sposób przyjęty przez Kierownika jednostki organizacyjnej. W jednej teczce nie mogą znajdować się dokumenty zawierające Dane osobowe, do Przetwarzania których Pracownicy określonej jednostki organizacyjnej są

upoważnieni oraz dokumenty zawierające Dane osobowe, do których Przetwarzania Pracownicy określonej jednostki organizacyjnej nie są upoważnieni. W przypadku możliwości segregacji dokumentów, o której mowa w zdaniu poprzednim, Kierownik jednostki organizacyjnej w uzgodnieniu z Członkiem Zarządu podejmuje inne środki techniczno-organizacyjne zapobiegające umożliwienia dostępu do Danych Pracownikom nieupoważnionym.

13.5. Dostęp do pomieszczeń w Przedsiębiorstwie ograniczany jest w drodze wydawania indywidualnych kart dostępowych lub/i kart dostępu, haseł dostępowych, uprawniających pracowników do dostępu do pomieszczeń właściwych ze względu na zakres przyznanych uprawnień.

13.6. Dokumenty zawierające Dane osobowe w pomieszczeniach, w których znajdują się stanowiska pracy Pracowników, przechowywane są po zakończeniu pracy przez Pracowników w szafach i szufladach zamykanych na klucz. Nośniki danych zawierające Dane osobowe przechowywane są w sposób określony w 10.5 Polityki.

13.7. W przypadku obecności w pomieszczeniu, w którym znajdują się stanowiska pracy Pracowników, osoby nieupoważnionej do przetwarzania Danych osobowych określonej kategorii zgodnie z Załącznikiem nr 9 do Polityki, Pracownicy podejmują wszelkie niezbędne czynności uniemożliwiające dostęp osób nieupoważnionych do Danych osobowych.

13.8. Zasady przewidziane w niniejszym paragrafie stosuje się także w przypadku przechowywania Danych osobowych poza siedzibą Przedsiębiorstwa, o której mowa w ust. 3.4 Polityki.

14 Usuwanie Danych osobowych

14.1. Przedsiębiorstwo przechowuje Dane osobowe przez okres nie dłuższy, niż jest to niezbędne do celów Przetwarzania. Po upływie okresu wskazanego w Rejestrze, Przedsiębiorstwo usuwa Dane osobowe w sposób trwały.

14.2. Przedsiębiorstwo usuwa Dane osobowe za pomocą własnych środków i mechanizmów lub powierza usuwanie Danych osobowych podmiotom współpracującym, którzy zapewniają

wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych zapobiegających zagrożeniom naruszenia lub naruszeniom bezpieczeństwa Danych osobowych.

14.3. Dane osobowe zawarte w dokumentach, które ze względu na potrzeby zachowania ciągłości współpracy z kontrahentami, klientami i innymi podmiotami, bieżącego prawidłowego funkcjonowania Przedsiębiorstwa lub z innych ważnych powodów nie mogą być usunięte po upływnie czasu określonego w Rejestrze, podlegają anonimizacji.

14.4. Niezależnie od postanowień ust. 14.1-powyżej, Przedsiębiorstwo usuwa Dane osobowe w przypadkach, o których mowa w ust. 7.13 Polityki.

14.5. Podmiotem upoważnionym do usuwania Danych osobowych z serwerów jest Administrator Systemu Informatycznego.

14.6. Przed przekazaniem do podmiotu zewnętrznego komputerów, Urządzeń mobilnych, Nośników danych zawierających Dane osobowe, przeznaczonych do zniszczenia lub naprawy, Administrator Systemu Informatycznego usuwa umieszczone na urządzeniu Dane osobowe. W przypadku braku możliwości usunięcia Danych osobowych, Administrator Systemu Informatycznego podejmuje niezbędne czynności zapobiegające dostępowi do Danych osób nieupoważnionych, np. szyfruje lub anonimizuje Dane.

15 Naruszenie ochrony danych osobowych

15.1. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych osobowych uważa się w szczególności, ale nie wyłącznie:

i) naruszenie bezpieczeństwa systemów informatycznych, oprogramowania i zasobów sieciowych, w których przetwarzane są Dane osobowe;

ii) udostępnienie Danych osobowych osobom nieupoważnionym;

iii) przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem ich Przetwarzania;

iv) nieuprawnione lub przypadkowe uszkodzenie, utratę, zniszczenie lub zmianę Danych osobowych.

15.2. W przypadku stwierdzenia naruszenia ochrony Danych osobowych Przedsiębiorstwo dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych oraz szacuje skalę ryzyka.

15.3. W przypadku naruszenia ochrony Danych Osobowych, Przedsiębiorstwo bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu właściwemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Wzór zawiadomienia, o którym mowa w zdaniu poprzedzającym, stanowi Załącznik nr 7 do Polityki.

15.4. Jeżeli ryzyko naruszenia praw i wolności osoby, której Dane osobowe dotyczą jest wysokie, Przedsiębiorstwo zawiadamia o incydencie także osobę, której danej dotyczą, chyba że:

i) Przedsiębiorstwo wdroży odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

ii) Przedsiębiorstwo zastosuje następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą; lub

iii) wymagałoby to niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

15.5. Niezależnie od obowiązków wskazanych w ust. 15.2-powyżej, Przedsiębiorstwo dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Wzór rejestru naruszeń danych osobowych stanowi Załącznik nr 8 do Polityki.

16 Powierzenie przetwarzania

16.1. Przedsiębiorstwo może powierzyć Przetwarzanie Danych osobowych Podmiotowi przetwarzającemu wyłącznie w drodze umowy zawartej w formie pisemnej lub innego instrumentu prawnego (np. Regulaminu lub ogólnych Zasad powierzania Danych osobowych) zgodnie z wymogami wskazanymi w art. 28 ust. 3 RODO.

16.2. Przedsiębiorstwo korzysta wyłącznie z usług takich Podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których Dane osobowe dotyczą. W celu weryfikacji spełnienia obowiązku, o którym mowa w zdaniu poprzedzającym, Przedsiębiorstwo przed powierzeniem przetwarzania potencjalnemu Podmiotowi przetwarzającemu w miarę możliwości uzyskuje informacje o zasadach ochrony Danych osobowych stosowanych przez potencjalny Podmiot przetwarzający oraz o praktykach tego podmiotu dotyczących zabezpieczenia Danych osobowych.

16.3. Szczegóły i zasady powierzenia Danych osobowych określa właściwa umowa lub instrument prawny.

17 Przekazywanie Danych osobowych w obrębie Przedsiębiorstwa

17.1. Dokumentacja zawierająca Dane osobowe przekazywana jest pomiędzy poszczególnymi jednostkami organizacyjnymi oraz Pracownikami z uwzględnieniem zasad ochrony Danych osobowych wskazanych w niniejszej Polityce.

17.2. W przypadku braku upoważnienia Pracownika odbierającego dokument do przetwarzania Danych osobowych, przekazywany jest on w sposób uniemożliwiający naruszenie Danych osobowych przy zastosowaniu wystarczających środków technicznych i organizacyjnych:

i) wiadomości e-mail przesyłane są do innego Pracownika nieupoważnionego do przetwarzania Danych po wcześniejszym usunięciu Danych osobowych ze stopek maila oraz jego treści lub zaszyfrowaniu Danych w sposób uniemożliwiający identyfikację osoby, której Dane dotyczą;

ii) dokumenty papierowe i elektroniczne przekazywane do innego Pracownika nieupoważnionego do przetwarzania Danych osobowych podlegają anonimizacji lub szyfrowaniu w zakresie Danych;

iii) dokumenty w formie papierowej przekazywane do osoby, której Dane osobowe dotyczą za pośrednictwem innego Pracownika nieupoważnionego do przetwarzania Danych, wkładane są do kopert lub nieprzezroczystych teczek opisanych w sposób uniemożliwiający identyfikację adresata.

17.3. Dokumenty papierowe przekazywane do osoby, której Dane osobowe dotyczą za pośrednictwem innego Pracownika, przechowywane są i transportowane do czasu ich wydania adresatowi w sposób uniemożliwiający naruszenie Danych osobowych.

18 Przekazywanie danych do Państwa trzeciego

18.1. Przedsiębiorstwo nie przekazuje Danych osobowych do państwa trzeciego położonego poza terytorium Unii Europejskiej lub Europejskiego Obszaru Gospodarczego, poza sytuacjami, w których następuje to na wniosek osoby, której Dane osobowe dotyczą.

18.2. Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych, Przedsiębiorstwo okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.

19 Postanowienia końcowe

19.1. Polityka wchodzi w życie z dniem ogłoszenia.

19.2. W sprawach nieuregulowanych w Polityce odpowiednie zastosowanie znajdują postanowienia RODO oraz powszechnie obowiązujące przepisy prawa polskiego i europejskiego.

19.3. Wszelkie zmiany lub uzupełnienia do Polityki wymagają dla swej skuteczności formy pisemnej pod rygorem nieważności. Zmiany lub uzupełnienia do Polityki wchodzą w życie nie wcześniej niż w terminie 7 dni od dnia ich ogłoszenia.