Polityka Ochrony Danych osobowych

„STOLGRAF" Pasternak Rodziewicz Sp. J.
ul. Świebodzka 41
58-141 Stanowice
NIP 884-001-32-85

zwanej dalej Firmą wprowadzona od dnia 25.05.2018

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 Firmie 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 Firma 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 Firmie 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 Firmie wymogów, procedur oraz zasad ochrony danych osobowych. Polityka zawiera:
   (I) zawiera opis zasad ochrony danych obowiązujących w Firmie;
   (II) zbiór procedur, instrukcji i regulacji szczegółowych dotyczących przetwarzania Danych osobowych w Firmie, dotyczących poszczególnych obszarów z zakresu ochrony danych osobowych; stanowiących załączniki do Polityki.

1.2. Polityka obowiązuje wszystkich pracowników oraz współpracowników Firmy Za przestrzeganie i utrzymanie postanowień Polityki odpowiedzialni są:
   (I) Firma;
   (II) komórki organizacyjne Firmy, 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 Firma zapewnia:
   (I) wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających zgodność przetwarzania Danych osobowych z wymogami prawa oraz niezbędne zabezpieczenie przetwarzanych danych osobowych;

(II) stałe monitorowanie zgodności przetwarzania Danych osobowych z wymogami prawa oraz poddawanie środków, o których mowa w ust. 1.3.(I) wyżej ciągłym przeglądom oraz uaktualnianiu;

(III) kontrolę i nadzór nad przetwarzaniem Danych osobowych.

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

1.5. Firma zapewnia zgodność postępowania kontrahentów Firmy, 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 Firmy.

1.7. Politykę udostępnia się:

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

(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) Polityka – oznacza niniejszą Politykę wraz ze wszystkimi ewentualnymi Załącznikami;

(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) 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);

(IV) Osoba upoważniona – oznacza osobę upoważnioną przez Firmę do przetwarzania Danych osobowych w danym zakresie;

(V) 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;

(VI) Zbiór danych – oznacza każdy uporządkowany zestaw Danych osobowych, dostępny według określonych kryteriów;

(VII) Podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Firmy.

(VIII) Rejestr - oznacza Rejestr Czynności Przetwarzania Danych Osobowych Firmy;

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

(X) Firma – oznacza "STOLGRAF" Pasternak Rodziewicz Sp. J. ul. Świebodzka 41 58-141 Stanowice; NIP 884-001-32-85; KRS 0000090951.

(XI) Pracownicy – oznaczają zarówno osoby zatrudnione w Firmie na podstawie stosunku pracy, jak również osoby fizyczne współpracujące z Firmą na podstawie Umowy cywilnoprawnej;

(XII) System – oznacza System ochrony danych osobowych w Firmie, o którym mowa w § 5 Polityki;

(XIII) Dane wrażliwe – oznaczają Dane Osobowe, o których mowa w art. 9 RODO.

§ 3 Dane osobowe

3.1. Firma przetwarza Dane osobowe gromadzone w zbiorach danych. Zbiory danych przetwarzane w Firmie 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. Firma 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 Firma obligatoryjnie przeprowadza uprzednią ocenę skutków przetwarzania, o których mowa w art. 35 RODO.

3.4. Dane osobowe domyślnie Przetwarzane są na obszarze na terenie obejmującym pomieszczenia biurowe Firmy zlokalizowane w Stanowicach ul. Świebodzka 41 58-141 i w oddziale zlokalizowanym w Świdnicy 58-100 ul. M. Konopnickiej 13. Dodatkowy obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym w zdaniu poprzedzającym.

§ 4 Podstawy ochrony Danych Osobowych w Firmie

4.1. Firma 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 Firmie zobowiązane są do Przetwarzania Danych osobowych zgodnie z wymogami prawa oraz zgodnie z postanowieniami Polityki, jak również innych wewnętrznych aktów prawnych Firmy lub procedur wewnętrznych związanych z Przetwarzaniem Danych Osobowych.

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

(I) Pracownicy przez przystąpieniem do wykonywania obowiązków służbowych otrzymują należytą wiedzę w zakresie zasad Przetwarzania i ochrony Danych Osobowych w Firmie;

(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 w tajemnicy sposób zachowania poufności i integralności Danych Osobowych;

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

4.4. Firma zapewnia, aby Dane Osobowe Przetwarzane w Firmie 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; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("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. 4.1 wyżej Firma opiera Przetwarzanie na następujących podstawach:

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

(II) Bezpieczeństwo − Firma zapewnia odpowiedni poziom bezpieczeństwa Danych osobowych podejmując stale działania w tym zakresie;

(III) Prawa Jednostki − Firma umożliwia osobom, których Dane Osobowe są przetwarza, wykonywanie swoich praw i prawa te realizuje;

(IV) Rozliczalność – Firma zapewnia należyte udokumentowanie sposobu spełniania obowiązków w zakresie ochrony danych osobowych.

.

§ 5 System ochrony danych osobowych

5.1. Firma 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 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) wdrożenie Procedury otwierania i zamykania budynków oraz pomieszczeń biurowych, która stanowi Załącznik nr 5 do Polityki;

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

(VIII) 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 Firmie przed złośliwym oprogramowaniem,

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

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

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

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

(XI) monitorowanie zmian w zakresie procesów Przetwarzania Danych osobowych w Firmie oraz na bieżąco zarządza zmianami mającymi wpływ na ochronę Danych osobowych w Firmy.

§ 6 Rejestr

6.1. Rejestr obejmuje kategorie czynności przetwarzania Danych Osobowych w Firmie. Za pośrednictwem Rejestru Firma 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, Firma 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 Firmy, 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, Firma dokonuje niezwłocznego uaktualnienia Rejestru celem zapewnienia

zgodności Rejestru ze stanem faktycznym oraz zakresem operacji przetwarzania Danych osobowych w Firmie.

6.5. Postanowienia ust. 6.3 wyżej 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. Firma 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 Firmę, uzasadniony cel Firmy.

§ 7 Realizacja obowiązków wobec osób, których dane osobowe dotyczą

7.1. Firma 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, takich jak zgłoszenie sprzeciwu lub ograniczenie przetwarzania.

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

7.3. Firma publikuje na stronie internetowej Firmy oraz pozostawia do wglądu w siedzibie Firmy:

(I) Politykę;

(II) Informację o prawach osób, których dane dotyczą;

(III) Informację o zakresie przetwarzanych danych osobowych w poszczególnych celach;

(IV) Metodach kontaktu z Firmą w zakresie danych osobowych;

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

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

(I) o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.

(II) o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej;

(III) o planowanej zmianie celu przetwarzania danych.

(IV) przed uchyleniem ograniczenia przetwarzania.

(V) o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).

(VI) o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

7.6. Firma 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. 7.5 wyżej, Firma określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).

7.8. Na żądanie osoby dotyczące dostępu do jej danych, Firma informuje osobę, czy przetwarza jej dane 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. Firma wydaje osobie, której Dane osobowe dotyczą kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.

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

7.11. Firma uzupełnia i aktualizuje dane na żądanie osoby, której Dane osobowe dotyczą. Firma ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Firma może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Firmę procedur, prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

7.12. Z uwzględnieniem ust. 7.13 niżej, na żądanie osoby, Firma 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. Firma 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 Firmę, Firma 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 Firma informuje osobę o odbiorcach danych, na żądanie tej osoby.

7.15. Firma 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) Firma 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 Firmy zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

7.16. W trakcie ograniczenia przetwarzania Firma 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. Firma informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Firma informuje osobę o odbiorcach danych, na żądanie tej osoby.

7.17. Na żądanie osoby Firma 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 Firmie, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Firmy.

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 Firmę w oparciu o uzasadniony interes Firmy lub o powierzone Firmie zadanie w interesie publicznym, Firma zobowiązuje się uwzględni sprzeciw, o ile nie zachodzą po stronie Firmy 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 Firmę na potrzeby marketingu bezpośredniego, Firma uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

§ 8 Minimalizacja danych

8.1. Firma 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 Firmę.

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

8.3. Firma stosuje ograniczenia dostępu do Danych Osobowych poprzez wdrożenie:

(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;

(III) wdrożenie logicznych środków technicznych ochrony Danych osobowych poprzez ograniczenie dostępu do systemów, oprogramowania oraz zasobów sieciowych wykorzystywanych w procesie Przetwarzania Danych Osobowych;

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

8.4. Firma dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających. Firma dokonuje okresowego przeglądu ustanowionych użytkowników systemów i 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 Firmy.

8.6. Firma przetwarza dane osobowe z uwzględnieniem kryteriów wskazanych w Rejestrze FIRMY wdraża mechanizmy kontroli cyklu życia danych osobowych w Firmie, 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 Firmy, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Firmę. 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. 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 Firma wdraża środki techniczne i organizacyjne zapewniające należyty stopień ochrony Danych osobowych, odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Firmę.

9.2. Firma przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

(I) Firma kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają;

(II) Firma przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Firma 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;

9.3. Firma 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.

§ 10 Naruszenie ochrony danych osobowych

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

(I) Naruszenie bezpieczeństwa systemów informatycznych, 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.

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

10.3. W przypadku naruszenia ochrony Danych Osobowych, Firma 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.

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

(I) Firma 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) Firma 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.

10.5. Niezależnie od obowiązków wskazanych w ust. 10.2-10.4 wyżej, Firma 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.

§ 11 Powierzenie przetwarzania

11.1. Firma może powierzyć Przetwarzanie Danych osobowych Podmiotowi przetwarzającemu wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi w art. 28 ust. 3 RODO. Powierzenie Przetwarzania Danych osobowych, o którym mowa w zdaniu poprzedzającym nie może prowadzić do naruszenia tajemnicy Firmy.

11.2. Firma korzysta wyłącznie z usług takich Podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą. W celu weryfikacji spełnienia obowiązku, o którym mowa w zdaniu poprzedzającym, Firma 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.

§ 12 Przekazywanie danych do Państwa trzeciego

12.1. Firma 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.

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

§ 13 Postanowienia końcowe

13.1. Polityka wchodzi w życie z dniem ogłoszenia.

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

13.3. 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.

Stanowice, dnia 23.05.2018

Zarząd firmy Stolgraf