Polityka

Bezpieczeństwa Danych Osobowych

Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski

ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo

w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), USTAWA z dnia 25 maja 2018 r. o ochronie danych osobowych

Regulacje prawne i organizacyjne

Data wydania: 24 maja 2018 r.	Wydanie: 1
Dokument spełnia wymagania:	• Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), • Ustawa z dnia 25 maja 2018 roku o ochronie danych osobowych, • Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 poz. 2247),

Metryka dokumentu

ZATWIERDZENIE DOKUMENTU		
Sporządził	Sprawdził	Zatwierdził
Krzysztof Michalski	Krzysztof Michalski	Krzysztof Michalski
Status: obowiązuje od	Właściciel dokumentu	Data zatwierdzenia
24.05.2018 r.	Krzysztof Michalski	24.05.2018 r.

Historia przeglądu i zmian dokumentu

Data / wydania/zmiany	Opis zmiany
	Pierwsze wydanie dokumentu

Spis treści

1. Postanowienia ogólne

Administratorem przetwarzanych w Firmie Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo jest Krzysztof Michalski.

Nad sprawnym nadzorowaniem prawidłowego przetwarzania danych osobowych w Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo pieczę sprawuje Administrator.

Administrator zgodnie z art.30 RODO prowadzi rejestr czynności przetwarzania danych osobowych.

Niniejsza Polityka Bezpieczeństwa Danych Osobowych:

a) określa zasady postępowania w związku z przetwarzaniem danych osobowych w Firmie Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo
b) jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych w Firmie Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo
c) obowiązuje wszystkich użytkowników w Firmie Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo
a) odnosi się zarówno do przetwarzania danych osobowych w formie papierowej (tradycyjnej) jak i przetwarzanych w systemach informatycznych w Firmie Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo

Przetwarzanie danych osobowych w Firmie Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo jest dopuszczalne tylko pod warunkiem przestrzegania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), oraz wydanych na jej podstawie przepisów wykonawczych.

2. Podstawowe definicje

Ilekroć w dokumencie jest mowa o:

Rozporządzeniu – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.

w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

Ustawie – rozumie się ustawę z dnia 25 maja 2018 roku o ochronie danych osobowych;

Firma – rozumie się Firma Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo;

Administratorze – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

Inspektorze Ochrony Danych (IOD) – rozumie się przez to osobę, którą Administrator powołał do wsparcia w wypełnianiu ustawowych obowiązków;

Danych osobowych – w rozumieniu Rozporządzenia oznaczają 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;

Szczególnych kategoriach danych osobowych – rozumie się przez to dane określone w art. 9 RODO, a więc dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatach karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym;

Danych genetycznych - oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

Danych biometrycznych - oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

Dokumentacji bezpieczeństwa informacji – rozumie się przez to dokument Polityki Bezpieczeństwa Danych Osobowych, Instrukcję Zarządzania Systemem Informatycznym oraz pozostałe polityki, regulaminy, procedury, instrukcje, formularze przyjęte do stosowania w organizacji, mające na celu wskazanie reguł i zasad postępowania w związku z przetwarzaniem danych osobowych;

Haśle – rozumie się przez to co najmniej 8-znakowy ciąg znaków literowych, cyfrowych, zawierający duże i małe litery oraz znaki specjalne, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

Identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w wyznaczonych przez Administratora obszarach systemu informatycznego;

Incydencie bezpieczeństwa – rozumie się przez to czynności, zdarzenia, zjawiska naruszające przepisy niniejszej polityki bezpieczeństwa oraz pozostałych dokumentów bezpieczeństwa informacji, mogące zagrozić utracie aktywów informacyjnych w Firmie Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo ich integralności lub dostępności, a także dopuścić do nieuprawnionego dostępu do danych, mogące stanowić sytuację kryzysową;

Przetwarzaniu danych – 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;

Rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

Systemie informatycznym – rozumie się przez to 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;

Użytkowniku – rozumie się przez to pracownika, zleceniobiorcę, współpracownika, zatrudnionego na podstawie: umowy o pracę, umowy zlecenia lub innej umowy przewidzianej przepisami prawa oraz osobę odbywającą staż, praktykę studencką, wolontariat, która przetwarza dane osobowe;

Zgoda osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

Podmiot przetwarzający oznacza organizację lub osobę, której Spółka powierzyła przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna księgowość, usługodawca BHP, usługodawca monitoringu i ochrony obiektu).

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.

Rejestr czynności przetwarzania / Rejestr kategorii czynności przetwarzania - Jest to dokument, który ma pokazywać w szczególności w jakich procesach w organizacji są przetwarzane dane osobowe, w jakim celu, kogo dotyczą oraz jak są zabezpieczane. Dokument ten będzie musiał zostać udostępniony na każde wezwanie Organu Nadzorczego (art.30 ust. 1 i 2 RODO).

3. Wykaz osób odpowiedzialnych za zarządzanie ochroną danych osobowych

3.1 Za zarządzanie ochroną danych osobowych w Firmie Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo odpowiadają:

a) Administrator;
b) Osoby uprawnione do wykonywania prac administracyjnych w systemie informatycznym;
c) Podmioty, którym powierzono przetwarzanie danych.

3.2 Wykaz osób powołanych do pełnienia funkcji określonych w ust. 3.1 stanowi zał. 1 PBDO.

4. Obowiązki Administratora

4.1. **Administrator** realizuje zadania w zakresie ochrony danych osobowych, a w szczególności:

a) może wyznaczyć Inspektora Ochrony Danych oraz Administratora Systemów Informatycznych;
b) podejmuje odpowiednie działania w celu zabezpieczenia danych osobowych;
c) zleca odpowiednim służbom w Firmie Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo zapewnienie użytkownikom danych osobowych wyposażenie w odpowiednie środki bezpieczeństwa stanowisk pracy, umożliwiające bezpieczne przetwarzanie danych;
d) wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane;
e) prowadzenie rejestrów czynności przetwarzania (rejestr czynności przetwarzania oraz rejestr powierzonych czynności przetwarzania);
f) 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 wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą;
g) wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

h) zarządzanie systemami informatycznymi organizacji w sposób gwarantujący utrzymanie poufności, dostępności i integralności gromadzonych w nich danych na poziomie pozwalającym zachować zgodność z wymogami prawnymi i organizacyjnymi;

i) sprawowanie nadzoru nad funkcjonowaniem zabezpieczeń systemów informatycznych;

j) podejmowanie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa powierzonego mu systemu informatycznego, zgodnie z procedurami nadzoru nad incydentami bezpieczeństwa oraz utrzymania ciągłością działania;

5. Organizacja przetwarzania danych osobowych

5.1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

e) przetwarzanie jest niezbędne do wykonania zadania realizowa-nego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nad-rzędny charakter wobec tych interesów mają interesy lub pod-stawowe prawa i wolności osoby, której dane dotyczą, wyma-gające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

5.2. Przetwarzanie szczególnych kategorii danych osobowych Art. 9 RODO

1. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.
2. Do przetwarzania powyższych danych dopuszcza się jedynie jeśli został spełniony jeden z poniższych warunków i wykazany w Rejestrze Czynności Przetwarzania:

a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;

b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wy-konywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidu-jącymi odpowiednie zabezpieczenia praw podstawowych i inte-resów osoby, której dane dotyczą;

c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;

d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;

e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;

h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;

i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;

j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

3. Dane osobowe, o których mowa w punkcie 1, mogą być przetwarzane do celów, o których mowa w pkt. 2 lit. h), jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa powszechnie obowiązującego.

5.3. Rejestr czynności przetwarzania - RCPD

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.

Prowadzenie rejestru czynności przetwarzania jest obowiązkiem dla Administratora wprowadzonym przez RODO (art.30).

W rejestrze tym zamieszcza się następujące informacje:

1. Imię i nazwisko lub nazwa oraz dane kontaktowe Administratora oraz wszelkich współadminstratorów, a także gdy to ma zastosowanie przedstawiciela administratora i IODO;
2. Cele przetwarzania;
3. Opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych;

4. Kategorie odbiorców, którym dane osobowe zostały ujawnione w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych;
5. Gdy ma to zastosowanie, przekazanie do państwa trzeciego lub organizacji międzynarodowej;
6. Jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych danych;
7. Jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Rejestr czynności przetwarzania ma mieć formę pisemną oraz formę elektroniczną. Innymi słowy, plik elektroniczny zawierający rejestr czynności przetwarzania powinien być możliwy do wygenerowania w formie papierowej.

Administrator udostępni przedmiotowy rejestr na żądanie organu nadzorczego.

5.4. Rejestr kategorii czynności przetwarzania powierzonego

W momencie gdy **podmiot trzeci** występuje w roli podmiotu przetwarzającego prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje:

a) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
c) gdy ma to zastosowanie –przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

Rejestr kategorii czynności przetwarzania powierzonego ma mieć formę pisemną oraz formę elektroniczną. Innymi słowy, plik elektroniczny zawierający rejestr czynności przetwarzania powinien być możliwy do wygenerowania w formie papierowej.

Administrator udostępni przedmiotowy rejestr na żądanie organu nadzorczego.

5.5. Gromadzenie i przetwarzanie danych osobowych

Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie Administratora.

Dane osobowe przetwarzane w Firmie Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo mogą być uzyskiwane w granicach dozwolonych przepisami prawa.

Dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu”);
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);

d) 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”);

e) 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; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);

f) 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 („integralność i poufność”).

Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).

5.6. Obowiązek informacyjny

Przy przetwarzaniu danych osobowych Administrator musi pamiętać o spełnieniu tzw. obowiązku informacyjnego względem osoby, której dane dotyczą.

Osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem. W szczególności, konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania.

Firmie Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo spełnia niniejszy obowiązek poprzez zamieszczenie informacji:

a) w stopce wiadomości elektronicznej
b) dodanie odpowiedniej klauzuli w stosowanych formularzach
c) stosowanie odpowiedniej klauzuli w procesie rekrutacyjnym
d) dodając zapisy do umowy o pracę, umowy zlecenia, umowy o dzieło i innych umów pozostających w obrocie
e) informując w regulaminie wykorzystania plików „cookies”

5.7. Udzielanie informacji o przetwarzaniu danych osobowych art. 13 – 21 RODO

Osobom, których dane przetwarzane są w Firmie Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski, ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo przysługuje prawo do kontroli treści ich danych osobowych, a w szczególności prawo do uzyskania wyczerpujących informacji na temat tych danych.

Każda osoba, która wystąpi z wnioskiem o otrzymanie informacji o jej danych, musi ją otrzymać w nieprzekraczalnym terminie miesiąca od otrzymania żądania art. 12 ust. 3 RODO. Odpowiedź przygotowuje Administrator Danych lub osoba przez niego wyznaczona.

W uzasadnionych przypadkach termin ten może być przedłużony o kolejne 2 miesiące z podaniem osobie żądającej wyjaśnienia przyczyny opóźnienia.

W przypadku gdy dane osobowe są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem ustawy lub są zbędne do realizacji celu, dla którego zostały zebrane, osoba wyznaczona przez Administratora jest zobowiązana do dokonania zmiany celem ich uzupełnienia, uaktualnienia lub sprostowania. O każdym wniosku o udzielenie informacji oraz ewentualnej konieczności sprostowania danych należy powiadomić IOD.

5.8. Zgoda

Jedną z przesłanek uprawniających do przetwarzania danych osobowych jest zgoda wyrażona przez osobę, której dane dotyczą, na ich przetwarzanie. Tworząc formularz zgody, administrator danych stosuje osobne zgody w zależności od celu w jakim będą zbierane i przetwarzane dane osobowe.

Osoba, która wyraża zgodę na przetwarzanie danych osobowych, musi wiedzieć, na czyją rzecz udziela przedmiotowej zgody i w jakim celu oraz jakie konkretnie dane będą przetwarzane.

Osoba, której dane dotyczą ma prawo w dowolnym momencie wycofać udzieloną zgodę.

W momencie kiedy firma przetwarza dane na podstawie zgody osób niepełnoletnich zgodę na powyższe działania musi wyrazić prawny opiekun dziecka.

5.9. Prawa osób, które dane dotyczą

Ogólne rozporządzenie o ochronie danych nadaje daleko idące uprawnienia osobom, których dane dotyczą. Prawa te dają osobie, której dane dotyczą, większą kontrolę nad dotyczącymi jej informacjami. Rozporządzenie dostrzega przede wszystkim, iż osoby fizyczne powinny mieć kontrolę nad własnymi danymi osobowymi.
Osoba, której dane dotyczą, powinna mieć przede wszystkim zapewniony łatwy dostęp do swoich danych, a informacje, które są jej komunikowane, powinny, zgodnie z zasadą przejrzystości, być dla niej jasne i precyzyjne. Rozporządzenie przyznaje następujące prawa osobom, których dane dotyczą:

1) Prawo do przejrzystego informowania i przejrzystej komunikacji oraz zachowania trybu wykonywania praw przez osobę, której dane dotyczą (art. 12 RODO);
2) Prawo do bycia poinformowanym o przetwarzaniu danych przy zbieraniu danych od osoby, której dane dotyczą (art. 13 RODO);
3) Prawo do bycia poinformowanym o przetwarzaniu danych w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą (art. 14 RODO);
4) Prawo dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO);
5) Prawo ograniczenia przetwarzania danych;
6) Prawo do sprostowania danych (art. 16 RODO);
7) Prawo do usunięcia danych - „prawo do bycia zapomnianym” (art. 17 RODO);
8) Prawo do ograniczenia przetwarzania (art. 18 RODO);
9) Prawo do powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19 RODO);
10) Prawo do przenoszenia danych (art. 20 RODO);
11) Prawo do sprzeciwu (art. 21 RODO);
12) Ograniczenie profilowania (art. 22 RODO).

5.10. Procedury egzekwowania praw osób, których dane dotyczą.

Realizacja prawa do poprawiania danych osobowych

Poprawienie danych osobowych w zbiorach przetwarzanych przez Administratora następuje poprzez zebranie od osoby, której dane są przetwarzane i poprawiane zaktualizowanego formularza na podstawie, którego pobrano od tej osoby dane.

W momencie gdy dane zostały zebrane z innych źródeł poprawienie danych następuje na pisemny wniosek osoby, której dotyczą przetwarzane dane.

Jeśli dane zostały przekazane do odbiorców lub podmiotów przetwarzających na mocy umowy, Administrator informuje ich o fakcie poprawienia danych osobowych, chyba że zostanie wykazane, iż wymaga to zbyt dużego wysiłku lub jest technicznie niewykonalne.

Realizacja prawa do przeniesienia danych osobowych

Prawo do przeniesienia danych osobowych realizowane jest tylko w zakresie danych osobowych, których podstawę legalności przetwarzania stanowi zgoda osoby, której dane są przetwarzane, w innym wypadku prawo do przeniesienia danych osobowych nie ma zastosowania.

Powyższe uprawnienie jest realizowane tylko na pisemny wniosek, osoby której dane dotyczą.

Wniosek identyfikuje osobę, której dane należy przenieść, wskazuje konkretnie jakie dane mają zostać przeniesione oraz dane podmiotu do którego dane mają zostać przeniesione, a w szczególności ze wskazaniem podstawowych danych identyfikacyjnych podmiotu (NIP, REGON, KRS itp.).

Realizacja prawa do zapomnienia

Prawo do zapomnienia realizowane jest tylko w zakresie danych osobowych, których podstawę legalności przetwarzania stanowi zgoda osoby, której dane są przetwarzane, w innym wypadku prawo do zapomnienia nie ma zastosowania.

Powyższe uprawnienie jest realizowane tylko na pisemny wniosek, osoby której dane dotyczą.

Wniosek identyfikuje osobę, której dane należy usunąć, wskazuje konkretnie jakie dane mają zostać usunięte.

Realizacja prawa do sprzeciwu

Prawo do sprzeciwu jest realizowane tylko na skutek pisemnego wniosku osoby, której dane dotyczą i ograniczone tylko do danych, których legalność przetwarzania stanowi przesłanka uzasadnionego interesu prawnego realizowanego przez administratora.

W momencie otrzymania powyższego wniosku Administratora rozważa czy jego interesy są prawnie uzasadnione i nadrzędne w stosunku do praw i wolności osoby, która złożyła wniosek.

Jeśli dane są wykorzystywane do marketingu bezpośredniego lub podlegają tzw. profilowaniu Administratora usuwa takie dane niezwłocznie.

Po usunięciu danych osobowych Administratora informuje wnioskodawcę o zakończeniu realizacji procesu sprzeciwu.

5.11. Zasady udostępniania danych osobowych

Firma Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo udostępnia dane osobowe przetwarzane w swoich zasobach tylko podmiotom uprawnionym do ich otrzymywania na podstawie umowy lub innego instrumentu prawnego. Dane osobowe udostępnia się na podstawie pisemnej zgody Administratora, chyba że odrębne przepisy prawa stanowią inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zasobach oraz wskazywać ich zakres i przeznaczenie. Decyzje w sprawie udostępnienia danych podejmuje Administrator.

5.12. Powierzenie przetwarzania danych osobowych

Administrator może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej. Podmiot, któremu w drodze umowy powierza się przetwarzanie danych osobowych, jest zobowiązany do zastosowania środków organizacyjnych i technicznych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania,

charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

Podjęcie współpracy z firmą zewnętrzną, która w trakcie realizacji powierzonych jej zadań (zleceń) będzie / może być związana z dostępem do danych osobowych wymaga zawarcia Umowy powierzenia przetwarzania danych osobowych.

5.13. Użytkownicy zatrudnieni przy przetwarzaniu danych osobowych

Użytkownicy zatrudnieni przy przetwarzaniu danych osobowych są zobowiązani powiadomić Administratora o ewentualnych naruszeniach bezpieczeństwa systemu ochrony danych osobowych.

5.14. Konsekwencje naruszenia Polityki Bezpieczeństwa Danych Osobowych

Naruszenie przepisów skutkuje nałożeniem:

a) administracyjnej kary pieniężnej art. 83 ust. 1 – 5 RODO;
b) sankcjami z tytułu naruszenia zasad Kodeksu Karego, Kodeksu Cywilnego, Kodeksu Pracy za nieprzestrzeganie postanowień dokumentacji oraz brak nadzoru nad bezpieczeństwem informacji, ujawnienie informacji osobie nieuprawnione;
c) odpowiedzialności cywilnej za naruszenie przepisów o ochronie danych osobowych;
d) odpowiedzialności karnej i administracyjnej kary pieniężnej za naruszenie przepisów o ochronie danych osobowych;

5.15. Wprowadzanie zmian do organizacji zabezpieczeń

Wprowadzanie, ustanawianie zabezpieczeń mających na celu ochronę danych osobowych musi uwzględniać normy prawne, normy zarządzania bezpieczeństwem informacji oraz pozostałe polityki, instrukcje i procedury przyjęte w Firmie Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo.

6. Organizacyjne i techniczne środki ochrony przetwarzanych danych

6.1. Stosowanie ochrony fizycznej pomieszczeń służbowych w Firmie Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo. Dane osobowe przetwarzane są w pomieszczeniach Firmy Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo w budynku zlokalizowanym przy: ul. Piłsudskiego 24b. Pomieszczenia, w których przetwarzane są dane, winny mieć zabezpieczone wejścia za pomocą zamków w sposób uniemożliwiający dostęp do nich osób niepowołanych, a użytkownicy muszą sprawować nadzór nad powierzonymi kluczami.

6.2. Zabezpieczenie danych osobowych przetwarzanych tradycyjnie.

Dane przetwarzane tradycyjnie (w formie papierowej) po godzinach pracy przechowywane winny być w szafkach zamkniętych (zamki, kłódki). Przetwarzanie danych osobowych w pomieszczeniach publicznie dostępnych musi odbywać się w sposób uniemożliwiający osobom niepowołanym podglądnięcie lub ich kradzież.

6.3. Zabezpieczenie danych przetwarzanych cyfrowo.

a) Dostęp do zasobów i usług informatycznych.

Stanowiska komputerowe w pomieszczeniach, gdzie przebywać mogą osoby nieupoważnione do przetwarzania danych - w tym danych osobowych (np. interesanci/petent) albo inni użytkownicy Firmy Gryf 1877 Złotnictwo –

Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo winny być umieszczone w sposób, który uniemożliwi takim osobom wgląd do tych danych.

W celu zapewnienia dostępu do danych każdy użytkownik systemu komputerowego korzysta z indywidualnego konta, o uprawnieniach dostępu odpowiednich do pełnionych obowiązków.

Dostęp do konta możliwy jest po podaniu prawidłowej pary (unikalnej nazwy użytkownika i hasła o długości min. 7 znaków). System powinien umożliwiać dostęp do zasobów użytkownika osobie zastępującej go podczas nieobecności przy zastosowaniu własnej nazwy użytkownika i własnego hasła, zgodnie z nadanym wcześniej poleceniem do pełnienia zastępstwa i upoważnienia do przetwarzania danych osobowych.

Każdy użytkownik, który ma dostęp do systemów informatycznych, winien posiadać unikalny login i hasło. Posiadacz hasła:

- zobowiązany jest uwierzytelniać się w systemie informatycznym wyłącznie na podstawie własnego loginu i hasła (za wyjątkiem hasła początkowego),
- odpowiedzialny jest za wykorzystywanie zgodnie z zasadami bezpieczeństwa swojego loginu i hasła oraz za wszystkie czynności wykonane przy użyciu swojego loginu i hasła,
- w żadnym wypadku nie może ujawniać swojego hasła komukolwiek, włącznie ze służbami informatycznymi, przełożonymi czy współpracownikami i innymi użytkownikami.

Hasło użytkownika nie może być przechowywane w formie możliwej do odczytania, tj. zapisane w plikach tekstem jawnym, skryptach i makrach, w pamięci przeglądarek internetowych, zapisane na kartkach i w miejscach, do których mają dostęp osoby nieupoważnione.

b) Nośniki danych używane w procesie przetwarzania danych, które przestają pełnić swoja funkcję winny zostać fizycznie zniszczone, bądź poddane procesowi „czyszczenia" w sposób uniemożliwiającej ich ponowne odczytanie.

Wykorzystywanie jakichkolwiek prywatnych nośników elektronicznych (np.: pendrive, przenośne dyski twarde, itd.) jest zabronione.

c) Ochrona przed szkodliwym oprogramowaniem.

Na wszystkich komputerach wymagana jest ochrona antywirusowa, która nie może być wyłączona przez użytkownika. Dodatkowo komputer winien być zabezpieczony przed możliwością instalowania i uruchamiania oprogramowania, którego celem jest nieuprawniony dostępu do systemu informatycznego oraz każdego innego nie posiadającego licencji.

d) Zasady bezpiecznego użytkowania laptopów i przenośnych nośników danych.

Laptopy podlegają tym samym regułom ochrony jak komputery stacjonarne, ponadto podlegają dodatkowej ochronie prawnej ze względu na traktowanie ich jako przenośna baza danych, a szczególnie:

- powinny być zabezpieczone fizycznie podczas użytkowania, transportu oraz przechowywania przed dostępem osób nieuprawnionych i kradzieżą (np. specjalna torba, linki "kensington lock", stały nadzór w przestrzeni publicznej),
- w trakcie pracy poza terenem kontrolowanym przez Firmę Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo (np. w podróży) należy zadbać, aby informacje chronione, zabezpieczone były odpowiednimi narzędziami kryptograficznymi,

6.4. Przebywanie na terenie Firmy Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo.

Użytkownikom wolno przebywać na terenie Firmy Gryf 1877 Złotnictwo – Grawerstwo Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo tylko w wyznaczonych godzinach pracy a po nich jedynie po zawiadomieniu i uzyskaniu zgody Administratora. Przebywanie w Firmie Gryf 1877 Złotnictwo – Grawerstwo

Krzysztof Michalski , ul. Piłsudskiego 24b/lok 6, 05-120 Legionowo w godzinach między 22:00 a 06:00 oraz w dni wolne od pracy możliwe jest jedynie po uzyskaniu zgody Administratora lub osoby przez niego upoważnionej.

6.5. Postępowanie w przypadku naruszenia bezpieczeństwa informacji

Wszyscy użytkownicy mają obowiązek natychmiastowego zgłaszania zauważonych zdarzeń i incydentów - potencjalnie niebezpiecznych Administratorowi (jeśli jest związane z systemem/siecią teleinformatycznym/ą).

W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Należy podkreślić, że ciężar dowodu wskazujący, iż jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, spoczywa na Administratorze.