POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Karol Kubicki

prowadzący działalność gospodarczą pod firmą

GOTREX KAROL KUBICKI

Zarzecze, 2021 r.

Wstęp

Karol Kubicki prowadzący działalność gospodarczą pod firmą GOTREX KAROL KUBICKI (dalej, jako ,,Administrator" i „GOTREX KAROL KUBICKI") tworzy niniejszy dokument dla wdrożenia rozwiązań pozwalających na zabezpieczenie przetwarzanych danych osobowych przed wszelkiego rodzaju incydentami naruszenia ochrony tych danych, zarówno wewnętrznymi, jak i zewnętrznymi, zwłaszcza prowadzącymi do naruszenia praw i wolności osób, których dane dotyczą.

Niniejsza Polityka bezpieczeństwa danych osobowych jest więc zbiorem procedur regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych członków personelu, klientów i kontrahentów GOTREX KAROL KUBICKI.

Karol Kubicki prowadzący działalność gospodarczą pod firmą GOTREX KAROL KUBICKI gwarantuje zabezpieczenie i ochronę danych poprzez: wdrożenie weryfikowalnych systemów zabezpieczeń fizycznych oraz informatycznych, tworzenie procedur organizacyjno-systemowych, wykorzystywanie odpowiedniego oprogramowania systemowego oraz utrzymywanie wysokiej świadomości obowiązków wynikających z treści przepisów prawa w zakresie ochrony danych osobowych przez wszystkich członków personelu GOTREX KAROL KUBICKI.

Karol Kubicki prowadzący działalność gospodarczą pod firmą GOTREX KAROL KUBICKI, mając na uwadze konieczność zapewnienia skutecznej ochrony przetwarzanych danych osobowych, deklaruje stałe wsparcie dla działań związanych z bezpieczeństwem danych osobowych i wdrożeniem niezbędnych mechanizmów zabezpieczających, zarówno o charakterze technicznym, jak i organizacyjnym. Wsparcie to przejawiać się będzie zarówno poprzez zapewnienie organizacji pracy pozwalającej na zagwarantowanie wymaganej ochrony danych, jak również alokację środków finansowych i pozafinansowych, niezbędnych do realizacji przedmiotowych działań.

Spis treści

Spis załączników

Zał. nr 26 – Protokół zniszczenia danych osobowych

Zał. nr 27 – Lista posiadaczy kluczy do GOTREX KAROL KUBICKI

Zał. nr 28 – Upoważnienie do wydawania kluczy

Zał. nr 29 – Ewidencja użytkowników kluczy zapasowych do GOTREX KAROL KUBICKI

Niniejsza Polityka bezpieczeństwa danych osobowych ma za zadanie zapewnić:

- ✓ Usystematyzowaną, formalną i skuteczną ochronę podstawowych praw i wolności osób fizycznych, w tym w szczególności prawa do ochrony danych osobowych, prawa do prywatności.
- ✓ Właściwe funkcjonowanie procedur gwarantujących realizację praw, o których mowa w pkt. 1 powyżej, właściwą implementację zasad oraz rozwiązań zawartych w Ogólnym rozporządzeniu o ochronie danych osobowych (RODO), z uwzględnieniem stopnia ryzyka związanego z przetwarzaniem danych osobowych oraz specyfiki działalności.
- ✓ Prawidłowe i praktyczne wdrożenie zasad przetwarzania danych osobowych, wskazanych w art. 6 ust. 1 Ogólnego rozporządzenia o ochronie danych osobowych (RODO) w oparciu o dokonywanie stałego szacowania ryzyka, w tym również dla ochrony praw i wolności osób fizycznych.
- ✓ Wdrożenie mechanizmów zapewniających realizację zasady rozliczalności, o której mowa w art. 6 ust. 2 Ogólnego rozporządzenia o ochronie danych osobowych (RODO).

🗁🖋 Postanowienia wstępne

1.1. Niniejsza Polityka bezpieczeństwa danych osobowych jest dokumentem, opisującym zasady przetwarzania danych osobowych w GOTREX KAROL KUBICKI oraz opisującym wszelkie środki techniczne i organizacyjne przyjęte w celu zapewnienia ich ochrony, jak również wymagania w zakresie bezpieczeństwa danych. Polityka musi być rygorystycznie przestrzegana we wszelkich procesach przetwarzania danych osobowych przez GOTREX KAROL KUBICKI.

1.2. Polityka bezpieczeństwa danych osobowych sporządzona została w związku z wymogami wynikającymi z postanowień 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).

1.3. Powyższe Rozporządzenie ma na celu ochronę prywatności osób, których dane dotyczą oraz samych danych przetwarzanych w ramach zdefiniowanych zbiorów w sposób zautomatyzowany lub niezautomatyzowany.

1.4. GOTREX KAROL KUBICKI przeprowadził inwentaryzację przetwarzanych danych osobowych poprzez zidentyfikowanie zasobów danych, ich kategorii, zależności pomiędzy zasobami, sposobów przetwarzania danych oraz aktualnego stanu ich zabezpieczeń.

1.5. **Celem ogólnym** niniejszej Polityki bezpieczeństwa danych osobowych jest zapewnienie stanu, w ramach którego przetwarzanie danych osobowych odbywa się w sposób zapewniający ochronę praw i wolności osób, których dane dotyczą oraz gwarantuje stopień bezpieczeństwa danych właściwy dla występujących ryzyk i zagrożeń związanych z poszczególnymi czynnościami przetwarzania.

1.6. **Celami szczegółowymi** Polityki bezpieczeństwa danych osobowych są:

1.6.1. praktyczna realizacja podstawowych praw i wolności osób fizycznych, w szczególności prawa do ochrony danych osobowych osób fizycznych

poprzez zapewnienie ochrony danych osobowych w najszerszym możliwym zakresie wymaganym przez prawo, a także wynikającym ze społecznej funkcji prawa do ochrony danych osobowych;

1.6.2. zmniejszenie ryzyka dostępu do danych osobowych przez osoby nieuprawnione;

1.6.3. ochrona prawa do prywatności osób, których dane są przetwarzane;

1.6.4. określenie zakresu obowiązków osób odpowiedzialnych za bezpieczeństwo danych;

1.6.5. stałe utrzymanie wysokiego poziomu poszanowania przepisów i zasad dotyczących ochrony danych osobowych w ramach działalności GOTREX KAROL KUBICKI.

1.7. Dla realizacji celów wskazanych w ust. 1.4. oraz 1.5. powyżej niezbędne są:

1.7.1. zastosowanie odpowiednich środków technicznych, organizacyjnych, systemowych, proceduralnych oraz wszelkich innych, które w skuteczny, weryfikowalny i trwały sposób są w stanie zapewnić realizację celów niniejszej Polityki;

1.7.2. prowadzenie okresowych szkoleń z zakresu zasad przetwarzania i ochrony danych osobowych dla personelu GOTREX KAROL KUBICKI oraz wszystkich osób, za które odpowiada GOTREX KAROL KUBICKI, a które mogą w sposób uprawniony korzystać z danych osobowych przetwarzanych w ramach działalności GOTREX KAROL KUBICKI;

1.7.3. bieżąca kontrola stanu zabezpieczeń ochrony danych oraz systematyczne szacowanie ryzyk występowania zagrożeń dla czynności przetwarzania, w tym również dla aktywów, w ramach których dochodzi do przetwarzania;

1.7.4. stała analiza adekwatności, aktualności i skuteczności środków przyjętych przez GOTREX KAROL KUBICKI dla realizacji celów niniejszej Polityki.

1.8. Niniejsza Polityka odnosi się do wszelkich czynności przetwarzania danych dokonywanych przez Karola Kubickiego prowadzącego działalność gospodarczą pod

firmą GOTREX KAROL KUBICKI., niezależnie od tego czy GOTREX KAROL KUBICKI występuje w nich jako administrator danych czy jako podmiot przetwarzający.

1.9. Karol Kubicki prowadzący działalność gospodarczą pod firmą GOTREX KAROL KUBICKI odpowiada za:

1.9.1. wdrożenie,

1.9.2. stosowanie,

1.9.3. nadzór oraz monitorowanie przestrzegania,

1.9.4. bieżące aktualizowanie

- przepisów niniejszej Polityki bezpieczeństwa danych osobowych.

1.10. Karol Kubicki prowadzący działalność gospodarczą pod firmą GOTREX KAROL KUBICKI w miarę możliwości zapewnia również zgodność postępowania swoich kontrahentów z niniejszym dokumentem w zakresie w jakim powierza się im lub udostępnia przetwarzane przez siebie dane osobowe.

2. Definicje

2.1. **Administrator danych** (również: **„Administrator", „GOTREX KAROL KUBICKI"**) -Karol Kubicki prowadzący działalność gospodarczą pod firmą GOTREX KAROL KUBICKI z siedzibą w Zarzeczu 120, 36-040 Boguchwała, wpisany do Centralnej Ewidencji i Informacji o Działalności Gospodarczej pod numerem NIP: 5170030089, numer REGON 180195538; Administrator realizuje swoje uprawnienia i obowiązki wynikającej z niniejszej Polityki bezpieczeństwa danych osobowych oraz przepisów powszechnie obowiązującego prawa.

2.2. **Rozporządzenie -** 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), zwane potocznie RODO lub GDPR;

2.3. **Inspektor ochrony danych (**również: „**IOD**", „**Inspektor**") **–** osoba fizyczna wyznaczona przez Administratora danych do stałego i systematycznego nadzorowania stosowania przepisów Rozporządzenia w ramach działalności GOTREX KAROL KUBICKI, włączona we wszelkie sprawy związane z ochroną danych osobowych w ramach działalności Administratora, o zapewnionym statusie niezależności w zakresie realizacji powierzonych sobie obowiązków;

2.4. **Administrator systemów informatycznych** (również „**ASI**") – osoba fizyczna wyznaczona przez Administratora danych do nadzorowania działania systemu informatycznego służącego do przetwarzania danych;

2.5. **dane osobowe** (również: **„dane"**) - wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną,

genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

2.6. **dane szczególnej kategorii** – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej;

2.7. **Polityka –** Polityka bezpieczeństwa danych osobowych, tj. niniejszy dokument;

2.8. **Rejestr** – Rejestr czynności przetwarzania danych osobowych, prowadzony przez Administratorów danych w oparciu o treść art. 30 ust. 1 Rozporządzenia, którego treść oraz zasady opracowania szczegółowo reguluje par. 12 Polityki; załącznikiem do Rejestru, obejmującym swoją treścią czynności przetwarzania dokonywane w ramach poszczególnych rodzajów oprogramowania wykorzystywanych przez Administratora, jest ID Card;

2.9. **DPIA** (*Data Protection Impact Assesment*) – ocena skutków dla ochrony danych osobowych, przetwarzanych przez Administratora danych, wykonywana w sytuacji wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych wskutek czynności przetwarzania danych; przeprowadzenie DPIA nie jest jednak równoznaczne ze stwierdzeniem przez Administratora wystąpienia sytuacji ryzyka naruszenia praw lub wolności osób fizycznych, a może wynikać z dbałości o zapewnienie należytej ochrony danych osobowych poddanych czynnościom przetwarzania; Administrator przeprowadza DPIA obowiązkowo w sytuacji, gdy dochodzi do: zautomatyzowanego przetwarzania danych, przetwarzania na dużą skalę danych o szczególnym charakterze, systematycznego monitorowania miejsc publicznie dostępnych oraz w przypadkach określonych w wykazie rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych; ocena skutków dla ochrony danych osobowych może zostać przeprowadzona z wykorzystaniem odpowiedniego oprogramowania informatycznego;

2.10. **podmiot przetwarzający** (również **„procesor”**) - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny administrator, który przetwarza dane osobowe w imieniu Administratora i w zakresie przez niego wskazanym;

2.11. **powierzenie przetwarzania danych osobowych** - zlecenie wykonywania czynności przetwarzania danych podmiotowi przetwarzającemu w drodze umowy zawartej na piśmie lub klauzuli umownej w odpowiedniej treści, wyłącznie w zakresie i w celu przewidzianym w zleceniu;

2.12. **odbiorca** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny administrator, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego nie są jednak uznawane za odbiorców;

2.13. **użytkownik danych** (również: „**użytkownik**”, „**użytkownicy danych”**) – osoba fizyczna będąca pracownikiem Administratora lub współpracująca z Administratorem w oparciu o umowę cywilnoprawną (umowa zlecenie, umowa o dzieło, umowa o staż/praktykę, umowa o współpracy);

2.14. **osoba upoważniona** (również: **osoby upoważnione**) – użytkownik, któremu Administrator udzielił upoważnienia do przetwarzania danych osobowych;

2.15. **system informatyczny** (również: „**systemy informatyczne**”) – rozumie się przez to zespół współpracujących ze sobą urządzeń (stacji roboczych: komputerów oraz komputerów przenośnych, serwerów, drukarek, systemu monitoringu, urządzeń wielofunkcyjnych, zewnętrznych dysków i nośników danych, UPS-ów, urządzeń emitujących sygnał), oprogramowania (systemów operacyjnych Windows, systemów, serwerów poczty wewnętrznej) i narzędzi programowych (aplikacji, skryptów, arkuszy roboczych, programów biurowych, w tym w ramach pakietu Microsoft Office, programów pocztowych; oprogramowania monitoringu) zastosowanych w celu przetwarzania danych oraz innych informacji chronionych, działających w oparciu o technologie informacyjne;

2.16. **przetwarzanie danych osobowych** (również „**czynności przetwarzania**”) – operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych

osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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;

2.17. **naruszenie ochrony danych osobowych** - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

2.18. **Ustawa –** Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z 2018 r. poz. 1000 z późn. zm.);

2.19. **państwo trzecie –** podmiot państwowy spoza Europejskiego Obszaru Gospodarczego**;**

2.20. **organ nadzorczy** - Prezes Urzędu Ochrony Danych Osobowych.

3. Zasady przetwarzania danych osobowych

3.1. Zasady przetwarzania danych osobowych w GOTREX KAROL KUBICKI to:

3.1.1. **legalizm –** przetwarzanie tylko w oparciu o podstawę prawną i zgodnie z przepisami prawa;

3.1.2. **rzetelność –** przetwarzanie danych w sposób rzetelny, uczciwy, przejrzysty dla osoby, której dane są przetwarzane;

3.1.3. **transparentność –** przetwarzanie danych w sposób jawny i czytelny dla osób, których dane dotyczą, z poszanowaniem prawa do informacji;

3.1.4. **minimalizacja –** przetwarzanie danych tylko w zakresie niezbędnym do realizacji konkretnych, wyraźnych i prawnie uzasadnionych celów Administratora lub wymaganych prawem oraz nieprzetwarzanie dalej w sposób niezgodny z tymi celami; minimalizacja dotyczy zakresu danych, dostępu do nich oraz czasu przetwarzania;

3.1.5. **adekwatność –** przetwarzanie tylko danych takiego rodzaju i takiej treści jakie niezbędne są do realizacji celów przetwarzania;

3.1.6. **prawidłowość –** przetwarzanie z dbałością o zgodność przetwarzanych danych z rzeczywistością, usuwanie lub uaktualnianie danych nieaktualnych;

3.1.7. **czasowość –** przetwarzanie tylko w czasie niezbędnym do realizacji celów Administratora lub wymaganym prawem;

3.1.8. **bezpieczeństwo –** przetwarzanie z zapewnieniem najlepszych dostępnych dla Administratora zabezpieczeń technicznych, organizacyjnych oraz systemowych, zapewniającym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.

3.2. Realizacja powyższych zasad odbywa się odpowiednio m.in. poprzez:

3.2.1. zidentyfikowanie dla każdej czynności przetwarzania danych w GOTREX KAROL KUBICKI konkretnej przesłanki prawnej, legalizującej przetwarzanie danych osobowych; przesłanki te wykazane zostały w Rejestrze;

3.2.2. rzetelną realizację obowiązku informacyjnego, właściwą obsługę żądań osób fizycznych oraz rejestrowania przypadków naruszeń zgodnie z treścią par. 17 Polityki;

3.2.3. przejrzystość działania Administratora danych w zakresie realizacji czynności opisanych w niniejszej Polityce, pełną realizację obowiązku informacyjnego; zdefiniowanie celów przetwarzania danych dla każdej czynności przetwarzania danych wraz ze wskazaniem zakresu danych niezbędnych do przetwarzania dla realizacji celu tego przetwarzania; co wyszczególnione zostało w Rejestrze;

3.2.4. zapewnienie, aby kierownicy komórek organizacyjnych, w ramach których odbywa się przetwarzanie danych osobowych, a w przypadku ich braku – osoby upoważnione, zobowiązani byli do okresowego, co najmniej raz do roku, weryfikowania czy dane osobowe przetwarzane w ramach zdefiniowanych zbiorów danych, są adekwatne do celów przetwarzania i czy nie są przetwarzane z przekroczeniem ustalonych okresów retencji danych; wszelkie dane nieadekwatne (nadmiarowe), niepotrzebne Administratorowi do realizacji prawnie uzasadnionych zadań będą niezwłocznie usuwane;

3.2.5. zapewnienie realizacji uprawnień osób, których dane dotyczą, opisane szczegółowo w par. 9 i par. 10 Polityki, jak również poprzez weryfikację danych otrzymywanych od osób fizycznych;

3.2.6. określenie - w ramach Rejestru oraz z uwzględnieniem przepisów prawa - dla każdego ze zbiorów danych okresu przechowywania; po przekroczeniu określonych w Rejestrze okresów należy trwale usunąć dane z wszelkich nośników; ustalenie maksymalnego okresu retencji danych, odbywa się z uwzględnieniem przepisów prawa, o ile określają one okresy przechowywania danych; szczegółowe zasady dotyczące realizacji obowiązku przechowywania danych jedynie przez określony, ograniczony okres czasu reguluje Polityka Retencji Danych Osobowych, stanowiąca załącznik nr 19 do Polityki;

3.2.7. poprzez stosowanie się do zasad określonych w par. 12 – par. 23 Polityki.

3.3. Realizacja zasad opisanych w ust. 1 powyżej odbywa się w sposób pozwalający zachować danym osobowym wskazanych atrybutów przetwarzania:

3.3.1. **poufność** – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;

3.3.2. **integralność** – rozumianą jako właściwość chroniącą dane osobowe przed nieautoryzowaną zmianą lub zniszczeniem;

3.3.3. **dostępność** – rozumianą jako właściwość pozwalającą na realizację żądań osób, których dane dotyczą w każdym czasie.

3.4. Za przetwarzanie danych oraz ich ochronę, zgodnie z przepisami Rozporządzenia oraz Polityki odpowiedzialni są:

3.4.1. Administrator danych;

3.4.2. IOD;

3.4.3. ASI;

3.4.4. osoby upoważnione.

4. Podstawy prawne przetwarzania danych

4.1. Administrator może przetwarzać dane osobowe tylko w sytuacji, gdy ma do tego określone prawem podstawy.

4.2. Przed rozpoczęciem przetwarzania danych, Administrator wskazuje podstawy legalizujące przetwarzanie danych oraz odnotowuje je w Rejestrze.

4.3. W sytuacji braku podstawy prawnej legalizującej przetwarzanie danych, Administrator zakończy operacje przetwarzania oraz dokona usunięcia lub, w wymaganych prawem okolicznościach, anonimizacji danych.

4.4. Podstawami prawnymi przetwarzania danych, zgodnie z treścią Rozporządzenia, są:

4.4.1. **zgoda osoby**, której dane dotyczą; zgoda ta musi być:

4.4.1.1. jednoznaczna - osoba udzielająca zgody musi zostać klarownie poinformowana co do tego na co wyraża zgodę; jeśli zgoda jest udzielana w formie pisemnej deklaracji, która również obejmuje inne kwestie (tj. rejestrację na stronie internetowej, potwierdzenie regulaminu, podpisanie zamówienia, akceptację ogólnych warunków umownych), należy zapewnić że zgoda jest jasno odróżnialna od innych kwestii, wyrażona jasnym i prostym językiem, a dostęp do jej treści możliwy dla osoby, której te dane dotyczą;

4.4.1.2. dobrowolna – Administrator nie może zmuszać do udzielenia zgody, np. poprzez uzależnianie udzielenia świadczenia od udzielenia zgody w określonym przez siebie zakresie;

4.4.1.3. konkretna – zakres zgody musi być maksymalnie szczegółowy i dokładny i odnosić się do jasno sprecyzowanego celu przetwarzania danych; przetwarzanie musi ograniczać się do celów określonych w zgodzie; zgoda nie może mieć charakteru ogólnego;

4.4.1.4. świadoma – osoba, której dane dotyczą musi być w sposób wyczerpujący o wszelkich konsekwencjach udzielenia zgody; ponadto, treść zgody powinna być wyrażona jasnym i prostym językiem;

4.4.1.5. wycofywalna – osoba, której dane dotyczą może w każdym czasie, bez podawania przyczyny, swoją zgodę wycofać, bez wpływu na zgodność z prawem przetwarzania, które miało miejsce przed wycofaniem zgody; wycofanie zgody powinno być dla osoby, której dane dotyczą równie łatwe, co jej udzielenie;

4.4.1.6. zgoda podlega utrwaleniu dla celów dowodowych (na piśmie lub elektronicznie);

4.4.2. **niezbędność przetwarzania do wykonania umowy** zawartej pomiędzy Administratorem a osobą, której dane dotyczą (lub do podjęcia działań na żądanie tej osoby przed zawarciem umowy); jeśli przetwarzanie danych jest niezbędne do wykonania zleconej usługi, podstawą do przetwarzania nie jest „zgoda", ale wskazana przesłanka;

4.4.3. **niezbędność przetwarzania do celów wynikających z prawnie uzasadnionych interesów Administratora**, za wyjątkiem sytuacji, gdy ochrona prywatności osoby, której dane dotyczą przeważa nad tymi celami; prawnie uzasadniony interes Administratora musi być każdorazowo jasno zdefiniowany i racjonalnie uzasadniony; interes ten Administrator wskazuje również osobie, której dane dotyczą, np. w treści klauzuli informacyjnej; Administrator dokonuje ważenia interesu dla weryfikacji czy nad jego interesem przeważa interes osoby, której dane dotyczą;

4.4.4. **niezbędność przetwarzania do wypełnienia obowiązku prawnego** ciążącego na Administratorze;

4.4.5. **niezbędność przetwarzania do ochrony żywotnych interesów osoby**, której dane dotyczą;

4.4.6. **niezbędność przetwarzania do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej** powierzonej Administratorowi i/lub osobom/podmiotom trzecim, którym dane zostały udostępnione.

4.5. Eksport danych do kraju spoza Europejskiego Obszaru Gospodarczego jest dozwolony wyłącznie, jeśli podmiot otrzymujący te dane w swoim kraju zapewnia adekwatny poziom ochrony do obowiązującego na terenie państw Europejskiego Obszaru Gospodarczego.

4.6. GOTREX KAROL KUBICKI unika przekazywania danych do podmiotów trzecich z siedzibą w państwach spoza Europejskiego Obszaru Gospodarczego, które nie są uznawane przez Komisję Europejską, jako kraje „bezpieczne". Przekazanie danych do państw spoza Europejskiego Obszaru Gospodarczego podlega surowym regułom.

4.7. Przetwarzanie danych szczególnej kategorii co do zasady jest zabronione. Przetwarzania takiego Administrator dokonywać może jedynie w przypadku zaktualizowania się jednej z przesłanek wymienionych w art. 9 ust. 2 Rozporządzenia.

5. Status Administratora danych

5.1. Administrator danych, celem zapewnienia ochrony danych osobowych i ich właściwego przetwarzania, zobowiązany jest w szczególności do:

5.1.1. wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z wymogami Rozporządzenia;

5.1.2. poddawanie w/w środków okresowym aktualizacjom, przeglądom i ocenom pod kątem należytego zapewnienia wysokiego poziomu ochrony danych;

5.1.3. prowadzenia rzetelnej dokumentacji dla wykazania wdrożenia właściwych i adekwatnych środków dla zapewnienia przetwarzania danych zgodnie z treścią Rozporządzenia oraz Polityki, z uwzględnieniem stałego monitorowania poziomu ryzyka dla ochrony danych;

5.1.4. zapewnienia, aby do przetwarzania danych osobowych dopuszczone były wyłącznie osoby upoważnione, przeszkolone w zakresie przetwarzania danych osobowych oraz ich ochrony;

5.1.5. zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo są przetwarzane oraz komu są one przekazywane;

5.1.6. prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, ewidencji naruszeń ochrony danych, ewidencji podmiotów, którym powierzono przetwarzanie danych osobowych;

5.1.7. bieżącego reagowania na zmiany przepisów prawa i okoliczności towarzyszących przetwarzaniu danych osobowych, dostosowywania procedur, w tym Polityki, do wymagań natury prawnej, technicznej lub organizacyjnej;

5.1.8. wdrażania procedur, mających na celu zapewnienie bezpieczeństwa danych osobowych, w szczególności wynikających z Polityki;

5.1.9. edukacji pracowników i innych osób upoważnionych w zakresie ochrony danych osobowych;

5.1.10. w sytuacji prawem wymaganej, wyznaczenia oraz zgłoszenia do organu nadzorczego inspektora ochrony danych;

5.1.11. dbanie o to by przekazywanie danych osobowych do państwa trzeciego odbywało się w zgodzie z przepisami prawa (w przypadku gdy ma zastosowanie);

5.1.12. zapewnienie właściwego włączenia Inspektora ochrony danych (o ile został powołany) we wszystkie sprawy dotyczące ochrony danych osobowych.

6. Status Inspektora ochrony danych osobowych

6.1. Administrator wyznacza Inspektora ochrony danych osobowych oraz właściwie i niezwłocznie włącza go we wszystkie sprawy dotyczące ochrony danych w ramach działalności GOTREX KAROL KUBICKI.

6.2. Inspektor jest zobowiązany do:

6.2.1. organizacji ochrony danych i bezpieczeństwa przetwarzania danych zgodnie z wymogami powszechnie obowiązującego prawa, w szczególności Rozporządzenia i Ustawy, oraz Polityki;

6.2.2. informowania Administratora oraz jego personelu o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz innych przepisów o ochronie danych osobowych, jak również stałego doradzania Administratorowi w tym zakresie;

6.2.3. nadzorowania wydawania przez Administratora danych upoważnień do przetwarzania danych osobowych;

6.2.4. nadzorowania prowadzenia wszelkich ewidencji (naruszeń, udzielonych upoważnień, administratorów, którym powierzono dane osobowe) przez Administratora;

6.2.5. prowadzenia i bieżącego aktualizowania Rejestru oraz Arkusza analizy ryzyka;

6.2.6. monitorowania przestrzegania przepisów prawa, w zakresie związanym z ochroną danych osobowych, w ramach działalności GOTREX KAROL KUBICKI;

6.2.7. udzielania zaleceń co do potrzeby przeprowadzenia DPIA, jak również monitorowania jej prawidłowego wykonania;

6.2.8. prowadzenie stosownych działań wyjaśniających w przypadku naruszenia ochrony danych osobowych, opisanych szczegółowo w par. 17 Polityki;

6.2.9. nadzoru nad stosowanymi metodami, środkami technicznymi i organizacyjnymi niezbędnymi dla zapewnienia poufności, integralności, dostępności i przejrzystości przetwarzania danych osobowych;

6.2.10. dbałości o realizację zasady rozliczalności wespół z Administratorem;

6.2.11. kontroli działań komórek organizacyjnych, w ramach GOTREX KAROL KUBICKI, pod względem zgodności przetwarzania danych osobowych z przepisami Rozporządzenia, Ustawy oraz innymi przepisami powszechnie obowiązujących aktów prawnych;

6.2.12. okresowego szkolenia pracowników i współpracowników Administratora danych oraz weryfikacji ich aktualnej wiedzy oraz stanu świadomości w zakresie przestrzegania danych osobowych;

6.2.13. rozpatrywania wniosków o udostępnienie danych osobowych;

6.2.14. opiniowania umów dotyczących powierzenia przetwarzania danych osobowych podmiotom przetwarzającym;

6.2.15. współpracy z organem nadzorczym;

6.2.16. pełnienia funkcji punktu kontaktowego dla organu nadzorczego oraz prowadzenie z nim konsultacji w wymaganych przypadkach;

6.2.17. inicjowania oraz podejmowania przedsięwzięć w zakresie doskonalenia ochrony danych osobowych w ramach działalności Administratora.

7. Status Administratora systemów informatycznych

7.1. W celu osiągnięcia wysokiego poziomu bezpieczeństwa danych osobowych przetwarzanych w ramach wszelkich systemów informatycznych w GOTREX KAROL KUBICKI, powołuje się funkcję Administratora systemów informatycznych (ASI).

7.2. ASI jest zobowiązany do:

7.2.1. nadzoru nad zabezpieczeniami systemu informatycznego, w tym jego systematycznej oceny pod kątem zapewnienia ochrony przed nieuprawnionym dostępem, utratą danych, w tym spowodowaną awarią zasilania, zakłóceniami w sieci zasilającej lub spowodowaną innymi przyczynami niesprawnością i wadliwym działaniem systemu informatycznego;

7.2.2. prowadzenie okresowej aktualizacji oprogramowania oraz narzędzi służących do przetwarzania danych osobowych, w tym również aktualizacji zabezpieczeń;

7.2.3. nadzorowania niszczenia kopii bezpieczeństwa i nośników danych w systemie informatycznym;

7.2.4. pełnienia szczegółowego nadzoru nad realizacją zadań i obowiązków wskazanych w Instrukcji zarządzania systemem informatycznym, stanowiącej załącznik nr 1 do Polityki.

8. Status osób upoważnionych

8.1. Każdy użytkownik, który uzyskał dostęp do danych osobowych obowiązany jest do ochrony tych danych w sposób zgodny z zasadami opisanymi w Rozporządzeniu oraz Polityce.

8.2. Użytkownik uzyskuje prawo do przetwarzania danych osobowych po otrzymaniu pisemnego upoważnienia do przetwarzania danych osobowych. Upoważnienie do przetwarzania danych osobowych szczegółowo precyzuje zakres danych, które użytkownik może przetwarzać, rodzaj czynności wykonywanych na danych, okres obowiązywania upoważnienia, cele przetwarzania w ramach udzielonego upoważnienia, systemy informatyczne, w ramach których dochodzi do przetwarzania danych.

8.3. Osoby upoważnione są zobowiązane do:

8.3.1. dysponowania na czas przetwarzania danych osobowych stosownym upoważnieniem wydanym przez Administratora danych;

8.3.2. przetwarzania danych osobowych wyłącznie w celach wynikających z udzielonego upoważnienia oraz zakresu obowiązków powierzonych przez Administratora;

8.3.3. przetwarzania danych osobowych w zgodzie z przepisami prawa, postanowienia Polityki i innymi regulacjami obowiązującymi w tym zakresie w ramach działalności GOTREX KAROL KUBICKI;

8.3.4. zachowania w tajemnicy wszelkich danych osobowych oraz informacji

9. Realizacja żądań i wniosków osób, których dane dotyczą (zasady ogólne)

9.1. Administrator zapewnia zgodną z treścią Rozporządzenia oraz Polityki realizację praw jednostki, której dane dotyczą, w szczególności poprzez:

9.1.1. **realizację obowiązku informacyjnego** – Administrator udziela osobom, których dane dotyczą niezbędnych informacji już na etapie ich gromadzenia, jak również w innych sytuacjach prawem wymaganych oraz dokumentuje w miarę możliwości realizację tych obowiązków;

9.1.2. **obsługę wniosków i żądań** – Administrator wdraża procedury umożliwiające weryfikację zasadności wniosków i żądań składanych wobec siebie oraz podmiotów przetwarzających, którym powierzył przetwarzanie danych osobowych, jak również zgodną z prawem oraz terminową obsługę tych wniosków i żądań, w tym rzetelne udokumentowanie jej realizacji;

9.1.3. **zawiadomienia o naruszeniach** – Administrator wdraża procedury umożliwiające odpowiednie reagowanie na przypadki naruszeń ochrony danych osobowych, w tym, w sytuacjach prawem wymaganych, poinformowanie o naruszeniu organu nadzorczego lub poinformowanie o naruszeniu osób, których dane dotyczą.

9.2. Administrator wprowadza adekwatne metody identyfikacji osób dla potrzeb realizacji żądań i wniosków, gwarantujące ochronę danych przed ich udostępnieniem osobom nieupoważnionym.

9.3. Administrator zapewnia, aby dostęp do treści żądań i wniosków osób, których dane dotyczą posiadały jedynie osoby, legitymujące się aktualnym upoważnieniem do przetwarzania danych osobowych, obejmującym swym zakresem przedmiotowym czynności w ramach przyjmowania wniosków od osób fizycznych (osoba upoważniona).

9.4. Przed zrealizowaniem żądania osoby uprawnionej:

9.4.1. Administrator lub osoba przez niego upoważniona bada treść wniosku oraz ewentualnie zasięga dodatkowych informacji od osoby upoważnionej zaangażowanej bezpośrednio w czynności przetwarzania, jak również od samej osoby uprawnionej;

9.4.2. jeżeli wniosek lub żądanie osoby, której dane dotyczą nie trafia bezpośrednio do Administratora, lecz do osoby upoważnionej, ta niezwłocznie przekazuje informację o wpływie wniosku lub żądania do Administratora;

9.4.3. osoby upoważnione obsługujące wniosek lub żądanie podejmują działania zmierzające do potwierdzenia tożsamości osoby składającej żądanie, tj. pozyskania jej imienia, nazwiska (w oparciu o okazany dokument tożsamości – w przypadku obecności osoby składającej wniosek lub żądanie) oraz okoliczności składanego wniosku;

9.4.4. jeżeli w dalszym ciągu istnieją uzasadnione wątpliwości co do tożsamości osoby składającej wniosek lub żądanie, osoba upoważniona obsługująca wniosek lub żądanie może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą, pozwalających na jej jednoznaczną weryfikację;

9.4.5. w przypadku wniosku składanego drogą telefoniczną lub elektroniczną Administrator zasięga dodatkowych informacji weryfikujących dotyczących zakresu danych objętych treścią wniosku (np. zapytanie o nazwisko panieńskie, PESEL lub inne dane osoby fizycznej przetwarzane przez Administratora);

9.4.6. Administrator odmawia osobie wykonania praw jej przysługujących jedynie w sytuacji, w której nie jest w stanie zidentyfikować osoby, której dane dotyczą.

9.5. Administrator zapewnia przejrzystość komunikacji z osobami, których dane dotyczą, w szczególności poprzez wyjaśnianie tym osobom treści przysługujących im uprawnień oraz podejmowanych przez siebie działań, stosując przy tym prosty język, dostosowany do możliwości percepcyjnych osoby, której wniosek dotyczy. Administrator w miarę możliwości ułatwia osobie, której dane dotyczą realizację jej praw, przedkładając posiadane przez siebie wzory wniosków, formularzy oraz materiałów informacyjnych.

9.6. Administrator informuje osobę o podjętych w związku ze złożonym wnioskiem lub żądaniem działaniach bezzwłocznie, nie później jednak niż w ciągu jednego miesiąca kalendarzowego.

9.7. W przypadku otrzymania żądania o skomplikowanym charakterze lub otrzymania dużej liczby żądań Administrator ma możliwość przedłużenia terminu o kolejne dwa miesiące, co wymaga pisemnego poinformowania osoby składającej wniosek lub przedstawiającej żądanie.

9.8. Jeżeli Administrator nie ma możliwości podjęcia działania w związku z żądaniem złożonym przez osobę fizyczną, najpóźniej w terminie jednego miesiąca od otrzymania żądania informuje ją o powodach niepodjęcia działania, o możliwości wniesienia skargi do organu nadzorczego oraz o możliwości skorzystania z innych środków ochrony prawnej przed sądem powszechnym. Również w ciągu jednego miesiąca od otrzymania żądania, Administrator informuje osobę o odmowie rozpatrzenia żądania i o prawach z tym związanych.

9.9. Realizacja uprawnień przysługujących osobie, której dane dotyczą jest wolna od opłat, chyba że żądania osoby są ewidentnie nieuzasadnione lub nadmierne (szczególnie ze względu na notoryczność). W takim wypadku Administrator może pobrać rozsądną opłatę lub odmówić podjęcia działań w związku ze złożonym żądaniem lub wnioskiem. Na Administratorze spoczywa obowiązek wykazania, że żądanie osoby miało ewidentnie nieuzasadniony lub nadmierny charakter.

10. Realizacja żądań i wniosków osób, których dane dotyczą (zasady szczegółowe)

10.1. Osobom fizycznym, których dane są przetwarzane w ramach działalności GOTREX KAROL KUBICKI, przysługują w związku z przetwarzaniem tych danych, pod warunkiem ziszczenia się w określonych sytuacjach przesłanek wymienionych w przepisach Rozporządzenia oraz innych przepisach powszechnie obowiązującego prawa, uprawnienia do:

10.1.1. uzyskania informacji na temat przetwarzania ich danych osobowych w momencie ich pozyskania (bezpośrednio od osoby, której dane dotyczą lub z innych źródeł);

10.1.2. dostępu do danych, w tym uzyskania informacji na temat przetwarzania danych (obowiązek informacyjny Administratora);

10.1.3. uzyskania kopii danych;

10.1.4. sprostowania danych;

10.1.5. usunięcia danych (tzw. prawo do bycia zapomnianym), w tym uzyskania informacji o usunięciu danych lub ich sprostowaniu;

10.1.6. ograniczenia przetwarzania;

10.1.7. przenoszenia danych;

10.1.8. sprzeciwu względem dalszego przetwarzania danych;

10.1.9. niepodlegania decyzji Administratora, która opierać by się miała wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, a która to decyzja wywoływałaby wobec danej osoby skutki prawne lub w podobny sposób istotnie na nią wpływała.

10.2. **Prawo do uzyskania informacji na temat przetwarzania ich danych osobowych w momencie ich pozyskania**

10.2.1. W momencie, w którym dochodzi do pierwszego utrwalenia informacji o osobie, której dane dotyczą, Administrator poprzez osoby upoważnione realizuje obowiązek informacyjny, o którym mowa w art. 13 Rozporządzenia, udzielając wszechstronnej informacji w formie pisemnej (tradycyjnej lub elektronicznej) osobom, których dane są przetwarzane (klauzule informacyjne);

10.2.2. Klauzula informacyjna obejmuje co najmniej informację o:

10.2.2.1. celu przetwarzania,

10.2.2.2. kategoriach danych osobowych,

10.2.2.3. odbiorcach lub kategoriach odbiorców danych,

10.2.2.4. planowanym okresie przechowywania danych osobowych, lub, gdy to niemożliwe, kryteriach ustalenia tego okresu,

10.2.2.5. prawie do żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych oraz do wniesienia sprzeciwu wobec takiego przetwarzania,

10.2.2.6. prawie wniesienia skargi do organu nadzorczego,

10.2.2.7. w przypadku, gdy dane nie zostały zebrane od osoby, której dotyczą - źródle danych,

10.2.2.8. zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu, istotnych informacjach o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą,

10.2.2.9. stosowanych zabezpieczeniach w przypadku przekazywania danych osobowych do państwa trzeciego

10.2.3. Wzór klauzuli informacyjnej (zbieranie danych od osoby, której dane dotyczą) stanowi załącznik nr 20 do Polityki.

10.2.4. W sytuacjach, gdy możliwe jest udokumentowanie realizacji obowiązku informacyjnego, Administrator może zrealizować go poprzez udzielenie informacji w formie audio lub audiowizualnej.

10.2.5. W przypadku gdy pracownicy Administratora pozyskują informacje dotyczące osoby z innych źródeł niż od osoby, której dane dotyczą, są zobowiązani do niezwłocznego przekazania tej osobie klauzuli informacyjnej, nie później niż w terminie 30 dni. Wzór klauzuli informacyjnej (pozyskiwanie danych z innych źródeł niż od osoby, której dane dotyczą) stanowi załącznik nr 21 do Polityki.

10.3. Prawo dostępu do danych

10.3.1. Administrator umożliwia osobom, których dane dotyczą uzyskanie dostępu do treści danych osobowych.

10.3.2. Administrator w następstwie złożonego zapytania udziela informacji osobie o tym czy jej dane są przetwarzane (w formie potwierdzenia lub zaprzeczenia).

10.3.3. Administrator realizuje obowiązek informacyjny, o którym mowa w art. 15 Rozporządzenia, udzielając wszechstronnej informacji osobom, których dane dotyczą, na każde przedstawione żądanie takiej osoby.

10.3.4. Administrator udziela przy tym informacji obejmującej informacje, o których mowa w ust. 10.2.2. powyżej.

10.3.5. Przykładowy wzór Udzielenia informacji o przetwarzaniu danych stanowi załącznik nr 4 do Polityki.

10.4. Prawo do uzyskania kopii danych

10.4.1. Dostęp do danych może być również zrealizowany poprzez wydanie nieodpłatnej kopii danych (dotyczy pierwszej kopii).

10.4.2. Administrator wydaje kopię przetwarzanych danych osobowych na wniosek osoby, której dane dotyczą.

10.4.3. Administrator udokumentowuje wydanie kopii danych (ewidencja udostępnień wydania kopii danych).

10.4.4. Prawo uzyskania kopii danych nie może wpływać niekorzystnie na prawa i wolności innych osób. Wymaga się aby kopia danych przekazana do udostępnienia była wolna od danych osób trzecich (np. poprzez anonimizację lub zaciemnienie kopii).

10.4.5. W przypadku realizacji każdego kolejnego wniosku o wydanie kopii danych Administrator uprawniony jest do pobrania opłaty w uzasadnionej wysokości, odpowiadającej kosztowi obsługi takiego żądania.

10.5. Prawo do sprostowania danych nieprawidłowych

10.5.1. Administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby, której dane dotyczą, kiedy osoba ta w sposób rozsądny wykaże nieprawidłowość danych, których sprostowania się domaga.

10.5.2. Na żądanie osoby, której dane dotyczą, Administrator informuje o sprostowaniu danych osobowych również ich odbiorców, tj. podmioty którym dane udostępnił lub powierzył do przetwarzania.

10.5.3. Administrator uzupełnia dane niekompletne oraz aktualizuje dane nieaktualne na wniosek osoby, której dane dotyczą.

10.5.4. Administrator uprawniony jest do odmowy realizacji żądania w sytuacji, gdy byłoby ono niezgodne z celami przetwarzania danych (np. stałoby w sprzeczności z zasadą minimalizacji, prowadziło do przetwarzania danych w nadmiernym zakresie, prowadziło do naruszenia praw osób trzecich).

10.6. Prawo do usunięcia danych

10.6.1. Administrator usuwa dane na żądanie osób, których dane dotyczą, w sytuacji gdy:

10.6.1.1. dane nie są niezbędne do realizacji celów przetwarzania;

10.6.1.2. osoba, której dane dotyczą cofnęła zgodę na przetwarzanie danych, zaś Administrator nie ma żadnej innej podstawy prawnej do przetwarzania danych (z podstaw wymienionych w par. 4 Polityki);

10.6.1.3. osoba, której dane dotyczą wniosła sprzeciw wobec czynności przetwarzania danych i sprzeciw ten jest skuteczny w świetle przepisów Rozporządzenia;

10.6.1.4. dane były przetwarzane niezgodnie z prawem;

10.6.1.5. konieczność usunięcia danych wynika z obowiązku prawnego;

10.6.1.6. żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. udział w konkursie na stronie internetowej, inne przypadki, w których dochodzi do świadczenia usług drogą elektroniczną).

10.6.2. Jeżeli dane podlegające usunięciu powierzone zostały procesorom do przetwarzania, Administrator podejmuje działania celem poinformowania tych procesorów o treści zgłoszonego przez daną osobę żądania.

10.6.3. Administrator odmawia realizacji żądania usunięcia danych osoby, której dane dotyczą w sytuacji gdy:

10.6.3.1. są one niezbędne do realizacji prawa do wolności wypowiedzi i informacji;

10.6.3.2. są one niezbędne do wywiązania się z obowiązku prawnego wynikającego z przepisów krajowych lub przepisów Unii Europejskiej;

10.6.3.3. są one niezbędne do ustalenia, dochodzenia lub obrony roszczeń.

10.7. Prawo do ograniczenia przetwarzania

10.7.1. Administrator dokonuje ograniczenia przetwarzania danych na żądanie osoby, której dane dotyczą w sytuacji, gdy:

10.7.1.1. osoba ta kwestionuje prawidłowość danych – na okres weryfikacji prawidłowości danych;

10.7.1.2. przetwarzanie danych jest niezgodne z prawem, jednak osoba, której dane dotyczą sprzeciwia się ich usunięciu, żądając w zamian ograniczenia ich przetwarzania;

10.7.1.3. dane są zbędne dla Administratora, jednak osoba, której dane dotyczą potrzebuje ich dla ustalenia, dochodzenia lub obrony roszczeń,

10.7.1.4. osoba, której dane dotyczą wniosła sprzeciw wobec czynności przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, że zachodzą prawnie uzasadnione podstawy wobec sprzeciwu tej osoby.

10.7.2. W przypadku realizacji żądania ograniczenia przetwarzania danych osoby, której dane dotyczą przez GOTREX KAROL KUBICKI, przez cały czas trwania ograniczenia przetwarzania, jedyną dopuszczalną formą przetwarzania przez GOTREX KAROL KUBICKI jest przechowywanie tych danych.

10.7.3. Dane względem, których przetwarzanie zostało ograniczone, mogą być przetwarzane w zakresie szerszym niż przechowywanie, jedynie:

10.7.3.1. w przypadku zgody osoby, której dane dotyczą;

10.7.3.2. w celu ustalenia, dochodzenia lub obrony roszczeń;

10.7.3.3. w celu ochrony praw innej osoby fizycznej lub prawnej;

10.7.3.4. z uwagi na ważne względy interesu publicznego UE lub państwa członkowskiego.

10.7.4. Zanim GOTREX KAROL KUBICKI podejmie decyzję o uchyleniu ograniczenia przetwarzania, informuje się o tym osobę, która zażądała ograniczenia przetwarzania.

10.7.5. GOTREX KAROL KUBICKI informuje każdego odbiorcę danych, któremu uprzednio przekazano dane, o wniesionym żądaniu ograniczenia przetwarzania danych. GOTREX KAROL KUBICKI informuje również osobę, której dane dotyczą o odbiorcach danych, o ile o to się zwróciła.

10.8. Prawo do przenoszenia danych

10.8.1. Na żądanie osoby, której dane dotyczą, Administrator wydaje w ustrukturyzowanym, powszechnie wykorzystywanym formacie (np. txt, xml) lub, o ile to jest technicznie możliwe, przekazuje innemu administratorowi dane dotyczące tej osoby, zgodnie z treścią jej żądania.

10.8.2. Realizacja prawa do przenoszenia danych jest możliwa jeżeli:

10.8.2.1. przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy oraz

10.8.2.2. przetwarzanie odbywa się w sposób zautomatyzowany.

10.9. Prawo do złożenia sprzeciwu wobec przetwarzania danych

10.9.1. Osoba której dane dotyczą ma prawo w dowolnym momencie wnieść sprzeciw - z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania dotyczących jej danych osobowych.

10.9.2. Od chwili wniesienia sprzeciwu GOTREX KAROL KUBICKI winna zaprzestać przetwarzania danych, chyba że sprzeciw nie jest skuteczny w świetle przepisów Rozporządzenia. W takiej sytuacji GOTREX KAROL KUBICKI musi wykazać istnienie ważnych, prawnie uzasadnionych podstaw do przetwarzania – nadrzędnych względem interesów, praw i wolności osoby, której dane dotyczą lub wykazanie podstaw do ustalenia, dochodzenia lub obrony roszczeń.

10.9.3. O ile dane osoby, której dane dotyczą są przetwarzane na potrzeby marketingu bezpośredniego, ma ona prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym również profilowania.

10.9.4. Jeżeli osoba, której dane dotyczą zgłasza sprzeciw wobec przetwarzania danych na potrzeby marketingu bezpośredniego, a Administrator taki marketing wobec tej osoby prowadził, Administrator bezzwłocznie uwzględnia takie żądanie oraz nie może powołać się na okoliczności, o których mowa w par. 10.9.3. powyżej.

10.10. Prawo do niepodlegania decyzji Administratora, która opierać by się miała wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu

10.10.1. Administrator zapewnia możliwość odwołania się do interwencji człowieka w sytuacji, gdy stosuje zautomatyzowane przetwarzanie danych, w szczególności polegające na profilowaniu osób oraz podejmowaniu względem niej decyzji wywołującej skutki prawne.

10.11. Instrukcja praw podmiotów, o których traktuje niniejszy paragraf, w tym instrukcja obsługi żądań osób, których dane dotyczą i procedury przekazywania tych żądań stanowi załącznik nr 2 do Polityki.

10.12. W celu udzielenia wszechstronnej informacji osobom, których dane przetwarza w ramach swojej działalności GOTREX KAROL KUBICKI tworzy się Ogólną Politykę Prywatności i Ochrony Danych Osobowych, stanowiącą załącznik nr 3 do Polityki, publikowaną na stronie internetowej www.gotrex.pl oraz udostępnianą osobom, których dane dotyczą na ich żądanie.

11. Wykaz budynków, pomieszczeń oraz obszarów, w których dochodzi do przetwarzania danych

11.1. Ustala się wykaz budynków, pomieszczeń lub części pomieszczeń, a także obszarów, w których przetwarzane są dane osobowe:

11.1.1. budynek GOTREX KAROL KUBICKI położony w Zarzeczu 120, 36-040 Boguchwała.

11.1.2. Budynek GOTREX KAROL KUBICKI położony przy ul. Kwiatkowskiego 9, 36-040 Boguchwała.

11.1.3. budynek GOTREX KAROL KUBICKI położony w Karlikowie 11, 38-505 Bukowsko.

11.2. Graficzny schemat budynku, pomieszczeń i części pomieszczeń oraz obszarów stanowi załącznik nr 5 do Polityki.

11.3. Dane osobowe mogą być przetwarzane wyłącznie w budynkach, pomieszczeniach lub ich częściach oraz obszarach ustalonych w wykazie.

11.4. Budynki i pomieszczenia, w których przetwarzane są dane osobowe są zamykane podczas nieobecności osób upoważnionych, tak by zabezpieczyć je przed wszelkimi osobami trzecimi. Ponadto stosowane są zabezpieczenia antywłamaniowe wraz z systemem alarmowym.

11.5. Przebywanie osób nieupoważnionych, w tym klientów GOTREX KAROL KUBICKI, w pomieszczeniach lub budynkach określonych w wykazie jest dopuszczalne wyłącznie w obecności Administratora lub osób upoważnionych.

11.6. W ramach lokalizacji nośników danych osobowych uwzględnia się wymagane aspekty bezpieczeństwa danych, w szczególności takie jak: źródła energii elektrycznej, klimatyzację oraz wentylację, potencjalne źródła pożaru lub powodzi, możliwość fizycznego dostępu.

11.7. Budynki i pomieszczenia, w których przetwarzane są dane wyposażone są w odpowiednie środki ochrony fizycznej i organizacyjnej chroniące przed nieautoryzowanym lub nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami pracy.

12. Czynności przetwarzania danych osobowych

12.1. Tworzy się Rejestr czynności przetwarzania danych osobowych przez Administratora danych, stanowiący załącznik nr 6 do Polityki.

12.2. Rejestr stanowi formę udokumentowania czynności przetwarzania danych, całościowo i w sposób kompletny identyfikuje wszystkie czynności przetwarzania danych osobowych w ramach działalności Administratora oraz jest podstawowym narzędziem realizacji zasady rozliczalności, umożliwiających wykazanie zgodności przyjętych przez Administratora praktyk oraz podejmowanych działań zgodnie z przepisami Rozporządzenia oraz innymi przepisami powszechnie obowiązującego prawa.

12.3. Rejestr zawiera:

12.3.1. imię i nazwisko lub nazwę oraz dane kontaktowe Administratora danych oraz Inspektora ochrony danych;

12.3.2. określenie czynności przetwarzania;

12.3.3. określenie jednostki organizacyjnej (komórki), w ramach której dochodzi do przetwarzania;

12.3.4. określenie celu przetwarzania;

12.3.5. opis kategorii osób, których dane osobowe dotyczą;

12.3.6. opis kategorii danych osobowych;

12.3.7. podstawę prawną przetwarzania;

12.3.8. źródło danych osobowych;

12.3.9. (gdy ma zastosowanie) nazwę oraz dane kontaktowe pozostałych współadministratorów;

12.3.10. (gdy ma zastosowanie) nazwę oraz dane kontaktowe podmiotów, którym Administrator powierza dane osobowe do przetwarzania;

12.3.11. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;

12.3.12. nazwę i opis systemu zastosowanego do przetwarzania danych osobowych;

12.3.13. ogólny opis technicznych oraz organizacyjnych środków bezpieczeństwa zastosowanych w celu ochrony danych;

12.3.14. wskazanie czy wykonano DPIA oraz jakie były jej wyniki;

12.3.15. (gdy ma to zastosowanie) przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej;

12.3.16. (jeżeli jest to możliwe) planowane terminy usunięcia poszczególnych kategorii danych;

12.3.17. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 Rozporządzenia.

12.4. W ramach Rejestru Administrator dokumentuje podstawę prawną dla każdej czynności przetwarzania. Administrator winien dbać o to, aby osoby upoważnione miały świadomość podstawy prawnej, w oparciu o którą dokonują przetwarzania danych osobowych.

12.5. Administrator uwzględnia rozwiązania służące ochronie danych przez pełny cykl przetwarzania danych, począwszy od planowania (projektowania) czynności przetwarzania, poprzez sam proces przetwarzania, skończywszy na zakończeniu przetwarzania.

12.6. Przepływ danych pomiędzy poszczególnymi systemami w ramach działalności Administratora może odbywać się wyłącznie poprzez wewnętrzną sieć informatyczną lub przy wykorzystaniu fizycznych nośników danych.

12.7. Ustala się bezpieczny system przepływu danych w zbiorach danych.

12.7.1. Materiały zawierające dane osobowe w formie papierowej przekazywane są przez osoby upoważnione „z ręki do ręki” i nie są pozostawiane bez nadzoru

osób upoważnionych w miejscach, gdzie dostęp do nich mogłyby mieć osoby nieuprawnione lub zagrożona byłaby ich integralność, poufność lub dostępność.

12.7.2. Materiały przesyłane drogą elektroniczną mogą zostać przesłane jedynie poprzez szyfrowane połączenie internetowe oraz za pomocą adresów mailowych w domenach gotrex.pl, na zabezpieczonym serwerze. Z administratorem odpowiadającym za dostarczenie, utrzymanie oraz bieżące serwisowanie serwera zawarto stosowną umowę o powierzenie przetwarzania danych osobowych, zgodną z wymogami określonymi w art. 28 Rozporządzenia oraz par. 33 Polityki.

12.8. Eksport danych do kraju spoza Europejskiego Obszaru Gospodarczego jest dozwolony wyłącznie, jeśli podmiot otrzymujący te dane w swoim kraju zapewnia adekwatny poziom ochrony do obowiązującego na terenie państw Europejskiego Obszaru Gospodarczego.

12.9. GOTREX KAROL KUBICKI unika przekazywania danych do podmiotów trzecich z siedzibą w państwach spoza Europejskiego Obszaru Gospodarczego, które nie są uznawane przez Komisję Europejską jako kraje „bezpieczne". Przekazanie danych do państw spoza Europejskiego Obszaru Gospodarczego podlega surowym regułom.

13. Środki techniczne, organizacyjne i systemowe służące bezpieczeństwu danych

13.1. Zastosowane zabezpieczenia (techniczne i organizacyjne) powinny być adekwatne do stwierdzonych zagrożeń mających wpływ na poziom ryzyka dla poszczególnych systemów, rodzajów zbiorów, kategorii i zakresu przetwarzanych danych osobowych.

13.2. Środki te mają zapewniać bezpieczeństwo procesom, w ramach których dochodzi do przetwarzania danych osobowych oraz umożliwiać zachowanie danym atrybutów poufności, integralności i rozliczalności.

13.3. Administrator stosuje następujące środki techniczne, organizacyjne i systemowe:

13.3.1. udzielenie dostępu do danych osobowych jedynie osobom posiadającym ważne upoważnienie nadane przez Administratora;

13.3.2. pisemne zobowiązanie osób upoważnionych do zachowania w tajemnicy przetwarzanych danych;

13.3.3. przechowywanie zbiorów danych osobowych w formie papierowej lub innej w meblach biurowych lub szafkach metalowych zamykanych na klucz;

13.3.4. zamykanie pomieszczeń biurowych, w których znajdują się nośniki danych osobowych, na klucz każdorazowo po zakończeniu pracy;

13.3.5. zabezpieczenie pomieszczeń, w których przechowywane są zbiory danych oraz dochodzi do czynności przetwarzania danych przed skutkami pożaru za pomocą systemu przeciwpożarowego lub wolnostojącej gaśnicy;

13.3.6. wdrożenie oraz stosowanie polityki kluczy, o której mowa w par. 22;

13.3.7. obowiązywanie zakazu udzielania osobom trzecim informacji dotyczących danych osobowych, za wyjątkiem spraw związanych z wykonywaniem obowiązków służbowych oraz prawnie uzasadnionych wniosków o udostępnienie danych, jednakże zawsze po rzetelnej weryfikacji osoby kierującej prośbę lub wniosek, zgodnie z zasadami opisanymi par. 9.4. Polityki;

13.3.8. obowiązywanie polityki „czystego biurka" i „czystego monitora", opisanych szczegółowo w Instrukcji zarządzania systemem informatycznym, stanowiącej załącznik nr 1 do Polityki;

13.3.9. niszczenie brudnopisów oraz zbędnych kopii materiałów zawierających dane osobowe w sposób uniemożliwiający odczytanie zawartej w nich treści tylko z wykorzystaniem niszczarek do papieru;

13.3.10. zakaz przebywania osób nieuprawnionych w obszarze przetwarzania danych bez jednoczesnej obecności osoby upoważnionej, a w przypadku pomieszczeń przechowujących elementy systemu informatycznego, sprecyzowane w Instrukcji zarządzania systemem informatycznym, stanowiącej załącznik nr 1 do Polityki - wyłącznie w obecności ASI;

13.3.11. zobowiązanie każdego użytkownika do blokowania dostępu do swojego systemu komputerowego po każdym opuszczeniu stanowiska pracy, chyba że system nie pozwala na dostęp do danych osobowych przetwarzanych w ramach działalności GOTREX KAROL KUBICKI;

13.3.12. zdalne monitorowanie sieci z jednej centralnej lokalizacji (serwer centralny);

13.3.13. ochrona systemów informatycznych służących do przetwarzania danych osobowych przed zagrożeniami pochodzącymi z sieci publicznej z wykorzystaniem zapory firewall lub innego równoważnego rozwiązania;

13.3.14. udostępnianie danych tylko zgodnie z przyjętą procedurą (par. 19 Polityki);

13.3.15. przyjmowanie interesantów podających dane osobowe (w formie ustnej lub papierowej) wyłącznie pojedynczo, w sposób zapewniający, że dane te nie zostaną w żaden sposób udostępnione osobom nieuprawnionym;

13.3.16. stosowanie zabezpieczeń systemu (w tym wygaszanie ekranu, konieczność uwierzytelnienia za pomocą hasła lub za pomocą tokena) w przypadku dłuższej nieaktywności użytkownika;

13.3.17. zabezpieczenie dostępu do systemu przetwarzającego dane klientów i kontrahentów za pomocą procesu zdublowanego uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła przy logowaniu do systemu operacyjnego oraz wykorzystywanej aplikacji roboczej (przy użyciu 8-znakowego hasła alfanumerycznego);

13.3.18. stosowanie mechanizmu blokady dostępu do systemu operacyjnego po 5 nieudanych próbach logowania;

13.3.19. w miarę możliwości, stosowanie systemu rejestracji dostępu do zbiorów danych lub czynności przetwarzania danych;

13.3.20. prowadzenie szkoleń w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz podstawowych zagrożeń związanych z przetwarzaniem danych osobowych dla osób upoważnionych do przetwarzania danych osobowych przed dopuszczeniem ich do czynności przetwarzania;

13.3.21. zapewnienie, aby każda osoba upoważniona została zapoznana z zasadami przetwarzania danych osobowych w ramach działalności Administratora, w tym z postanowieniami Polityki; w tym celu Administratorzy danych mogą korzystać z pomocy Inspektora ochrony danych;

13.3.22. wykorzystywanie systemów informatycznych wyłącznie dla celów służbowych, w precyzyjnie określonym zakresie wymaganym do realizacji czynności służbowych;

13.3.23. niszczenie w niszczarce wszelkich tymczasowych wydruków z danymi osobowymi niezwłocznie po ustaniu ich przydatności;

13.3.24. niszczenie wszelkich dokumentów zawierających dane osobowe, co do których brak aktualnej podstawy prawnej do przetwarzania, za pomocą niszczarki;

13.3.25. wyznaczenie w ramach działalności GOTREX KAROL KUBICKI Inspektora ochrony danych osobowych oraz Administratora systemów informatycznych;

13.3.26. stosowanie klauzul poufności w umowach z wszystkimi podmiotami zewnętrznymi mającymi dostęp do danych osobowych przetwarzanych przez Administratora, a w przypadku powierzenia przetwarzania danych – stosownych umów o powierzenie przetwarzania, zgodnie z treścią załącznika nr 15 do Polityki.;

13.3.27. stosowanie odpowiednio złożonych haseł dostępu do systemów, w których przetwarzane są dane;

13.3.28. stosowanie mechanizmów systemowych wymuszających okresową zmianę haseł;

13.3.29. wykonywanie kopii zapasowych danych i programów (kopia przechowywana na serwerze znajdującym się w zabezpieczonej serwerowni);

13.3.30. dokonywania archiwizacji danych w sposób zapewniający odpowiednie ich zabezpieczenie;

13.3.31. stosowanie reguł ostrożności przy otrzymywaniu wiadomości mailowych od nieznanych adresatów, w szczególności nieotwieranie załączników o nieznanej i budzącej podejrzenia treści oraz powiadamianie Administratora o wszelkich wątpliwościach;

13.3.32. zapewnienie, aby podczas transportu, przechowywania i użytkowania komputerów przenośnych i elektronicznych nośników informacji zawierających dane osobowe zagwarantowane były zabezpieczenia zapewniające poufność i integralność tych danych, np. dzięki wykorzystaniu środków ochrony kryptograficznej, oraz egzekwowanie odpowiedzialności za powierzony elektroniczny nośnik informacji wobec osób upoważnionych;

13.3.33. stosowanie zasad wykonywania okresowych przeglądów systemu informatycznego;

13.3.34. opracowanie i wdrożenie niniejszej Polityki;

13.3.35. opracowanie i wdrożenie Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, która stanowi załącznik nr 1 do Polityki;

13.3.36. zapewnienie odpowiedniego poziomu bezpieczeństwa nośników informacji zawierających dane osobowe w przypadku, gdy zachodzi konieczność naprawy sprzętu, w którym te nośniki są zamontowane lub stosowanie oprogramowania umożliwiającego trwałe usunięcie danych z urządzeń, dysków lub innych elektronicznych nośników informacji, które przeznaczone są do naprawy, przekazania lub likwidacji;

13.3.37. wprowadzenie zakazu testowania, naruszania zabezpieczeń, wprowadzania modyfikacji w oprogramowaniu stosowanym przez Administratora jak również zakaz podłączania zewnętrznych urządzeń bez zgody Administratora;

13.3.38. zastosowanie systemów ochrony ciągłości zasilania, zmniejszających ryzyko utraty danych oraz uszkodzenia urządzeń pamięci masowej (UPS-y lub generator prądu wraz z wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania);

13.3.39. zabezpieczenie pomieszczeń, w których przetwarzane i przechowywane są dane osobowe przed dostępem osób trzecich;

13.3.40. stosowanie najlepszych adekwatnych oraz możliwych do pozyskania przez Administratora zabezpieczeń, w tym zamków do drzwi, szafek zamykanych na klucz, sejfów;

13.3.41. stosowanie procedury rozpoczęcia, zawieszenia, zakończenia pracy przez użytkownika;

13.3.42. definiowanie praw dostępu do systemu informatycznego, w tym wprowadzenie mechanizmów autoryzacji użytkownika;

13.3.43. zakaz otwierania podejrzanych wiadomości mailowych pochodzących z nieznanych źródeł;

13.3.44. zapewnienie, aby osoba upoważniona do przetwarzania danych w systemie informatycznym posiadała w miarę możliwości swój własny i unikalny identyfikator, który umożliwia dostęp do danych osobowych zgodnie z treścią udzielonego upoważnienia;

13.3.45. wprowadzenie zakazu używania nośników elektronicznych (w tym płyt, dysków, pendrive'ów) niedopuszczonych do użytku przez Administratora danych;

13.3.46. dokonywanie wszelkich zmian, konfiguracji, serwisu oraz większych aktualizacji oprogramowania wyłącznie przez Administratora danych lub – za jego upoważnieniem - Administratora systemów informatycznych;

13.3.47. stosowanie zasad postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych opisanych w niniejszej Polityce.

13.4. Zastosowane zabezpieczenia (techniczne i organizacyjne) powinny być adekwatne do stwierdzonych zagrożeń mających wpływ na poziom ryzyka dla poszczególnych systemów, rodzajów zbiorów, kategorii i zakresu przetwarzanych danych osobowych. Administrator dokonuje oceny adekwatności zabezpieczeń we współpracy z IOD oraz ASI.

14. Analiza adekwatności przyjętych środków bezpieczeństwa

14.1. Administrator okresowo przeprowadza oraz dokumentuje analizę adekwatności stosowanych przez siebie środków ochrony danych osobowych.

14.2. Administrator stosuje oraz dokonuje na bieżąco przeglądów stosowanych środków ochrony danych, uwzględniając przydatność tych środków oraz koszt ich wdrożenia. Środki te uwzględniają w szczególności:

14.2.1. pseudonimizację danych, w postaci: stosowania numeru identyfikacyjnego oraz skróconej nazwy klienta w systemach informatycznych stosowanych przez Administratora;

14.2.2. szyfrowanie danych (w tym zarówno zidentyfikowanych zbiorów danych, jak również przesyłanych wiadomości zawierających dane);

14.2.3. inne dostępne środki zapewniające zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

14.2.4. narzędzia zapewniające ciągłość działania oraz szybkiego przywrócenia dostępności danych, w tym również dostępu do nich w sytuacji wystąpienia incydentu fizycznego lub technicznego w postaci UPS oraz systemów i narzędzi archiwizujących.

14.3. Środki ochrony danych osobowych stosowane przez Administratora są racjonalnie dobierane na podstawie przeprowadzonej analizy ryzyka i w sposób pozwalający na

maksymalne zminimalizowanie tego ryzyka, poprzez sprowadzenie do poziomu akceptowalnego.

14.4. Administrator stosuje adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa przetwarzania danych osobowych.

15. Zasada domyślnej ochrony danych osobowych (*privacy by default*)

15.1. Administrator wdraża środki techniczne i organizacyjne zapewniające, aby domyślnie przetwarzane były tylko te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

15.2. W tym celu Administrator dokonuje analizy w odniesieniu do:

15.2.1. ilości zbieranych danych osobowych,

15.2.2. zakresu przetwarzania,

15.2.3. okresu przetwarzania,

15.2.4. dostępności danych.

15.3. Narzędziem wspierającym wdrożenie domyślnej ochrony danych osobowych jest Rejestr.

15.4. Administrator nie może w ramach tworzonych przez siebie produktów czy usług, jak również przyjmowanych praktyk postępowania lub innych aktywności biznesowych, wprowadzać domyślnych ustawień ingerujących w prywatność osób, których dane dotyczą.

15.5. Ustawienia aplikacji czy systemów przetwarzających dane stosowanych przez GOTREX KAROL KUBICKI domyślnie udostępniają minimalną ilość informacji o użytkowniku. Rozszerzenie zakresu przetwarzanych danych może nastąpić jedynie na podstawie zmiany ustawień dokonanych przez samego użytkownika (osobę, której dane dotyczą).

16. Zasada ochrony danych osobowych w fazie projektowania (*privacy by design*)

16.1. Zasady ochrony danych osobowych w fazie projektowania dotyczą sytuacji tworzenia nowych zbiorów danych osobowych lub dokonywania nowych czynności przetwarzania w ramach działalności GOTREX KAROL KUBICKI.

16.2. Uprawnienie do podejmowania decyzji w sprawie tworzenia nowych zbiorów danych osobowych lub nowych czynności przetwarzania w ramach zbioru przysługuje wyłącznie Administratorowi.

16.3. Administrator może upoważnić użytkownika do utworzenia nowego zbioru danych lub czynności przetwarzania w ramach zbioru.

16.4. Każda decyzja o utworzeniu nowego procesu przetwarzania danych osobowych oraz doborze odpowiednich środków technicznych i organizacyjnych poprzedzona jest procesem analizy i oceny ryzyka, w ramach którego uwzględnia się:

16.4.1. stan wiedzy technicznej,

16.4.2. koszt wdrożenia,

16.4.3. charakter, zakres, kontekst i cele przetwarzania danych,

16.4.4. ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

16.5. Proces analizy oraz oceny ryzyka przeprowadzany jest przez Administratora. Administrator korzysta z pomocy IOD, a w przypadku procesów dotyczących danych przetwarzanych w systemach informatycznych – również z pomocy ASI. Podmioty te dokonują również weryfikacji czy w ramach nowej lub zaktualizowanej czynności przetwarzania danych nie jest konieczne przeprowadzenie DPIA.

16.6. W przypadku tworzenia nowych zbiorów danych osobowych lub dokonywania nowych czynności przetwarzania Administrator weryfikuje w szczególności:

16.6.1. czy zakres przetwarzanych danych jest zgodny z zasadą minimalizacji;

16.6.2. czy jest możliwe zastosowanie pseudonimizacji danych;

16.6.3. czy przetwarzanie danych jest transparentne z punktu widzenia osoby, której dane są przetwarzane;

16.6.4. czy jest możliwe udoskonalenie środków technicznych, organizacyjnych i systemowych służących przetwarzaniu danych osobowych.

16.7. Informację o utworzeniu nowej czynności przetwarzania uwzględnia się w Rejestrze, z zachowaniem wymogów wynikających z treści art. 30 ust. 1 Rozporządzenia.

16.8. W przypadku zaprzestania przetwarzania danych w ramach danej czynności przetwarzania, Administrator uwzględnia ten fakt w Rejestrze, usuwając czynność przetwarzania.

17. Naruszenie zasad przetwarzania danych osobowych

17.1. Wszelkie incydenty związane z naruszeniem zasad przetwarzania danych osobowych, w tym incydenty prowadzące do naruszenia ochrony danych osobowych, winny być wykrywane, rejestrowane i monitorowane w celu ich zidentyfikowania i zapobiegania ich ponownemu wystąpieniu.

17.2. Naruszenie ochrony danych osobowych

17.2.1. Za naruszenie ochrony danych osobowych uznaje się naruszenie bezpieczeństwa danych osobowych prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

17.2.2. Za naruszenie ochrony danych osobowych uznaje się w szczególności:

17.2.2.1. brak możliwości dostępu do danych osobowych z powodu naruszenia zabezpieczeń danych (np. zagubienie kluczy do pomieszczeń, w których przechowywane są nośniki danych, kradzież komputerów lub dysków, utrata haseł do plików zawierających dane osobowe);

17.2.2.2. nieautoryzowane usunięcie danych (np. przypadkowe lub umyślne zniszczenie dokumentów, wyczyszczenie pamięci dysku);

17.2.2.3. dostęp do danych przez osobę nieupoważnioną (np. dostęp do danych przez pracownika nieprzeszkolonego w zakresie znajomości przepisów dotyczących ochrony danych osobowych, nieposiadającego upoważnienia, zalogowanie się do systemu przetwarzającego dane przez osobę nieupoważnioną);

17.2.2.4. nieautoryzowane modyfikacje lub zniszczenie danych (np. modyfikacja plików z danymi w sposób uniemożliwiający ich powtórne otwarcie, przypadkowe zniszczenie materiałów drukowanych zawierających unikalne dane osobowe w sposób uniemożliwiający ich odczytanie);

17.2.2.5. udostępnienie danych nieupoważnionym podmiotom (przypadkowe lub umyślne wysłanie danych w wiadomości mailowej osobie nieupoważnionej, wydanie dokumentacji klienta osobie nieuprawnionej);

17.2.2.6. nielegalne ujawnienie danych (np. przypadkowe lub umyślne udostępnienie danych wykorzystywanych na cele marketingowe).

17.2.3. Naruszenie ochrony danych może być spowodowane w szczególności:

17.2.3.1. oddziaływaniem czynników zewnętrznych (takich jak np. temperatura otoczenia, wilgotność powietrza, występowanie pola elektromagnetycznego, działanie wirusów komputerowych oraz szkodliwego oprogramowania, występowanie klęsk żywiołowych);

17.2.3.2. działaniem osób trzecich (np. kradzież danych, zniszczenie danych);

17.2.3.3. umyślnym lub nieumyślnym działaniem osób upoważnionych oraz użytkowników (np. niezabezpieczenie nośników danych).

17.2.4. W przypadku naruszenia ochrony danych osobowych użytkownik obowiązany jest do bezzwłocznego poinformowania o tym fakcie Administratora oraz

Inspektora ochrony danych (a w przypadku gdy podejrzenie dotyczy naruszenia, do którego mogło dojść w ramach pracy systemu informatycznego – również Administratora systemów informatycznych).

17.3. **Uzasadnione podejrzenie naruszenia ochrony danych**

17.3.1. Niezależnie od obowiązku wskazanego w par. 17.2.4., Użytkownik jest obowiązany poinformować Administratora danych lub Inspektora ochrony danych (a w przypadku gdy podejrzenie dotyczy naruszenia, do którego mogło dojść w ramach pracy systemu informatycznego – również Administratora systemów informatycznych) również o każdym uzasadnionym podejrzeniu naruszenia ochrony danych osobowych.

17.3.2. Za uzasadnione podejrzenie naruszenia ochrony danych osobowych uznaje się w szczególności:

17.3.2.1. występowanie śladów na drzwiach, oknach i szafach, na sejfach, wskazujących na próbę włamania do pomieszczeń, w ramach których przechowywane są dane osobowe, w tym również, w których znajdują się systemy informatyczne przechowujące dane osobowe;

17.3.2.2. znajdowanie się w koszu na odpady dokumentów lub fragmentów dokumentów zawierających dane osobowe;

17.3.2.3. niezabezpieczony dostęp do pomieszczeń czy szaf, w których przechowywane są dane osobowe (np. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe);

17.3.2.4. niewylogowanie się przez użytkownika z systemu informatycznego przechowujących dane osobowe, pomimo opuszczenia stanowiska komputerowego;

17.3.2.5. pozostawienie nośników danych w drukarce, na ksero, na powierzchni biurek;

17.3.2.6. brak wykonania kopii zapasowej i/lub kopii bezpieczeństwa zgodnie z przyjętymi zasadami;

17.3.2.7. ustawienie monitorów pozwalające na wgląd osób nieupoważnionych w dane osobowe;

17.3.2.8. wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz obszaru przetwarzania bez zezwolenia Administratora i/lub bez udzielonego upoważnienia do przetwarzania danych;

17.3.2.9. uzasadnione podejrzenie próby ingerencji w dane osobowe przez podmiot nieupoważniony;

17.3.2.10. telefoniczne lub mailowe próby wyłudzenia danych osobowych;

17.3.2.11. zaobserwowanie obecności wirusa komputerowego lub szkodliwego oprogramowania na urządzeniach;

17.3.2.12. przechowywanie haseł w pobliżu stanowisk urządzeń elektronicznych.

17.3.3. Administrator danych, Inspektor ochrony danych lub Administrator systemów informatycznych weryfikuje otrzymane zgłoszenie, sprawdzając czy doszło do naruszenia ochrony danych osobowych oraz, w miarę potrzeby, podejmuje wszelkie działania zaradcze oraz weryfikuje:

17.3.3.1. stan wszystkich urządzeń i nośników, na których utrwalone są dane osobowe;

17.3.3.2. stan zabezpieczeń fizycznych i informatycznych służących do ochrony danych osobowych;

17.3.3.3. stan i prawidłowość działania programów wykorzystywanych do przetwarzania danych osobowych lub ich ochrony;

17.3.3.4. metody pracy osób upoważnionych do przetwarzania danych osobowych.

17.4. **Postępowanie w przypadku naruszenia ochrony danych**

17.4.1. Każda osoba upoważniona, a także każdy użytkownik, w przypadku stwierdzenia naruszenia ochrony danych osobowych są zobowiązane do niezwłocznego zawiadomienia o tym fakcie Administratora.

17.4.2. Użytkownik obowiązany jest do momentu podjęcia działań przez Administratora lub Inspektora ochrony danych przedsięwziąć niezbędne środki mające na celu zapobieżenie dalszemu naruszeniu ochrony danych osobowych oraz ich zabezpieczenia, w szczególności:

17.4.3.1. zabezpieczyć dostęp do pomieszczeń, urządzeń lub sieci, w ramach których przetwarzane są dane osobowe;

17.4.3.2. zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia, a także zidentyfikowanie osób winnych wystąpieniu naruszenia;

17.4.3.3. podjąć wszelkie czynności mające na celu uniemożliwienie dalszego naruszania ochrony danych.

17.4.3. Należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i prawidłowe udokumentowanie zdarzenia. Użytkownik, który stwierdził naruszenie ochrony danych osobowych obowiązany jest nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia, aż do momentu przybycia Administratora, Inspektora ochrony danych lub innej osoby upoważnionej przez Administratora.

17.4.4. Administrator:

17.4.4.1. podejmuje wszelkie niezbędne środki służące zaprzestaniu dalszemu naruszaniu ochrony danych osobowych;

17.4.4.2. zabezpiecza wszelkie urządzenia i dokumenty mogące pomóc w ustaleniu przyczyn naruszenia ochrony danych osobowych;

17.4.4.3. gromadzi informacje o zaistniałym naruszeniu od osoby powiadamiającej o naruszeniu, świadków naruszenia oraz wszelkich osób, które mogą posiadać istotne informacje związane z zaistniałym naruszeniem;

17.4.4.4. o ile jest to możliwe, odtwarza (np. w oparciu o utworzone kopie zapasowe) utracone lub zniszczone dane osobowe;

17.4.4.5. sporządza kopię zapisów rejestrów systemu informatycznego służącego do przetwarzania danych;

17.4.4.6. identyfikuje zaistniałe skutki naruszenia ochrony danych, sprawcę, miejsce, czas i okoliczności naruszenia;

17.4.4.7. dokonuje oszacowania szkód wynikłych z naruszenia ochrony danych osobowych;

17.4.4.8. sporządza szczegółową analizę w postaci pisemnego raportu zawierającego opis i przebieg zdarzenia, wskazanie prawdopodobnych przyczyn naruszenia ochrony danych osobowych, zgodnie z treścią 17.6., z zastrzeżeniem treści par. 17.4.7.;

17.4.4.9. szczegółowo bada aktualny stan ochrony danych oraz przyczyny wystąpienia naruszenia;

17.4.4.10. podejmuje wszelkie działania mające na celu uniemożliwienia lub zminimalizowanie możliwości ponownego zaistnienia naruszenia ochrony danych osobowych;

17.4.4.11. o ile istnieje taka potrzeba, korzysta z pomocy podmiotów zewnętrznych i/lub powołuje zespół mający na celu szczegółowe zbadanie okoliczności naruszenia ochrony danych.

17.4.5. W realizacji czynności, o których mowa w par. 17.4.4. powyżej Administrator może korzystać z pomocy Inspektora ochrony danych oraz Administratora systemów informatycznych.

17.4.6. Administrator systemów informatycznych obowiązany jest bezzwłocznie informować Administratora o wszelkich podejrzeniach naruszenia lub wysokiego ryzyka naruszenia ochrony danych osobowych występujących w ramach systemów informatycznych.

17.4.7. Za właściwe udokumentowanie naruszenia ochrony danych oraz podjęcie bez zbędnej zwłoki czynności mających na celu zaradzeniu występowania podobnych sytuacji w przyszłości odpowiada Inspektor ochrony danych we współpracy z Administratorem systemów informatycznych.

17.4.8. Ponowne uruchomienie urządzeń, systemów informatycznych, udzielenie dostępu do pomieszczeń, w których przetwarzane były dane osobowe możliwe jest za uprzednią zgodą wyrażoną przez Administratora.

17.5. Administrator prowadzi rejestr naruszeń bezpieczeństwa danych osobowych, stanowiący załącznik nr 7 do Polityki.

17.6. Raport z naruszenia ochrony danych

Inspektor ochrony danych dokumentuje zaistniały przypadek naruszenia ochrony danych osobowych sporządzając raport roboczy z incydentu naruszenia ochrony danych osobowych, którego wzór stanowi załącznik nr 8 do Polityki.

17.7. Konsekwencje dyscyplinarne

17.7.1. Użytkownik, który w przypadku naruszenia danych osobowych nie podjął działań określonych wskazanych w niniejszym rozdziale ponosi odpowiedzialność dyscyplinarną lub porządkową, bądź inną wynikającą z umowy.

17.7.2. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego paragrafu mogą zostać potraktowane jako ciężkie naruszenie obowiązków pracowniczych lub rażące naruszenie obowiązków umownych.

17.7.3. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej oraz cywilnej tej osoby na zasadach określonych w przepisach powszechnie obowiązującego prawa.

17.8. Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

17.8.1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki, w miarę możliwości, 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.

17.8.2. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

17.8.3. Wzór zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu stanowi załącznik nr 9 do Polityki.

17.8.4. Zgłoszenie, zawiera:

17.8.4.1. opis charakteru naruszenia ochrony danych osobowych, w tym kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

17.8.4.2. imię i nazwisko oraz dane kontaktowe Inspektora ochrony danych;

17.8.4.3. opis możliwych konsekwencji naruszenia ochrony danych osobowych;

17.8.4.4. opis środków zastosowanych lub proponowanych przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

17.8.5. Jeżeli informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

17.8.6. Administrator dokumentuje wszelkie przypadki naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze, zgodnie z paragrafami poprzedzającymi. Dokumentacja ta prowadzona jest w sposób pozwalający organowi nadzorczemu na weryfikację przestrzegania niniejszego artykułu (zasada rozliczalności).

17.9. Zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

17.9.1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

17.9.2. Administrator dokonuje każdorazowo skrupulatnej, opartej na obiektywnych kryteriach oceny naruszenia ochrony danych, badając czy prawa lub wolności osób fizycznych mogą zostać narażone na wysokie ryzyko naruszenia, w szczególności czy osobom fizycznym zagraża poważna szkoda lub krzywda. Ustalone w ten sposób ryzyko musi być wysokie, co oznacza, że musi być bardzo prawdopodobne, że efektem naruszenia ochrony danych osobowych stanie się naruszenie praw lub wolności osoby fizycznej, będącej podmiotem danych.

17.9.3. Za wysokie ryzyko naruszenia ochrony danych osobowych uważa się w szczególności:

17.9.3.1. utratę kontroli nad danymi osobowymi osoby fizycznej;

17.9.3.2. naruszenie dóbr osobistych osoby fizycznej, w tym prawa do prywatności oraz prawa do wizerunku;

17.9.3.3. naruszenie dobrego imienia oraz reputacji;

17.9.3.4. naruszenie poufności danych chronionych tajemnicą zawodową;

17.9.3.5. poniesienie strat finansowych przez osobę fizyczną;

17.9.3.6. dyskryminację;

17.9.3.7. nieuprawnione i nieautoryzowane odwrócenie pseudonimizacji;

17.9.3.8. kradzież lub sfałszowanie tożsamości;

17.9.3.9. inne szkody społeczne i gospodarcze.

17.9.4. Zawiadomienie, o którym mowa w ust. 1, powinno zostać sformułowane jasnym, prostym i zrozumiałym językiem oraz zawierać opis charakteru naruszenia ochrony danych osobowych.

17.9.5. Zawiadomienie nie jest wymagane w sytuacji, gdy:

17.9.5.1. Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

17.9.5.2. Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1 powyżej;

17.9.5.3. wymagałoby ono niewspółmiernie dużego wysiłku.

17.9.6. W przypadku wskazanym w par. 17.9.5. powyżej Administrator umieszcza stosowną informację na swojej stronie internetowej oraz w innych sposób gwarantujący skuteczne poinformowanie osób, których dane dotyczą.

17.9.7. Poglądowy Wzór zgłoszenia naruszenia ochrony danych osobowych osobie, której dane dotyczą stanowi załącznik nr 10 do Instrukcji.

18. Nadawanie upoważnień do przetwarzania danych

18.1. Administrator zarządza uprawnieniami użytkowników do przetwarzania danych osobowych w ramach wszelkich dokonywanych czynności przetwarzania,

udokumentowanych w Rejestrze, w ramach zbiorów danych tworzonych w formie papierowej lub elektronicznej.

18.2. Celem procedury jest zapewnienie, aby dostęp do czynności przetwarzania miały jedynie osoby upoważnione.

18.3. Przetwarzać dane osobowe może jedynie osoba posiadająca stosowne, prawidłowo udzielone upoważnienie.

18.4. Odpowiedzialnym za udzielanie upoważnień jest wyłącznie Administrator danych.

18.5. Upoważnienie udzielane jest na uzasadniony wniosek użytkownika, na wniosek Inspektora ochrony danych, kierownika odpowiedniej komórki organizacyjnej lub z inicjatywy własnej Administratora danych.

18.6. Zakres upoważnienia każdorazowo warunkowany jest zakresem obowiązków pracowniczych spoczywających na osobie upoważnionej oraz winien być maksymalnie ograniczony z uwzględnieniem naczelnych celów Polityki (zasada minimalizacji).

18.7. Przed uzyskaniem upoważnienia, osoba winna odbyć szkolenie organizowane przez Administratora i/lub osobę przez niego upoważnioną, w tym Inspektora ochrony danych, oraz złożyć podpis na oświadczeniu (zobowiązaniu do zachowania poufności) dołączonym do upoważnienia, którego wzór stanowi załącznik nr 11 do Polityki.

18.8. Należy zapewnić aby użytkownicy niebędący pracownikami GOTREX KAROL KUBICKI stosowali takie same zasady bezpieczeństwa przetwarzania danych oraz aby obowiązywały ich takie same reguły odpowiedzialności co użytkowników będących pracownikami.

18.9. Administrator przygotowuje dwa egzemplarze upoważnienia. Jeden egzemplarz otrzymuje osoba upoważniona, zaś drugi egzemplarz przekazywany jest do księgowości Administratora.

18.10. Upoważnienia przechowywane są w aktach osobowych pracownika i obowiązują do czasu ustania stosunku pracy lub obowiązków związanych z przetwarzaniem danych osobowych.

18.11. Administrator prowadzi ewidencję osób upoważnionych oraz odpowiada za jej utrzymanie zgodnie z aktualnym stanem faktycznym. Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych stanowi załącznik nr 12 do Polityki.

18.12. Administrator może w każdej chwili cofnąć udzielone upoważnienie z własnej inicjatywy lub na wniosek Inspektora ochrony danych i/lub osoby upoważnionej. Cofnięcie upoważnienia odnotowuje się na dokumencie upoważnienia.

18.13. Cofnięcie upoważnienia do przetwarzania danych osobowych nie wymaga uzasadnienia.

18.14. Administrator prowadzi w ramach ewidencji osób upoważnionych ewidencję anulowanych upoważnień do przetwarzania danych oraz odpowiada za jej utrzymanie zgodnie z aktualnym stanem faktycznym. Ewidencja upoważnień anulowanych może być prowadzona wraz z ewidencją upoważnień – w ramach jednego dokumentu.

19. Udostępnienie danych osobowych

19.1. Udostępnienie danych osobowych możliwe jest jedynie w ściśle określonych sytuacjach, wyłącznie podmiotom uprawnionym do ich otrzymania na podstawie przepisu prawa lub osobom, których te dane dotyczą, w przypadku, gdy:

19.1.1. wyraża na to zgodę osoba, której dane dotyczą;

19.1.2. udostępnienie jest niezbędne do realizacji obowiązku wynikającego z przepisów powszechnie obowiązującego prawa (przy czym obowiązek wskazania tej podstawy spoczywa na podmiocie, który wnioskuje o udostępnienie danych);

19.1.3. udostępnienie danych niezbędne jest dla celów zawarcia lub realizacji umowy, w przypadku gdy osoba, której dane dotyczą jest jej stroną;

19.1.4. udostępnienie niezbędne jest dla zrealizowania określonych prawem zadań realizowanych dla dobra publicznego (po wskazaniu podstawy prawnej przez administratora, który wnioskuje o udostępnienie danych);

19.1.5. udostępnienie jest wymagane dla wypełnienia prawnie uzasadnionych celów realizowanych przez Administratora danych lub odbiorców i jednocześnie przetwarzanie to nie narusza, ani nie stwarza ryzyka naruszenia praw i wolności osób, których dane dotyczą.

19.2. Wniosek o udostępnienie danych osobowych podlega przekazaniu do Inspektora ochrony danych przez pracownika GOTREX KAROL KUBICKI, do którego go złożono.

19.3. Pracownik GOTREX KAROL KUBICKI, do którego złożono wniosek o udostępnienie danych, zwraca się z zapytaniem o możliwość udostępnienia do Inspektora ochrony danych. Inspektor ochrony danych podejmuje decyzję o zgodzie lub braku zgody na udostępnienie danych osobowych, z zastrzeżeniem że udostępnieniu nie sprzeciwia się Administrator.

19.4. Wzór wniosku o udostępnienie danych osobowych stanowi załącznik nr 13 do Polityki.

19.5. Udostępniając dane Administrator informuje jednocześnie, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

19.6. Dokumenty lub inne nośniki zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom wyłącznie za potwierdzeniem odbioru listem poleconym za pokwitowaniem odbioru lub innym bezpiecznym sposobem, z wyłączeniem ingerencji osób lub podmiotów trzecich.

19.7. Udostępnienie danych podlega udokumentowaniu. Wzór ewidencji udostępnień danych osobowych stanowi załącznik nr 14 do Polityki.

19.8. Ewidencja udostępnień danych zawiera informację o:

19.8.1. dacie i godzinie udostępnienia;

19.8.2. osobie, która dokonała faktycznej czynności udostępnienia danych osobowych;

19.8.3. osobie lub podmiocie, któremu dane zostały udostępnione;

19.8.4. zakresie danych, które zostały udostępnione (rodzaju danych);

19.8.5. przesłance udostępnienia danych osobowych (spośród wymienionych w ust. 1 powyżej);

19.8.6. uzasadnieniu udostępnienia danych, tj. zastosowania przesłanki, o której mowa w pkt. 19.6.5 powyżej;

19.8.7. ewentualnych uwagach dodatkowych lub komentarzu.

20. Powierzenie przetwarzania danych osobowych

20.1. Powierzenie przetwarzania danych osobowych podmiotom przetwarzającym następuje w oparciu o pisemną umowę o powierzenie przetwarzania danych osobowych. Wzór umowy powierzenia przetwarzania danych osobowych stanowi załącznik nr 15 do Polityki.

20.2. Za przygotowanie szczegółowej treści umowy powierzenia przetwarzania danych, w tym za odpowiednie dostosowanie treści wzoru, o którym mowa w ust. 1 powyżej, odpowiedzialny jest kierownik komórki organizacyjnej GOTREX KAROL KUBICKI, w ramach działalności której dochodzi do powierzenia przetwarzania danych osobowych, działający we współpracy z osobą odpowiedzialną za obsługę prawną GOTREX KAROL KUBICKI oraz Inspektorem ochrony danych.

20.3. Osoby zaangażowane w proces zawierania umowy z podmiotem przetwarzającym, w szczególności kierownik komórki organizacyjnej, w ramach działalności której dochodzi do powierzenia przetwarzania danych, obowiązane są do rzetelnego zweryfikowania czy daje on rękojmię wdrożenia właściwych środków o charakterze technicznym i organizacyjnym, aby przetwarzanie spełniało wymogi powszechnie obowiązującego prawa i chroniło prawa osób, których dane dotyczą.

20.4. Osoby zaangażowane w proces zawierania umowy z podmiotem przetwarzającym, w szczególności kierownik komórki organizacyjnej, w ramach działalności, której dochodzi do powierzenia przetwarzania danych, weryfikują również czy zakres powierzonych danych, jak również sposób przekazania danych zgodny jest z zasadami przetwarzania danych określonych w rozdziale 3.

20.5. Podmiot przetwarzający obowiązany jest przetwarzać powierzone sobie dane jedynie w zakresie oraz dla realizacji celów wskazanych w pisemnej umowie o powierzenie przetwarzania danych.

20.6. Powierzenie przetwarzania danych nie zwalnia Administratora z odpowiedzialności za zgodne z prawem ich przetwarzanie, co wymaga respektowania przez podmioty przetwarzające prawa Administratora do kontroli wykonania przedmiotu umowy o powierzenie przetwarzania danych, w tym również w siedzibie podmiotu przetwarzającego, m. in. w zakresie zgodności z treścią Polityki, innych obowiązujących regulacji wewnętrznych, umów i przepisów powszechnie obowiązującego prawa.

20.7. W sytuacji, gdy powierzenie przetwarzania danych osobowych dotyczyć ma danych przetwarzanych w formie elektronicznej, lub powierzenie związane byłoby z obsługą teleinformatyczną – pracownik GOTREX KAROL KUBICKI zaangażowany w proces powierzenia przetwarzania danych osobowych konsultuje zasadność zawarcia umowy powierzenia z ASI.

20.8. Wzór ewidencji podmiotów, którym powierzono przetwarzanie danych osobowych stanowi załącznik nr 16 do Polityki.

20.9. Jeżeli Administrator danych występuje w roli procesora, tj. powierzono mu dane do przetwarzania, obowiązany jest do prowadzenia rejestru wszystkich kategorii przetwarzania danych, zgodnie z treścią art. 28 ust. 2 Rozporządzenia. Wzór rejestru kategorii czynności przetwarzania stanowi załącznik nr 17 do Polityki.

21. Stosowanie podejścia opartego o analizę ryzyka

21.1. Administrator zapewnia stopień bezpieczeństwa odpowiadający poziomowi ryzyka, w tym również ryzyka naruszenia praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych.

21.2. Administrator prowadzi cykliczną analizę ryzyka przetwarzania danych osobowych w odniesieniu do poszczególnych źródeł ryzyka.

21.3. Analiza ta prowadzona jest zwłaszcza w sytuacjach, gdy:

21.3.1. doszło do naruszenia ochrony danych osobowych;

21.3.2. Administrator powierza dane osobowe do przetwarzania procesorowi;

21.3.3. Administrator postanowił utworzyć nowy zbiór danych osobowych;

21.3.4. Administrator decyduje o wprowadzenia nowego rodzaju środków technicznych i organizacyjnych mających na celu zabezpieczenie danych.

21.4. Zarządzanie ryzykiem odbywa się poprzez:

21.4.1. identyfikację zagrożonych aktywów/ zbiorów danych;

21.4.2. identyfikację źródeł ryzyka;

21.4.3. identyfikację zagrożeń;

21.4.4. określenie oczekiwanego wyniku materializacji ryzyka;

21.4.5. określenie czynników i stosowanych obecnie środków zapobiegających;

21.4.6. ocena ryzyka (wpływ i prawdopodobieństwo);

21.4.7. podjęcie decyzji co do przeprowadzenia oceny skutków dla ochrony danych osobowych (Data Protection Impact Assessment – DPIA);

21.4.8. podjęcie decyzji co do ryzyka (akceptacja, unikanie, redukcja, przeniesienie);

21.4.9. sformułowania sugestii co do działań zaradczych;

21.4.10. dokonanie oceny ryzyka (prawdopodobieństwa) po podjęciu działań zaradczych.

21.5. Narzędziem umożliwiającym dokumentowanie procesu identyfikacji ryzyka, zagrożeń, ich ocenę oraz przedstawienie sugestii zabezpieczeń może być Arkusz zarządzania ryzykiem stanowiący załącznik nr 18 do Polityki.

21.6. Administrator dokonuje oceny skutków planowanych operacji przetwarzania danych (DPIA), w sytuacji gdy wstępna analiza ryzyka wskazuje na wysokie ryzyko naruszenia praw i wolności osób fizycznych oraz w sytuacjach wymaganych przepisami prawa. Administrator może w tym celu korzystać z narzędzi i systemów odpowiednich dla przeprowadzenia DPIA, o ile zapewniają one realizację celów wskazanych w Rozporządzeniu.

22. Polityka kluczy

22.1. Wprowadza się politykę kluczy normującą następujące zasady postępowania:

22.1.1. polityka kluczy obejmuje pomieszczenia, w ramach których przechowywane są nośniki danych osobowych;

22.1.2. klucze do pomieszczeń przechowywane są w pomieszczeniu pracownika upoważnionego do wydawania kluczy;

22.1.3. klucze zapasowe do pomieszczeń przechowywane są w pomieszczeniu administratora obiektu;

22.1.4. zabrania się otwierania drzwi oraz wydawania kluczy osobom nieupoważnionym do pobierania kluczy;

22.1.5. uprawnienie do pobrania kluczy uzyskuje się poprzez podpisanie oświadczenia o poufności oraz potwierdzenia odbioru upoważnienia do przetwarzania danych osobowych w zakresie, który wymaga dostępu do pomieszczeń, zamkniętych na klucz;

22.2. Zasady pobierania i zdawania kluczy

22.2.1. klucze do pomieszczeń wydawane są indywidualnie przez pracownika upoważnionego do wydawania kluczy;

22.2.2. osoba upoważniona do wydawania kluczy odnotowuje pobranie oraz zdanie kluczy w księdze pobrań;

22.2.3. klucze zapasowe do pomieszczeń wydawane są indywidualnie przez administratora obiektu;

22.2.4. osoba upoważniona do wydawania kluczy zapasowych odnotowuje pobranie oraz zdanie kluczy w księdze pobrań;

22.2.5. wydawanie kluczy zapasowych osobom upoważnionym może odbywać się tylko w uzasadnionych, wyjątkowych okolicznościach, z odpowiednią adnotacją i wyjaśnieniem w księdze pobrań;

22.2.6. osoba upoważniona obowiązana jest każdorazowo zwrócić klucze, w tym również klucze zapasowe, do administratora obiektu.

22.3. Zasady postępowania w czasie pracy:

22.3.1. klucze zabezpieczające pomieszczenia, szafy czy sejfy muszą być jednoznacznie opisane;

22.3.2. w godzinach pracy klucze znajdują się pod bezpośrednim nadzorem osób upoważnionych;

22.3.3. osoby upoważnione do wydawania kluczy ponoszą odpowiedzialność za ich należyte zabezpieczenie;

22.3.4. zabronione jest pozostawianie kluczy w drzwiach lub zamkach, zarówno w godzinach pracy, jak i po godzinach;

22.3.5. po zakończonej pracy klucze mogą być przechowywane jedynie w wyznaczonym do tego pomieszczeniu, tj. recepcji;

22.4. Administrator danych odpowiedzialny jest za nadzór nad przestrzeganiem polityki kluczy oraz jej bieżącą aktualizację z uwzględnieniem aktualnych potrzeb.

23. Kontrola stosowania zasad ochrony danych osobowych oraz stanu ich zabezpieczeń

23.1. Administrator danych przy pomocy Inspektora ochrony danych i/lub osób przez siebie upoważnionych dokonuje okresowej kontroli stopnia bezpieczeństwa przetwarzanych danych.

23.2. Kontrola powinna być przeprowadzona przynajmniej raz w roku. Kontrola może być prowadzona również doraźnie, zwłaszcza w przypadku wystąpienia naruszenia ochrony danych osobowych.

23.3. Z czynności kontrolnych sporządzany jest raport. Raport dokumentuje szczegółowy zakres kontroli oraz przedstawia zalecenia pokontrolne.

23.4. Raport podpisany zostaje przez osoby wykonujące czynności kontrolne oraz przez kierowników komórek organizacyjnych.

23.5. Administrator danych wraz z osobami przez siebie upoważnionymi i/lub Inspektorem ochrony danych uprawnieni są do wykonywania czynności sprawdzających w zakresie rzetelności wykonywanej kontroli, jak również wdrożenia zaleceń pokontrolnych.

24. Postanowienia końcowe

24.1. Polityka została przyjęta przez Karola Kubickiego prowadzącego działalność pod firmą GOTREX KAROL KUBICKI w drodze rozporządzenia nr 1 z dnia 02.01.2021 r. oraz wchodzi w życie z dniem 02.01.2021 r.

24.2. Polityka zastępuje w całości postanowienia Polityki bezpieczeństwa danych osobowych w GOTREX KAROL KUBICKI.

24.3. Polityka jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie, za wyjątkiem uzasadnionego żądania podmiotów sprawujących funkcje publiczne, w tym upoważnionych pracowników Urzędu Ochrony Danych Osobowych.

24.4. Wszelkie postanowienia Polityki wiążą Administratora, wszystkich pracowników Administratora, osoby współpracujące z Administratorem w oparciu o jakikolwiek stosunek prawny, a także wszelkie inne osoby upoważnione.

24.5. Każdy nowy pracownik obowiązany jest do zapoznania się z treścią Polityki oraz jej załączników. Kierownicy komórek organizacyjnych GOTREX KAROL KUBICKI winni zadbać o umożliwienie pracownikowi zapoznania się z treścią Polityki, jak również wglądu do jej treści.

24.6. Zmiana Polityki dokonywana jest wyłącznie w formie pisemnej, w trybie ustalonym przez Administratora, przy czym o wszelkich jej zmianach niezwłocznie informuje się osoby obowiązane do stosowania jej postanowień.

24.7. Naruszenie postanowień Polityki może być uznane przez Administratora w stosunku do pracowników – za ciężkie naruszenie obowiązków pracowniczych, a w przypadku współpracowników - za rażące naruszenie zobowiązań współpracownika wynikających ze stosunku prawnego wiążącego go z Administratorem.

24.8. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy Rozporządzenia oraz Ustawy. Administrator wdraża rozwiązania prawne, do których implementacji zobowiązany jest przez przepisy prawa, niezależnie od tego czy znajdują się one w Polityce.

24.9. Żaden z punktów Polityki nie może być interpretowany, jako stojący w sprzeczności z przepisami Rozporządzenia lub Ustawy. W sytuacji jakichkolwiek wątpliwości należy interpretować treść Polityki w sposób zapewniający jej całkowitą zgodność z przepisami Rozporządzenia i Ustawy.