POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH W FIRMIE: BIURO RACHUNKOWE VECTIGAL CONSULTING EWA DĄBROWSKA

HISTORIA WPROWADZANYCH ZMIAN:

Nr wydania	Charakter wprowadzonej zmiany	Podstawa wprowadzenia zmiany
1	wprowadzenie	

	Opracował	Uzgodnił	Zatwierdził
Podpisy			

CZĘŚĆ I.
PODSTAWOWE INFORMACJE

I. Podstawa prawna

Podstawę prawną niniejszego dokumentu stanowią:

1. 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), Dz.Urz. UE L 119/1 z 04.05.2016 roku [RODO],
2. Ustawa z … o ochronie danych osobowych (obecnie w fazie prac sejmowych) [ODO].

Celem dokumentu jest:

1. Wprowadzenie systemu ochrony danych osobowych,
2. Inicjowanie działań podnoszących efektywność i sprawność w zakresie ochrony danych osobowych w firmie,
3. Wskazanie działań, jakie należy wykonać oraz jakie ustanowić zasady i reguły postępowania, aby Administrator danych oraz jego pracownicy i współpracownicy mogli właściwie wykonywać zadania w zakresie ochrony danych osobowych.

II. Zakres zastosowania

1. Dokument dotyczy pracowników i współpracowników firmy … przetwarzających dane osobowe, a także każdej osoby mającej dostęp do tychże danych osobowych.
2. Dokument może obejmować również firmy, które zawrą umowę z firmą … na podstawie, której powierzone zostaną im dane osobowe do przetwarzania.
3. Procedurę stosują wszystkie osoby, które mają dostęp do danych osobowych w firmie.
4. Z Procedurą niniejszą należy zapoznać wszystkich pracowników oraz współpracowników mających dostęp do danych osobowych.

III. Podstawowe definicje

Poniżej zamieszczone są podstawowe definicje z zakresu ochrony danych osobowych. Są to pojęcia kluczowe do codziennej pracy z danymi osobowymi. Instytucje incydentalne zostaną wyjaśnione w dalszych częściach niniejszej Procedury.

Administrator danych	Zarząd spółki przetwarzającej dane osobowe oraz decydującej o sposobach i celach ich przetwarzania. W imieniu zarządu prawa i obowiązki administratora danych osobowych może wykonywać wskazany członek zarządu albo pełnomocnik zarządu. Administrator danych osobowych może powołać Inspektora Ochrony Danych Osobowych.
Dane osobowe	oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane

	dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej
Przetwarzanie	oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie
Pseudonimizacja	oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej
Zbiór danych	oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie
Zgoda	osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych

IV. Obowiązki Administratora danych oraz schematy postępowania

1. Wykaz obowiązków Administratora danych

W świetle RODO przetwarzanie danych osobowych jest możliwe, gdy spełnione zostaną łącznie następujące warunki:

1. Administrator danych uwzględnia zadania z zakresu ochrony danych już w fazie planowania wdrożenia nowej usługi – **zob. rozdział V**,
2. Do przetwarzania danych osobowych dopuszczone są wyłącznie osoby, które posiadają stosowne upoważnienie – **zob. rozdział VI**,
3. Dane osobowe są przetwarzane zgodnie z prawem – istnieje przepis prawa zezwalający Administratorowi danych na ich przetwarzanie – **zob. rozdziały VII-VIII**,
4. Administrator danych wykonuje obowiązek informacyjny względem osoby, której dane przetwarza – **zob. rozdział IX**,
5. Dane osobowe powinny być przetwarzane jedynie w zakresie niezbędnym do realizacji celu, dla którego zostały zebrane oraz w czasie koniecznym do jego

realizacji. Nie należy zbierać dodatkowych danych osobowych niż jest to konieczne – **zob. rozdział VII**,

6. W przypadku zmiany celu przetwarzania należy postąpić analogicznie, jak przy pierwotnym zebraniu danych osobowych – tj. Administrator danych musi posiadać prawną podstawę ich przetwarzania, a o zmianie celu należy powiadomić osobę, której dane dotyczą (o ile uprzednio już tego nie uczyniono) – **zob. rozdział VII**,
7. Administrator danych ma obowiązek respektować prawa osób, których dane osobowe przetwarza – **zob. rozdział X**, w tym pracowników i współpracowników – **zob. rozdział XV**,
8. Administrator danych zobowiązany jest zapewnić bezpieczeństwo przetwarzanych danych osobowych – **zob. rozdział XIII**,
9. Administrator danych prowadzi rejestr czynności przetwarzania danych – **zob. rozdział XII**.
10. W przypadku powierzenia przetwarzania danych osobowych osobom trzecim, Administrator danych zapewnia zgodność powierzenia z prawem, w tym odpowiednią konstrukcję umowy powierzenia – **zob. rozdział XI**.
11. W przypadku wykrycia naruszenia zasad przetwarzania danych osobowych Administrator danych zobowiązany jest do podjęcia odpowiednich działań - **zob. rozdział XIV**.

2. Podstawowe schematy postępowania przez Administratora danych

Schemat postępowania Administratora danych – zbieranie danych osobowych

1. Uzyskanie zgody osoby, której dane są gromadzone na ich przetwarzanie – zgoda może być zawarta w treści umowy, odrębnym oświadczeniu, w opcji wyboru formularza na stronie internetowej **(zob. rozdział VIII)**,
2. Weryfikacja, czy wszystkie dane osobowe są niezbędne do realizacji celów Administratora danych, gdy zgromadzono dane zbędne, należy je usunąć **(zob. rozdział VII)**,
3. Wykonanie obowiązku informacyjnego względem tej osoby – wymagane informacje mogą być zawarte w treści umowy, w odrębnym dokumencie, w mailu, na stronie internetowej **(zob. rozdział IX)**,
4. Przetwarzanie danych zgodnie z opisanymi w tym dokumencie zasadami,
5. W przypadku, gdy dane osobowe stały się zbędne dla realizacji celu, dla którego je zebrano (np. umowa została wykonana i rozliczona), należy je usunąć albo poddać pseudonimizacji.

Schemat postępowania Administratora danych – dane osobowe gromadzone pośrednio

1. Weryfikacja istnienia przesłanki legalizującej przetwarzanie danych osobowych (np. w celu wykonania umowy, w celu marketingu bezpośredniego) **(zob. rozdział VII)**,
2. Weryfikacja, czy wszystkie dane osobowe są niezbędne do realizacji celów Administratora danych, gdy zgromadzono dane zbędne, należy je usunąć **(zob. rozdział VIII)**,
3. Wykonanie rozszerzonego obowiązku informacyjnego względem osoby, której dane zostały pozyskane **(zob. rozdział IX)**,
4. Przetwarzanie danych zgodnie z opisanymi w tym dokumencie zasadami,
5. W przypadku, gdy dane osobowe stały się zbędne dla realizacji celu, dla którego je

zebrano, albo osoba ta wniosła uzasadnione żądanie ich usunięcia, należy je usunąć albo poddać pseudonimizacji.

Schemat postępowania Administratora danych – dostęp do danych osobowych

1. Zaprojektowanie ochrony danych osobowych **(zob. rozdział V),**
2. Wdrożenie fizycznych i logicznych zabezpieczeń procesu przetwarzania danych osobowych **(zob. rozdział XIII)**,
3. Zapoznanie pracowników i współpracowników mających uczestniczyć w przetwarzaniu danych osobowych z niniejszą Procedurą,
4. Nadanie pracownikom i współpracownikom upoważnień do przetwarzania danych osobowych **(zob. rozdział VI)**,
5. Zawarcie umów powierzenia przetwarzania danych osobowych z innymi podmiotami współpracującymi **(zob. rozdział XI)**,
6. Przetwarzanie danych zgodnie z opisanymi w tym dokumencie zasadami.

Schemat wdrożenia i weryfikacji środków bezpieczeństwa danych osobowych

1. Opracowanie schematów przepływu danych osobowych w firmie (jak są zbierane, gdzie są zapisywane, komu i w jaki sposób są przesyłane wewnątrz firmy, komu spoza firmy i w jaki sposób są przekazywane, itd.),
2. Analiza schematów pod kątem możliwości dostępu do danych osobowych osób nieuprawnionych (wycieku danych),
3. Dobór środków eliminujących albo zmniejszających ryzyko wskazane w punkcie 2 (**zob. rozdział XIII**),
4. Wdrożenie wybranych środków bezpieczeństwa,
5. Nadanie upoważnień osobom mającym przetwarzać dane osobowe (**zob. rozdział V**I),
6. Utworzenie rejestru czynności przetwarzania (**zob. rozdział XII**),
7. Okresowa analiza skuteczności zastosowanych środków bezpieczeństwa, w terminach określonych przez Administratora danych,
8. W przypadku wykrycia naruszenia zasad przetwarzania danych osobowych podjęcie działań wskazanych w **rozdziale XIV** oraz weryfikacja środków bezpieczeństwa pod kątem ich zmiany lub uzupełnienia.

Schemat postępowania na wypadek wykrycia naruszenia bezpieczeństwa danych osobowych

1. Weryfikacja zabezpieczeń danych osobowych pod kątem wykrycia ich naruszenia,
2. Podjęcie działań mających na celu zapewnienie prawidłowego funkcjonowania środków zapewniających bezpieczeństwo danych osobowych,
3. W przypadku zniszczenia albo uszkodzenia dokumentów lub plików zawierających dane osobowe – odtworzenie ich w oparciu o kopie zapasowe oraz inne posiadane materiały,
4. W przypadku naruszenia zabezpieczeń: odtworzenie zabezpieczeń lub wprowadzenie zabezpieczeń dodatkowych. Do czasu przywrócenia pełnej funkcjonalności dotychczasowych zabezpieczeń należy wprowadzić zabezpieczenia tymczasowe, które gwarantować będą niezbędny stopień bezpieczeństwa danych

osobowych **(zob, rozdział XIII)**,
5. Weryfikacja zakresu naruszenia,
6. Ustalenie osób odpowiedzialnych za zaistniałe naruszenie,
7. Zgłoszenie naruszenia właściwym organom, a także osobom, których dane osobowe zostały naruszone **(zob. rozdział XIV)**,
8. Jeżeli okaże się to konieczne, uzupełnienie procedury celem przeciwdziałania podobnym zdarzeniom w przyszłości.

Sposób wypełnienia wyżej wskazanych wymogów warunkujących zgodne z prawem przetwarzanie danych osobowych zostanie przedstawiony w dalszych częściach niniejszej Procedury.

Procedura przekazywanie danych osobowych klientów do banku została uregulowana w odrębnym dokumencie pn. Opis rozwiązań technicznych i organizacyjnych, zapewniających bezpieczne i prawidłowe wykonywanie przez przedsiębiorcę powierzonych czynności, w szczególności ochronę tajemnicy prawnie chronionej.

CZĘŚĆ II.

INFORMACJE SZCZEGÓŁOWE

V. Projektowanie ochrony danych osobowych

Administrator danych ma ogólny obowiązek uwzględniania zasad ochrony danych osobowych w procesie projektowania i wdrażania nowych usług. Administrator danych ma obowiązek uwzględnić i wdrożyć odpowiednie środki techniczne i organizacyjne zapewniające bezpieczeństwo przetwarzania danych osobowych – środki te zostały przedstawione w odrębnym punkcie Procedury.

Przykład

Planując nową funkcjonalność serwisu internetowego należy sprawdzić, czy procedura gromadzenia danych jest bezpieczna, czyli:

1. Serwis internetowy posiada zabezpieczenia przed atakami hackerskimi,
2. Dane osobowe z formularza trafiają na adres e-mail, do którego dostęp mają wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych albo, z którymi zawarto umowę przetwarzania danych osobowych,
3. Dane osobowe zapisywane są i przechowywane na komputerze chronionym programem antywirusowym oraz zaporą,
4. Komputer, o którym mowa w pkt 3 posiada uwierzytelnienie dostępu chroniące przed dostępem do zapisanych na dysku danych przez osoby trzecie,
5. Układ lub fizyczne zabezpieczenia pomieszczenia, w którym znajduje się komputer nie pozwalają na dostęp do komputera przez osobę trzecią,
6. W przypadku przenoszenia lub przekazywania danych osobowych ich odbiorca spełnia wymagania wskazane w pkt 2-5.

VI. Upoważnienie do przetwarzania danych osobowych

Admirator danych albo podmiot przetwarzający (podmiot, z którym administrator zawarł umowę o powierzenie przetwarzania danych osobowych), zobowiązani są do udzielenia upoważnień osobom dopuszczanym do przetwarzania danych osobowych. Niedozwolona jest praca z danymi osobowymi bez upoważnienia pochodzącego od jednego ze ww. podmiotów.

Przykładowe upoważnienie

Data nadania upoważnienia: .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważniam Panią/Pana .....
   o numerze PESEL .....
   zatrudnioną/-ego na stanowisku .....

w .....

do dostępu do następujących zbiorów danych osobowych w celu ich przetwarzania:

- .....
- .....
- .....

2. Identyfikator/Login: .....

3. Okres trwania upoważnienia: .....

Wystawił: .....

(podpis w imieniu Administratora Danych Osobowych)

4. Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej: .....

VII. Legalność przetwarzania danych osobowych

O legalności przetwarzania danych osobowych decyduje nie tylko istnienie podstawy w przepisach prawa ale także zgodność tejże podstawy z zakresem przetwarzanych danych. Oznacza to, że Administrator może przetwarzać dane wyłącznie, gdy:

1. Istnieje podstawa prawna uprawniająca Administratora danych do ich przetwarzania (patrz niżej),
2. Dane osobowe przetwarzane są wyłącznie w celu wynikającym z danej podstawy prawnej oraz zakomunikowanym osobie, której dane dotyczą (np. w celu świadczenia oraz rozliczenia usługi pośrednictwa w obrocie nieruchomościami),
3. Dane osobowe są gromadzone tylko w zakresie i czasie niezbędnym do realizacji celu, o którym mowa w pkt 2 (po wykonaniu i rozliczeniu usługi należy je usunąć, chyba że osoba, której dane dotyczą wyraziła zgodę na przetwarzanie danych w innym celu albo istnieje inna podstawa prawna ich przetwarzania – patrz ramka).

Zmiana celu przetwarzania – przykład

1. Klient wyraził zgodę na przetwarzanie danych osobowych w celu realizacji usługi pośrednictwa w obrocie nieruchomościami. Klient nie wyrażał innych zgód.
2. Po wykonaniu i rozliczeniu umowy, Administrator danych zamierza w dalszym ciągu przetwarzać te dane osobowe, tylko że w celu marketingu bezpośredniego.
3. Aby było to możliwe Administrator danych powinien powiadomić tę osobę o zmianie celu przetwarzania oraz przesłać stosowną informację (zob. rozdział IX).
4. Dane osobowe mogą być przetwarzane w celu marketingowym, chyba że osoba skorzysta z jej uprawnień, które okażą się zasadne (zob. rozdział X).

RODO za legalne uznaje przetwarzanie danych osobowych, gdy wystąpiła co najmniej jedna z niżej wskazanych przesłanek. Oznacza to w szczególności, że Administrator danych nie

musi każdorazowo dysponować zgodą osoby, której dane przetwarza – wystarczające jest spełnienie chociażby jednej z niżej wskazanych przesłanej:

1. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów,
2. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
3. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
4. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,
5. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
6. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

W praktyce obrotu gospodarczego najczęściej występującymi przesłankami są:

- odebranie zgody od osoby, której dane mają być przetwarzane – należy pamiętać, że oświadczenie o wyrażeniu zgody musi spełniać ustawowe wymagania (wskazane dalej),
- realizacja i zawarcie umowy – brak odrębnej zgody klienta albo kontrahenta nie uniemożliwia przetwarzania danych osobowych, gdy bez tego procesu nie jest możliwe wykonanie umowy na jego rzecz (w tym utrzymywanie bieżącego kontaktu, wystawienie faktury albo rachunku, dochodzenie należności, itp.). Przesłanka ta obejmuje również możliwość przetwarzania danych osobowych przed zawarciem umowy, jednakże zmierzających do jej zawarcia lub wykonania (np. prowadzenie negocjacji w zakresie oferty lub treści umowy, przesłanie próbek, wzorów, referencji, podjęcie innych czynności na wyraźne żądanie klienta/kontrahenta zmierzających do wykonania przyszłej umowy, np. umówienie spotkania, przesłanie ofert, itp),
- przetwarzania danych w uzasadnionych celach administratora (np. marketing bezpośredni własnych towarów i usług) – decydując się na tę przesłankę przetwarzania danych osobowych należy pamiętać o ochronie praw osoby, której dane dotyczą, w tym prawa do prywatności.

VIII. Klauzula zgody na przetwarzanie danych osobowych

Klauzula wyrażenia zgody na przetwarzanie danych osobowych musi spełniać niżej wskazane warunki:

- musi być wyrażona w sposób udokumentowany – nie musi przyjmować formy pisemnej, może być wyrażona drogą elektroniczną - np. mail albo wiadomość wygenerowana przez skrypt formularza zamieszczonego na stronie internetowej, a także w każdej innej postaci, o ile Administrator danych jest w stanie, w każdym czasie i bez dodatkowych środków, wykazać fakt udzielenia zgody,
- nie może być łączona z treścią innych zgód, oświadczeń i klauzul odbieranych przez Administratora danych. Przykładowo, jeżeli Administrator danych prócz zgody na przetwarzanie odbiera także zgodę na przesyłanie informacji handlowej, to obie

klauzule powinny być odrębne – dana osoba może wyrazić zgodę na jedną z nich, obie albo żadną z nich,
- klauzula musi zawierać informację o możliwości odwołania zgody w każdym czasie oraz sposobie i skutkach jej odwołania,
- zgoda powinna być udzielona dobrowolnie, co znaczy że od jej udzielenia nie może być uzależnione świadczenie przez Administratora danych usług, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

Przykład klauzuli zgody:

1. *Wyrażam zgodę na przetwarzanie moich danych osobowych w zakresie: imię, nazwisko, adres e-mail, numer telefonu przez spółkę …, w celu świadczenia na moją rzecz przez wskazaną Spółkę usług pośrednictwa w obrocie nieruchomościami.*
2. *Przyjmuję do wiadomości, że w dowolnym momencie mogę odwołać udzieloną zgodę, pisemnie na adres Administratora danych lub mailowo na adres: …, a wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.*
3. *Mam świadomość, że wyrażenie niniejszej zgody jest dobrowolne, jednakże bez jej wyrażenia nie jest możliwe wykonanie na moją rzecz usług pośrednictwa w obrocie nieruchomościami.*

Jeżeli dane osobowe mają być przekazywane innym podmiotom, bądź przetwarzane również w innych celach, klauzula niniejsza podlegać będzie dalszemu rozbudowaniu – o czym niżej.

IX. Obowiązek informacyjny

Jednym z podstawowych obowiązków Administratora danych jest wykonanie obowiązku informacyjnego względem osoby, której dane są zbierane. Zakres tego obowiązku zależny jest od tego, czy dane osobowe zbierane są bezpośrednio od tej osoby, czy też są one pozyskiwane od innych administratorów danych.

Obowiązek informacyjny może być wykonany w jeden z następujących sposobów - przekazanie osobie, której dane są zbierane:
1. Uprzednio przygotowanej informacji na piśmie,
2. Informacji drogą elektroniczną, np. jako załącznik do maila albo wygenerowanie ich przez skrypt zamieszczony na stronie internetowej, po wysłaniu przez użytkownika formularza kontaktowego,
3. Ustnie, na żądanie tej osoby.

Obowiązek informacyjny, przy zbieraniu danych osobowych bezpośrednio od osoby, której dane są zbierane, obejmuje:
1. tożsamość i dane kontaktowe Administratora danych oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe przedstawiciela,
2. dane kontaktowe inspektora ochrony danych – gdy został powołany,
3. cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania,
4. prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią - jeżeli przetwarzanie odbywa się na tej podstawie,
5. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,

6. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
7. informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
8. jeżeli przetwarzanie odbywa się na podstawie udzielonej zgody – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
9. informacje o prawie wniesienia skargi na Administratora danych do organu nadzorczego,
10. informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
11. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Przykład informacji:

W wykonaniu obowiązku informacyjnego, o którym mowa w art. 13 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), Dz.Urz. UE L 119/1 z 04.05.2016 roku, informuję, że:

1. *Administratorem Państwa danych osobowych jest spółka: …, z siedzibą w: …, numer telefonu: …., adres e-mail: …,*
2. *Osobą odpowiedzialną za realizację usługi na Państwa rzecz jest: …, numer telefonu: …., adres e-mail: …,*
3. *Państwa dane osobowe przetwarzane są w zakresie: imię, nazwisko, adres e-mail, numer telefonu, adres zamieszkania,*
4. *Celem przetwarzania Państwa danych osobowych jest świadczenie na Państwa rzecz usługi pośrednictwa w obrocie nieruchomościami polegającej na …,*
5. *Państwa dane osobowe nie będą przekazywane do krajów poza Unią Europejską, a także do innych odbiorców danych osobowych,*
6. *Podane przez Państwa dane osobowe będą przechowywane w okresie wykonywania usługi pośrednictwa w obrocie nieruchomościami, do czasu jej zakończenia i rozliczenia,*
7. *W każdym czasie uprawnieni są Państwo do dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych. Uprawnienia te mogą Państwo realizować w siedzibie Administratora danych, korespondencyjnie, za pomocą środków komunikacji elektronicznej lub telefonicznie,*
8. *W dowolnym momencie mogą Państwo odwołać udzieloną zgodę, pisemnie na adres Administratora danych lub mailowo na adres: …, a wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem,*
9. *Jeżeli uważają Państwo, że przetwarzanie Państwa danych osobowych przez*

Administratora danych narusza przepisy prawa, uprawnieni są Państwo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (adres: …). Skarga wolna jest od opłat,

10. *Podanie przez Państwa danych osobowych jest dobrowolne. Jednakże, bez ich podania nie będzie możliwe wykonanie na Państwa rzecz usługi pośrednictwa w obrocie nieruchomościami,*
11. *Państwa dane osobowe nie są przetwarzane w sposób zautomatyzowany oraz nie podlegają profilowaniu.*

Informacja nie musi obejmować danych, o których jej adresat ma wiedzę.

Jeżeli Administrator danych planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji.

X. Prawa osób, których dane są przetwarzane

Każda osoba, której dane są przetwarzane ma prawo do:

1. uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz informacji, o których mowa w art. 15 ust. 1 RODO,
2. żądania sprostowania danych,
3. żądania trwałego usunięcia danych (tzw. prawo do zapomnienia),
4. prawo do ograniczenia przetwarzania jej danych osobowych,
5. prawo do przenoszenia danych,
6. prawo do sprzeciwu względem przetwarzania jej danych osobowych dla uzasadnionych celów Administratora danych (np. marketing bezpośredni).

Poniższa tabela przedstawia <u>sposób postępowania</u> w przypadku otrzymania jednego ze ww. żądań od osoby, której dane są przetwarzane.

Żądanie przekazania informacji o przetwarzaniu danych osobowych	Administrator zobowiązany jest do wskazania, czy przetwarza dane osobowej takiej osoby oraz udzielenia jej informacji o: – celach przetwarzania; – kategorii przetwarzanych danych osobowych; – informacji o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych; – w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu; – informacje o prawie do żądania od administratora sprostowania, usunięcia

	lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania; – informacje o prawie wniesienia skargi do organu nadzorczego; – jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle; – informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Informacji należy udzielić bez zbędnej zwłoki, najpóźniej w terminie miesiąca.
Żądanie sprostowania danych	Należy uaktualnić przetwarzane dane osobowe i poinformować o tym osobę, której dane dotyczą. Administrator ma obowiązek – według swoich możliwości - przekazać informację o sprostowaniu danych odbiorcom danych.
Żądanie trwałego usunięcia	Administrator zobowiązany jest niezwłocznie usunąć dane osobowe, chyba że zachodzi jedna z następujących przesłanek: – dane nadal są niezbędne do celów, dla których zostały zebrane, – w przypadku, gdy osoba żądająca usunięcia danych cofnęła zgodę i nie istnieje inna podstawa do przetwarzania jej danych osobowych, – osoba wniosła sprzeciw względem przetwarzania jej danych osobowych, który nie jest zasadny, – dane osobowe są potrzebne do ustalenia, dochodzenia lub obrony roszczeń. Jeżeli dane osobowe zostały przekazane innym podmiotom, Administrator danych, w miarę swoich możliwości, zobowiązany jest do poinformowania innych administratorów

	danych o żądaniu usunięcia wszelkich tych danych, kopii tych danych osobowych lub ich replikacji.
Żądanie ograniczenia przetwarzania	Żądanie należy uwzględnić, jeżeli: – osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych; – przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania; – administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń; – d) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą. Ograniczenie przetwarzania polega na tym, że jej dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej. Administrator ma obowiązek – według swoich możliwości - przekazać informację o ograniczeniu przetwarzania odbiorcom danych.
Żądanie przeniesienia danych	Przysługuje ono osobie, której dane są przetwarzane w oparciu o jej zgodę. Polega ono na tym, że osoba ta może żądać: – prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, a następnie ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe,

	– by dane osobowe zostały przesłane przez Administratora danych bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.
Sprzeciw	Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego lub dla innych uzasadnionych celów Administratora danych (podstawą przetwarzania nie jest zgoda tej osoby), osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim Jeżeli podstawę prawną przetwarzania danych stanowi realizacja uzasadnionego celu administratora, innego niż marketing bezpośredni. Podstawą sprzeciwu może być wyłącznie szczególna sytuacja danej osoby. Wniesienie sprzeciwu uniemożliwia dalsze przetwarzanie danych osobowych na cele marketingowe. W pozostałych przypadkach skutek taki wystąpi, gdy osoba wnosząca sprzeciw wykaże istnienie szczególnej sytuacji uzasadniającej sprzeciw (może to być sytuacja osobista, zdrowotna, zawodowa – o ile dalsze przetwarzanie danych przez Administratora danych wpływa negatywnie na tą sytuację).

O sposobie wykonania albo nie wykonaniu żądania i jego przyczynach należy poinformować osobę, która z nim wystąpiła. Zastosowanie się do uzasadnionego żądania oraz udzielenie odpowiedzi powinno nastąpić niezwłocznie, nie później niż w terminie 30 dni od jego otrzymania.

XI. Powierzenie przetwarzania danych osobowych

Podmiot przetwarzający nie jest administratorem danych osobowych. Przetwarza on dane osobowe:

1. na podstawie umowy zawartej z administratorem danych osobowych,
2. wyłącznie w celu i zakresie wskazanych w umowie,
3. ma obowiązek zapewnić bezpieczeństwo ochrony danych osobowych,
4. ma obowiązek wystawienia upoważnienia do przetwarzania danych osobowych swoim pracownikom.

Podmiot przetwarzający (tzw. procesor) jest najczęściej podwykonawcą albo kontrahentem administratora danych osobowych, któremu dane osobowe przekazywane są w celu wykonania:

- niektórych usług na rzecz klienta, którego dane osobowe są przetwarzane (np. współpracującemu pośrednikowi w obrocie nieruchomościami) lub
- na rzecz administratora danych osobowych (np. biuro rachunkowe, kancelaria prawna).

Przekazanie danych osobowych procesorowi nie wymaga zgody osoby, której dane dotyczą. Jednakże procesor może przekazać dane osobowe uzyskane od administratora danych osobowych (tzw. podpowierzenie danych osobowych), tylko gdy dysponuje na to zgodą administratora:

- ogólną – na podpowierzenie innym podmiotom. W takim jednak przypadku o każdej zmianie grupy podmiotów, którym dane mają zostać przekazane, procesor ma obowiązek poinformować o tym administratora, a ten może wyrazić sprzeciw względem przekazania danych określonemu podmiotowi,
- szczególną – na podpowierzenie konkretnemu podmiotowi/podmiotom.

Przykładowa umowa powierzenia przetwarzania danych osobowych

Umowa powierzenia przetwarzania danych osobowych

zwana dalej „Umową", zwarta w dniu ….201. r. w …, pomiędzy:

… z siedzibą przy ul. … w Gdańsku, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy Gdańsk-Północ w Gdańsku Wydział VII Gospodarczy KRS, pod numerem: …, posiadająca kapitał zakładowy w wysokości: …, numer NIP: …., REGON: ……, którą reprezentuje:
… – Prezes zarządu,
zwana dalej „**Administratorem danych**",

a

…….
reprezentowaną przez:
zwana dalej „**Procesorem**",

zwanymi łącznie „Stronami".

Mając na uwadze, iż Strony łączy Umowa o świadczenie usług, przedmiotem której jest świadczenie usług hostingowych , Strony zgodnie postanowiły, co następuje:

§1
Przedmiot Umowy

1. Strony postanawiają, że w celu spełnienia obowiązków wynikających z przepisów prawa, a w szczególności przepisów 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), Dz.Urz. UE L 119/1 z 04.05.2016 roku (zwanej dalej „RODO") oraz właściwej realizacji postanowień Umowy …, Administrator danych, powierza Procesorowi do przetwarzania dane osobowe w zakresie wynikającym z łączącej Strony współpracy.
2. Z tytułu wykonywania świadczeń określonych w niniejszej Umowie Procesorowi nie przystukuje dodatkowe wynagrodzenie (ponad wynagrodzenie określone w Umowie, o której mowa w ust. 1).

§2
Oświadczenia Stron

1. Administrator danych oświadcza, że powierzone Procesorowi do przetwarzania dane osobowe zgromadził zgodnie z obowiązującymi przepisami prawa.
2. Procesor oświadcza, że zobowiązuje się do wykorzystania danych osobowych, wytycznie w zakresie i celu niezbędnym do realizacji obowiązków wynikających z łączącej Strony współpracy.
3. Dane osobowe przekazane Procesorowi stanowią tajemnicę przedsiębiorstwa Administratora danych, a Procesor zobowiązany jest do zachowania ich w poufności.

§3
Zakres powierzonych danych

Procesor uprawniony jest do przetwarzania powierzonych przez Administratora danych osobowych:

1. Imię i nazwisko,
2. Adres e-mail,
3. Numer telefonu komórkowego,

zawartych w zbiorach:

1. Zbiór danych osobowych klientów,
2. Zbiór danych osobowych kontrahentów,

w następującym zakresie:

1. przechowywanie,
2. kopiowanie,
3. wykorzystywanie w celu realizacji Umowy … .

§4
Zobowiązania Stron

1. Procesor przy przetwarzaniu danych osobowych zobowiązany jest stosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych, a w szczególności powinien zabezpieczyć dane przed ich udostepnieniem osobom nieupoważnionym, utratą, uszkodzeniem lub zniszczeniem.
2. Procesor nie jest uprawniony do przekazywania danych osobowych osobom trzecim, z wyłączeniem osób współpracujących lub pracujących dla Procesora, na co Administrator danych wyraża niniejszym zgodę (zgoda ogólna). Procesor ma obowiązek informować Administratora danych o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia osób wskazanych w zdaniu 1, dając tym samym Administratorowi danych możliwość wyrażenia sprzeciwu wobec takich zmian.
3. W celu uniknięcia wątpliwości, w imieniu Procesora powierzone dane osobowe mogą

przetwarzać wyłącznie osoby, które uprzednio uzyskały od niego pisemne upoważnienie.
4. Procesor zobowiązany jest do zebrania od swoich pracowników lub współpracowników, przy pomocy których realizować będzie przedmiot niniejszej Umowy, oświadczeń o nieograniczonym w czasie obowiązku zachowania w tajemnicy powierzonych danych osobowych. Procesor zobowiązuje się okazać oświadczenia, o których mowa w zdaniu poprzedzającym, na każde żądanie Administratora danych.
5. Procesor zobowiązany jest do przeszkolenia swoich pracowników tub współpracowników w zakresie sposobów zabezpieczenia przetwarzanych danych.
6. Ponadto Procesor zobowiązany jest do pomagania Administratorowi danych, poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO, a także obowiązków wskazanych w art. 32-36 RODO,

§5
Prawo kontroli

1. Administrator danych zastrzega sobie prawo kontroli właściwego przetwarzania przez Procesora powierzonych danych osobowych. Procesor na każdy pisemny wniosek Administratora danych zobowiązany jest do udzielenia pisemnej informacji dotyczącej przetwarzania powierzonych mu danych osobowych, w terminie 7 dni od dnia otrzymania wniosku Administratora danych.
2. Niezależnie od ust. 1, Procesor zobowiązany jest – w każdym czasie oraz na żądanie Administratora danych - udostępniać mu wszelkie informacje niezbędne do wykazania spełnienia obowiązków Administratora danych nałożonych na niego przez RODO.
3. Jeżeli w ocenie Procesora wydane mu przez Administratora danych polecenie stanowi naruszenie RODO lub innych przepisów prawa o ochronie danych, Procesor niezwłocznie informuje o tym Administratora danych.

§6
Odpowiedzialność

1. Każda ze Stron odpowiada za szkody wyrządzone drugiej Stronie oraz osobom trzecim w związku z wykonaniem niniejszej Umowy, zgodnie z przepisami RODO, Kodeksu cywilnego oraz postanowieniami niniejszej Umowy.
2. W celu uniknięcia wątpliwości, Procesor ponosi odpowiedzialność za działania swoich pracowników i innych osób, przy pomocy których przetwarza dane osobowe, w tym osób i podmiotów, o których mowa w §4 ust. 5, jak za własne działanie i zaniechanie.
3. Jeżeli osoba trzecia wystąpi do Administratora danych z roszczeniem spowodowanym z winy Procesora lub osób, za które Procesor ponosi odpowiedzialność, Procesor zobowiązany jest do zwolnienia Administratora danych ze wszelkich zobowiązań względem takiej osoby trzeciej.

§7
Czas trwania i wypowiedzenie Umowy

1. Umowa zostaje zawarta na czas obowiązywania Umowy …. W celu uniknięcia wątpliwości, wygaśnięcie Umowy wskazanej w zdaniu 1, z jakiejkolwiek przyczyny, skutkuje wygaśnięciem niniejszej Umowy.
2. Administrator danych uprawniony jest do rozwiązania Umowy bez wypowiedzenia,

jeżeli:

a) w wyniku kontroli zostanie wykazane, że Procesor nie podjął środków zabezpieczających, o których mowa w art. 32-34 RODO,
b) Procesor nie stosował się do wymogów przewidzianych w aktach wykonawczych do Ustawy,
c) przetwarza dane osobowe niezgodnie z niniejszą Umową lub innymi przepisami RODO.

3. W przypadku rozwiązania Umowy Procesor, w terminie 7 dni, zobowiązany jest do trwałego zniszczenia i wykasowania wszelkich sporządzonych w związku lub przy okazji wykonywania Umowy zapisów oraz dokumentów zawierających powierzone do przetwarzania dane osobowe. Procesor zobowiązany jest pisemnie potwierdzić Administratorowi danych, w terminie 7 dni, o dokonaniu czynności, o których mowa w zdaniu poprzedzającym.

§8
Postanowienia końcowe

1. Umowa wchodzi w życie z dniem podpisania przez Strony.
2. W sprawach nieuregulowanych stosuje się obowiązujące przepisy prawa, w szczególności Kodeksu cywilnego oraz RODO.
3. Wszelkie zmiany lub uzupełnienia Umowy wymagają zachowania formy pisemnej pod rygorem nieważności.
4. Sądem właściwym dla rozstrzygania sporów powstałych w związku z realizacja Umowy, jest sąd właściwy dla siedziby Administratora danych.
5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

[……] **[……]**

Każdy podmiot przetwarzający dane osobowe powierzone mu przez administratora danych ma obowiązek prowadzenia rejestru czynności dokonywanych w ramach powierzenia. W rejestrze tym powinny zostać zamieszczone następujące informacje:

1. imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający,
2. kategorie przetwarzań dokonywanych w imieniu każdego z administratorów (rodzaje wykonywanych operacji na danych osobowych,
3. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Rejestr może być prowadzony w formie pisemnej albo w formie elektronicznej.

XII. Rejestr czynności przetwarzania

RODO nie przewiduje obowiązku rejestracji zbiorów danych osobowych w krajowym organie administracji. Zamiast tego, każdy administrator danych osobowych ma obowiązek prowadzenia wewnętrznego rejestru czynności przetwarzania w swojej jednostce organizacyjnej.

Rejestr może być prowadzony w formie pisemnej albo w formie elektronicznej oraz powinien zawierać następujące informacje:

1. imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów (gdy występują), a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych (gdy zostali ustanowieni/powołani),
2. cele przetwarzania,
3. opis kategorii osób, których dane dotyczą (np. pracownicy, klienci, kontrahenci), oraz kategorii danych osobowych (imię, nazwisko, adres e-mail, telefon, itp.),
4. gdy ma to zastosowanie - kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
5. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
6. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
7. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Przykładowy rejestr czynności przetwarzania

Rejestr czynności przetwarzania danych osobowych w firmie…

1. Administrator danych osobowych:

Pełna nazwa: ……

Adres siedziby: ……

Numer telefonu: ……..

Inspektor ochrony danych osobowych (imię i nazwisko): …….

Numer telefonu Inspektora ochrony danych osobowych: ……

2. Czynności przetwarzania danych osobowych

Nazwa zbioru	**Cele przetwarzania**	**Kategorie osób, których dane dotyczą**	**Kategorie danych osobowych**	**Planowany termin usunięcia danych**	**Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa**
Dane osobowe klientów	Wykonywanie i rozliczanie usług pośrednictwa w	Klienci firmy	1. Imię, 2. Nazwisko, 3. Adres,	Dwa lata od zakończenia umowy	1. Firma stosuje zabezpieczenia logiczne

	obrocie nieruchomościami		4. Telefon, 5. Mail.		(hasłem) dostępu do komputerów, na których przetwarzane są dane osobowe, 2. Stosowane są środki ochrony fizycznej (zamykanie pomieszczeń na klucz, podczas nieobecności pracowników), 3. Stosowane są zabezpieczenia prawne – dane osobowe przekazywane są wyłącznie w oparciu o umowy lub upoważnienia.

XIII. Bezpieczeństwo przetwarzania danych osobowych

Administrator danych oraz podmiot przetwarzający zobowiązani są do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia danych osobowych.

Dobór tych środków należy do ww. podmiotów. Winny mieć one wszakże na względzie takie czynniki, jak: stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. Środki te powinny zapewniać:

1. pseudonimizację lub szyfrowanie danych osobowych,
2. zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
3. zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
4. regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Środki zapewniające bezpieczeństwo przetwarzania danych osobowych - przykłady

Do omawianych środków należą następujące – to spośród nich i nim podobnym, administrator powinien wybrać środki podlegające wdrożeniu w jego firmie:

- pomieszczenia zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych,
- stosuje się mechanizmy kontroli dostępu do danych (np. hasła dostępu), w przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 8 znaków,
- każdy z użytkowników otrzymuje odrębny login i hasło,
- system informatyczny posiada aktualne oprogramowanie antywirusowe oraz zapory, a także wykonujące automatyczne kopie zapasowe,
- urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
    - likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
    - przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
    - naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych,
- nośniki wykorzystywane do celów operacyjnych należy przechowywać, w czasie nieobecności w pomieszczeniu osoby upoważnionej, w zamykanych na klucz szafach lub sejfach. W przypadku, gdy zbiór danych osobowych był zapisany na nośniku w sposób trwały i nie będzie dalej wykorzystywany, należy go zniszczyć fizycznie po skopiowaniu danych na dysk twardy stacji roboczej (serwera), wprowadzeniu do systemu, aplikacji itp.
- komunikacja pomiędzy stacjami roboczymi i serwerami odbywa się w oparciu o bezpieczne protokoły transmisji danych. Styk sieci lokalnej z siecią publiczną chroniony jest przez zastosowanie zapory ogniowej (firewall) oraz jej bieżący monitoring,
- komunikacja z siecią publiczną powinna odbywać się przez jeden punkt dostępu. Porty protokołu TCP/IP, które nie są wykorzystywane do transmisji danych są blokowane. Na urządzeniach sieciowych włączono logowania na podstawie kodu i hasła. Adresy protokołu TCP/IP powinny być nadawane centralnie i otrzymać je mogą wyłącznie urządzenia, których adresy fizyczne zarejestrowano w bazie danych MAC adresów,
- w sytuacji przetwarzania danych osobowych, przez pracowników na komputerach przenośnych lub dokumentach papierowych poza obszarem przetwarzania danych osobowych, są oni zobowiązani chronić nośnik oraz dane przed utratą i dostępem osób nieuprawnionych. W tym do dodatkowego zabezpieczenia hasłem plików lub folderów zawierających dane osobowe,
- dokumenty papierowe zawierające dane osobowe powinny być chronione przed dostępem osób nieuprawnionych podczas ich przetwarzania. Dokumenty papierowe z danymi osobowymi, w czasie nieobecności w pomieszczeniu osoby upoważnionej do przetwarzania danych osobowych, muszą być przechowywane w zamykanych na klucz sprzętach biurowych,
- dokumenty lub nośniki danych zawierające dane osobowe powinny być archiwizowane lub niszczone w sposób gwarantujący brak możliwości odczytania danych osobowych zawartych w dokumentach lub nośnikach elektronicznych,
- Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

Zabezpieczenia stosowane aktualnie w firmie:

- korzystanie wyłącznie z legalnego i aktualizowanego na bieżąco oprogramowania,
- instalacja oprogramowania odbywa się tylko ze sprawdzonych i wiarygodnych źródeł,
- zakazane jest ściąganie i/lub instalowane oprogramowanie z niezweryfikowanych i niezbadanych źródeł jak fizyczne nośniki danych dostarczane przez postronne osoby, wyskakujące okienka, nieoczekiwana lub niezamawiana poczta elektroniczna z załącznikami, nielegalne usługi umożliwiające wymianę plików, itp.
- zakazane jest instalowanie oprogramowanie nie służące do celów służbowych, w szczególności typu gry (oprócz gier standardowo / domyślnie zainstalowanych przez producenta systemu operacyjnego),
- stosowany jest program antywirusowy w trybie monitorowania aktywnego oraz z automatyczną aktualizacją baz wirusów,
- stosowana jest zapora sieciowa (firewall),
- gdy jest to wymagana (np. na mocy odrębnej umowy) stosowane jest szyfrowanie danych,
- gdy jest to konieczne do realizacji umowy, dane są przesyłane pocztą elektroniczną tylko w postaci zaszyfrowanej,
- komputery oraz nośniki danych (np. pendrive) nie są pozostawiane bez zabezpieczenia oraz w miejscach dostępnych dla osób trzecich,
- przetwarzanie danych osobowych odbywa się wyłącznie przez osoby upoważnione przez ADO,
- dostęp do systemu informatycznego ograniczony jest indywidualnym loginem i hasłem:
    - Minimalna długość hasła: min 8 znaków.
    - Maksymalny okres używania hasła (po ilu dniach następuje wymuszanie zmiany hasła): 30 dni.
    - Historia haseł ustawiona na min 6 miesięcy.
    - Ustawione jest wymuszanie złożoności (nietrywialności) hasła.
- hasła nie są generalnie zapisywane w żaden sposób, w szczególności nie są zapisywane na nośnikach (papier, dysk, pendrive, itp.) możliwych do odczytania przez inne osoby,
- zakazane jest przekazywanie loginów i haseł innym osobom,
- wygaszacz ekranu na komputerze jest aktywny i zabezpieczony hasłem. Czas nieaktywności (po jakim czasie się włącza) ustawiony jest na : max 15 minut,
- komputer powinien być używany tak, by nie było możliwe zainstalowanie złośliwego oprogramowania (np. wirusów, trojanów itp.) czy nielegalne przejęcie komputera przez strony trzecie,
- komputer należy wykorzystywać wyłącznie w celach służbowych, zakazane jest np. korzystanie z prywatnych kont pocztowych, bądź prywatnych profili w portalach społecznościowych,
- nośniki z danymi osobowymi nie są przekazywane razem ze sprzętem do naprawy - są wyjmowane i zabezpieczane na czas naprawy czy konserwacji.

XIV. Zgłaszanie naruszeń

RODO wprowadza również, nieznany dotychczas, obowiązek raportowania o wykryciu naruszenia ochrony danych osobowych. Jest on zależny od osoby, która naruszenie wykryła, a także skutków naruszenia – stosowne zestawienie przedstawia poniższa tabela.

Za naruszenie praw lub wolności osób fizycznych uznać można przykładowo naruszenie prawa do prywatności, bądź ujawnienie danych osobowych osobie niepożądanej.

Procedurę postępowania w przypadku wykrycia naruszeń, wraz z podziałem na ich rodzaj, przedstawia poniższa tabela.

<table>
<tr><td></td><td>Naruszenie nieistotne – nie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych</td><td>Naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych</td><td>Naruszenie skutkuje wysokim ryzykiem naruszenia praw lub wolności osób fizycznych</td></tr>
<tr><td rowspan="2">Administrator danych</td><td colspan="3">Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.</td></tr>
<tr><td>Brak dodatkowych obowiązków ponad powyższe</td><td>Zgłoszenie tego faktu organowi nadzoru</td><td>Zgłoszenie tego faktu organowi nadzoru oraz osobie, której dane dotyczą*.</td></tr>
<tr><td>Podmiot przetwarzający</td><td colspan="3">Zgłoszenie tego faktu Administratorowi</td></tr>
</table>

* Zawiadomienie osoby, której dane dotyczą, nie jest wymagane, w następujących przypadkach:

- 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,
- administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
- wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

XV. Dane osobowe w zatrudnieniu

1. Zasady ogólne

Zgodnie z przepisami Kodeku pracy (art. 22^1) pracodawca uprawniony jest do przetwarzania szeregu danych osobowych pracowników. Co ważne, pracodawca posiada także uprawnienie do żądania ujawnienia tych danych przez pracownika, a także przez osobę ubiegającą się o zatrudnienie (aplikującą o pracę u pracodawcy). Podstawę prawną żądania tych danych stanowi ww. przepis Kodeksu pracy.

Przedmiotowe upoważnienie obejmuje następujące dane osobowe osoby ubiegającej się o zatrudnienie:

1. imię (imiona) i nazwisko,
2. imiona rodziców,
3. datę urodzenia,
4. miejsce zamieszkania (adres do korespondencji),
5. wykształcenie,
6. przebieg dotychczasowego zatrudnienia,

Względem pracownika natomiast, pracodawca uprawniony jest do przetwarzania danych osobowych:

1. wskazanych powyżej w punktach 1-6,
2. innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy,
3. numeru PESEL pracownika nadanego przez Rządowe Centrum Informatyczne Powszechnego Elektronicznego Systemu Ewidencji Ludności (RCI PESEL).

Pracodawca uprawniony jest także do żądana od ww. osób udokumentowania prawdziwości podanych informacji i danych osobowych.

Do danych osobowych ww. osób stosuje się zasady przetwarzania wynikające z RODO. Oznacza to, że:

1. osoby te mogą rozpocząć przetwarzanie danych osobowych po udzieleniu im upoważnienia przez Administratora danych,
2. dane osobowe ww. osób mogą być powierzone do przetwarzania innym podmiotom (np. biuro rachunkowe, kancelaria prawna) na mocy umowy powierzenia danych,
3. operacje na danych osobowych ww. osób wpisuje się do Rejestru czynności przetwarzania,
4. pracodawca zobowiązany jest do zapewnienia bezpieczeństwa przetwarzania danych ww. osób, a także stosować procedury zgłaszania naruszeń, na tych samych zasadach, co innych danych osobowych,
5. dane osobowe osób ubiegających się o zatrudnienie, po zakończeniu rekrutacji:
    a. należy usunąć albo zanonimizować, chyba że
    b. dana osoba została zatrudniona albo wyraziła zgodę na przetwarzanie danych osobowych na potrzeby dalszych rekrutacji.

Przykład klauzuli zgody w toku postępowania rekrutacyjnego:

1. *Wyrażam zgodę na przetwarzanie moich danych osobowych w zakresie: imię, nazwisko, adres e-mail, numer telefonu przez spółkę …, w celu uczestnictwa w procesie rekrutacji na stanowisko …, numer oferty pracy: … .*
2. *Wyrażam również zgodę na przetwarzanie moich danych osobowych w zakresie wskazanym w punkcie 1, przez spółkę …, w celu uczestnictwa w przyszłych procesach rekrutacji prowadzonych przez tego Administratora danych osobowych.*
3. *Przyjmuję do wiadomości, że w dowolnym momencie mogę odwołać udzieloną zgodę, pisemnie na adres Administratora danych lub mailowo na adres: …, a wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie*

zgody przed jej wycofaniem.

4. *Mam świadomość, że wyrażenie niniejszej zgody jest dobrowolne, jednakże bez jej wyrażenia nie jest możliwe uwzględnienie mojej aplikacji w procesie rekrutacji, o którym mowa w punkcie 1.*

2. Akta osobowe

Po zakończeniu zatrudnienia pracownika jego akta osobowe należy przekazać z upływem roku kalendarzowego, w którym zakończył się stosunek pracy do archiwum zakładowego oraz przechowywać przez okres 50 lat. Jeżeli następuje likwidacja zakładu pracy, pracodawca musi wskazać podmiot prowadzący działalność w zakresie przechowywania dokumentacji, któremu zostanie ona przekazana.

3. Współpracownicy

Osoby takie należy podzielić na dwie kategorie:

a) osoby współpracujące stale z Administratorem danych na warunkach samozatrudnienia, czyli gdy Administrator danych jest jedynym kontrahentem takiej osoby fizycznej prowadzącej działalność gospodarczą,
b) osoby współpracujące z Administratorem danych na zasadach rynkowych (osoby prowadzą również działalność gospodarczą poza współpracą z Administratorem danych).

Prawa i obowiązki względem obu kategorii współpracowników wskazuje poniższa tabela.

	Samozatrudnieni	**Inni współpracownicy**
Podstawa prawna przetwarzania danych osobowych współpracowników przez Administratora danych	– w czasie trwania umowy - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą (art. 6 ust. 1 lit. b) RODO) – po zakończeniu umowy - przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora, np. rozliczenie i windykacja należności (art. 6 ust. 1 lit. f) RODO).	
Podstawa udostępnienia danych osobowych przetwarzanych przez Administratora danych	Osobie takiej należy udzielić upoważnienia.	Z osobą taką należy zawrzeć umowę powierzenia danych osobowych do przetwarzania.
Prawa i obowiązki	Przestrzeganie wewnętrznej procedury przetwarzania danych osobowych wprowadzonej przez Administratora danych	Posiadanie własnej procedury przetwarzania danych osobowych
Bezpieczeństwo danych	Zapewnia Administrator danych	Samodzielny obowiązek zapewnienia środków bezpieczeństwa danych osobowych.

XVI. Postanowienia końcowe

1. Wątpliwości, dotyczące interpretacji lub zastosowania przepisów Procedury wyjaśnia Administrator danych.
2. Tekst Procedury powinien zostać udostępniony użytkownikom w taki sposób, aby mogli się
z nim zapoznać i wdrożyć w życie jej postanowienia. Jednocześnie tekst Procedury stanowi tajemnicę przedsiębiorstwa Administratora danych w rozumieniu ustawy z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji.
3. Zmiana Procedury wymaga zatwierdzenia przez Administratora danych uchwałą zarządu Spółki.
4. Procedura została przyjęta uchwałą zarządu Administratora danych z dnia … 2018 roku oraz wchodzi w życie z dniem … 2018 roku.