Załącznik do Uchwały Nr 2/07/2024
Zarządu spółki RR Security sp. z o.o.
z dnia 09 lipca 2024 r.

POLITYKA

OCHRONY DANYCH OSOBOWYCH

W RR SECURITY SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

ADMINISTRATOR DANYCH:
RR Security Spółka z ograniczoną odpowiedzialnością
INSPEKTOR OCHRONY DANYCH:
Damian Stachyra, iod@rrsecurity.pl
DATA PRZYJĘCIA DOKUMENTU:
09.07.2024

WYKAZ ZDARZEŃ ZWIĄZANYCH Z PROCEDURĄ		
Data zdarzenia	**Rodzaj zdarzenia**	**Osoba odpowiedzialna**
	Opracowanie dokumentu	
	Przyjęcie dokumentu	
	Weryfikacja dokumentu	
	Aktualizacja dokumentu	

Spis treści

1. POSTANOWIENIA OGÓLNE

Definicje

1.1. Pojęciom i skrótom użytym w dalszej części dokumentu nadaje się następujące znaczenie:

1.2.	**Administrator (ADO)**	–	RR Security Spółka z ograniczoną odpowiedzialnością
1.3.	**Dane osobowe (dane)**	–	wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
1.4.	**Dane osobowe szczególnych kategorii**	–	dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.
1.5.	**EOG**	–	Europejski Obszar Gospodarczy.
1.6.	**Inspektor (IOD)**	–	wyznaczony przez Administratora inspektor ochrony danych lub zastępca inspektora ochrony danych, którego dane kontaktowe znajdują się na stronie tytułowej.
1.7.	**Polityka**	–	niniejsza Polityka ochrony danych osobowych w RR Security Sp. z o.o. z ograniczoną odpowiedzialnością
1.8.	**Podmiot danych**	–	osoba fizyczna, której dane osobowe są przetwarzane przez Administratora.
1.9.	**Pracownik**	–	osoba fizyczna zatrudniona u Administratora, niezależnie od podstawy zatrudnienia (umowa o pracę, zlecenie, B2B).
1.10.	**Prezes UODO**	–	organ nadzorczy ds. ochrony danych osobowych – Prezes Urzędu Ochrony Danych Osobowych.
1.11.	**RODO**	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
1.12.	**Zarząd**	–	Zarząd RR Securitu Sp. z o.o. ograniczoną odpowiedzialnością

1.13. Pojęciom użytym w Polityce, które nie zostały wyżej zdefiniowane, nadaje się znaczenie zgodne ze znaczeniem przypisanym im w art. 4 RODO, a jeżeli nie zostały one zdefiniowane w tym przepisie, należy im nadać znaczenie zgodnie z powszechnie używanym.

Cele i zakres Polityki

1.14. Polityka określa podstawowe zasady, którymi kieruje się Administrator przy przetwarzaniu danych osobowych, określa role podmiotów biorących udział w procesie przetwarzania i ich odpowiedzialności. Stanowi ona również zbiór procedur przetwarzania danych osobowych, których celem jest zapewnienie zgodności działania Administratora z powszechnie obowiązującymi przepisami prawa. Wśród procedur uregulowanych w treści Polityki znajduje się nadawanie i odbieranie upoważnień, powierzenie przetwarzania danych osobowych, realizacja praw podmiotów danych, postępowanie w razie wystąpienia naruszenia ochrony danych oraz procedura współpracy z organem nadzorczym.

1.15. Polityka może być uzupełniana przez inne, nieuregulowane w niej bezpośrednio procedury związane z ochroną danych osobowych, w tym procedury dotyczące zarządzania systemami informatycznymi. W razie kolizji pomiędzy Polityką i innymi regulacjami wewnętrznymi, należy podjąć wszelkie działania umożliwiające ich współstosowanie. Jeżeli nie będzie to możliwe, konflikt rozstrzyga Zarząd wybierając rozwiązanie zapewniające jak najwyższy poziom bezpieczeństwa danych osobowych.

1.16. Polityka stanowi dokument wewnętrzny. Nie podlega ona ujawnieniu podmiotom zewnętrznym wobec organizacji Administratora, chyba że obowiązek jej ujawnienia wynika z powszechnie obowiązujących przepisów prawa lub żądania uprawnionego organu publicznego.

Odpowiedzialność – podział zadań

1.17. **Zarząd** – wdraża Politykę wraz z wynikającymi z niej procedurami, a także monitoruje i egzekwuje ich przestrzeganie. Rozstrzyga on również wątpliwości związane ze stosowaniem Polityki oraz wykonuje inne zadania przypisane do Zarządu lub ogólnie do Administratora w Polityce. Podejmuje on również decyzje o odstępstwach w zastosowaniu postanowień Polityki. Realizuje on też zadania niezastrzeżone do kompetencji innych podmiotów (domniemanie odpowiedzialności/kompetencji Zarządu).

1.18. **Inspektor** – monitoruje przestrzeganie Polityki i procedur związanych z ochroną danych osobowych, a także raportuje do Zarządu o wynikach tego monitoringu. Przedstawia on również opinię co do wykładni poszczególnych postanowień Polityki, dokonuje jej okresowych przeglądów i wykonuje inne zadania przypisane do jego kompetencji w dalszych postanowieniach Polityki.

1.19. **Osoby wyznaczone przez Administratora** – odpowiadają za realizację konkretnych zadań wynikających z Polityki, przypisanych im w Uchwale Zarządu przyjmującej Procedurę.

1.20. **Pracownicy** – zobowiązani są do przestrzegania postanowień Polityki oraz reagowania na wszelkie przejawy jej naruszenia, w tym do raportowania takich zdarzeń Inspektorowi.

2. ZASADY I PODSTAWY PRZETWARZANIA

Zasady przetwarzania danych osobowych

2.1. Administrator zapewnia, aby przetwarzanie danych osobowych w jego organizacji odbywało się zgodnie z zasadami:

2.1.1. **zgodności z prawem** – a więc, aby dane osobowe były przetwarzane zgodnie z powszechnie obowiązującymi przepisami prawa, w tym z przepisami RODO,

2.1.2. **rzetelności** – a więc, aby dane osobowe były przetwarzane w dobrej wierze, w sposób, dokładny, uczciwy i uwzględniający interesy podmiotów danych oraz ich autonomię w zakresie przetwarzania danych, z nakierowaniem na eliminację przetwarzania bezzasadnie szkodliwego, nieoczekiwanego, czy wprowadzającego podmiot danych w błąd,

2.1.3. **przejrzystości** – a więc, aby przetwarzanie danych odbywało się w sposób transparentny dla podmiotu danych, w szczególności, aby był on wcześniej poinformowany o fakcie przetwarzania jego danych oraz o zakresie takiego przetwarzania,

2.1.4. **ograniczenia celu** – a więc, aby dane osobowe były zbierane w konkretnych wyraźnych i prawnie uzasadnionych celach. Cele przetwarzania Administrator określa najpóźniej w momencie pozyskania danych. Zabronione jest pozyskiwanie danych dla przyszłych, bliżej nieokreślonych celów,

2.1.5. **minimalizacji danych** – a więc, aby dane osobowe były adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Administrator określa zakres danych, które są mu niezbędne do osiągnięcia założonego celu przetwarzania danych osobowych i dba o to, aby nie pozyskiwać danych, które są zbędne dla tego celu. Niedopuszczalne jest pozyskiwanie danych osobowych na wszelki wypadek,

2.1.6. **prawidłowości** – a więc, aby dane osobowe były prawidłowe i w miarę potrzeby uaktualniane. W tym celu Administrator podejmuje rozsądne działania, aby gromadzić dane jedynie z zaufanych źródeł, a także niezwłocznie prostować albo usuwać nieaktualne, niepełne lub nieprawidłowe dane,

2.1.7. **ograniczenia przechowywania** – a więc, aby dane osobowe były przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których są przetwarzane. Administrator określa okresy retencji danych i dba o to, aby po ich upływie dane osobowe zostały usunięte lub zanonimizowane,

2.1.8. **integralności i poufności** – a więc, aby dane osobowe były przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, a także przed przypadkową utratą, zniszczeniem lub uszkodzeniem. W tym celu Administrator przeprowadza analizę ryzyka przetwarzania danych z perspektywy praw i wolności podmiotów danych, a także wdraża odpowiednie środki bezpieczeństwa,

2.1.9. **rozliczalności** – a więc, aby przetwarzanie danych osobowych odbywało się w sposób pozwalający Administratorowi wykazać, że przestrzega on wskazanych wyżej zasad i przetwarza dane zgodnie z RODO. W tym celu Administrator dokumentuje proces przetwarzania danych oraz prowadzi właściwe rejestry określone niniejszą Polityką.

2.2. Administrator stosuje **ochronę danych osobowych w fazie projektowania** (*privacy by design*), w tym **domyślna ochronę danych osobowych** (*privacy by default*). W tym celu Administrator zapewnia, w szczególności, aby w każdym nowym procesie przetwarzania:

2.2.1. zostały ustalone cele przetwarzania, możliwie szczegółowy zakres danych osobowych niezbędnych do realizacji tego celu, a także podstawy prawne, które legalizują przetwarzanie określonych danych, z uwzględnieniem zasad ogólnych przetwarzania,

2.2.2. zostały określone narzędzia/sposoby przetwarzania danych osobowych i zweryfikowane zostały, czy przetwarzanie z ich udziałem zapewnia realizację zasad ogólnych oraz praw osób, których dane dotyczą, np. czy planowane sposoby i narzędzia przetwarzania danych umożliwiają sprostowanie wprowadzonych do nich danych osobowych, ich usuniecie, a także przeszukanie celem realizacji prawa dostępu do danych,

2.2.3. ustalono formę realizacji obowiązku informacyjnego wobec podmiotów danych, np. zaprojektowanie nowego rozwiązania z uwzględnieniem miejsca na klauzule informacyjną, treść zgody,

2.2.4. ustalono jakie kategorie podmiotów muszą mieć dostęp do danych osobowych, w tym czy w procesie będą wykorzystywane podmioty przetwarzające, a jeżeli tak, to jakie warunki powinny one spełniać,

2.2.5. określić przez jaki okres będą przechowywane dane osobowe, z uwzględnieniem celów ich przetwarzania,

2.2.6. upewnić się, że domyślnie włączona będzie ochrona prywatności, czyli z założenia zbierany będzie od użytkownika możliwie jak najwęższy zakres danych osobowych oraz celów przetwarzania, który poszerzany będzie wyłącznie z inicjatywy podmiotu danych – przykładowo, jeżeli w procesie przetwarzania przewiduje się pobieranie zgód marketingowych, to muszą one być domyślnie odznaczone, a ich ewentualne wyrażenie (zaznaczenie) musi być wyłączną intencją podmiotu danych,

2.2.7. zweryfikować czy planowany proces przetwarzania uwzględnia konieczność zapewnienia odpowiedniego bezpieczeństwa danych, a w tym celu – przeprowadzenie analizy ryzyka i dobranie odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych.

Podstawy prawne przetwarzania danych

2.3. Administrator przetwarza dane osobowe wyłącznie wówczas, gdy przetwarzanie takie znajduje oparcie w co najmniej jednej z przesłanek legalizujących takie przetwarzanie, wskazanych w art. 6 ust. 1 RODO, a w szczególności, gdy:

2.3.1. przetwarzanie danych jest **niezbędne do wykonania umowy, której stroną jest podmiot danych** lub do podjęcia na jego żądanie działań przed zawarciem umowy,

2.3.2. przetwarzanie jest **niezbędne do wypełnienia obowiązku prawnego** ciążącego na administratorze w oparciu o powszechnie obowiązujące przepisy prawa,

2.3.3. przetwarzanie jest **niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub stronę trzecią**, chyba że nadrzędny charakter mają wobec nich interesy lub podstawowe prawa i wolności podmiotu danych,

2.3.4. przetwarzanie jest **niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby trzeciej,**

2.3.5. osoba, której dane dotyczą wyraziła **zgodę na przetwarzanie swoich danych osobowych** przez Administratora.

2.4. Administrator nie przetwarza **danych szczególnych kategorii**, chyba że zachodzi co najmniej jeden z warunków przewidzianych w art. 9 ust. 2 RODO, a w szczególności:

2.4.1. osoba, której dane dotyczą wyraziła **wyraźną zgodę na przetwarzanie swoich danych,**

2.4.2. przetwarzanie takich danych jest **niezbędne do wypełnienia obowiązku prawnego lub wykonywania szczególnych praw przez Administratora lub podmiot danych,** w

dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone powszechnie obowiązującymi przepisami prawa,

2.4.3. przetwarzanie takich danych jest **niezbędne do ochrony żywotnych interesów podmiotu danych lub innej osoby fizycznej**, a podmiot danych jest fizycznie lub prawnie niezdolny do wyrażenia zgody,

2.4.4. przetwarzanie dotyczyć będzie takich danych szczególnych kategorii, które zostały w sposób oczywiście **upubliczniony przez podmiot danych**,

2.4.5. przetwarzanie takich danych jest **niezbędne do ustalenia, dochodzenia lub obrony roszczeń.**

Identyfikowanie procesów przetwarzania

2.5. Administrator identyfikuje wszystkie czynności przetwarzania danych osobowych, do których dochodzi w jego organizacji, a także ustala on cele i sposoby przetwarzania, podmioty biorące w nim udział, zasady wykorzystywane do przetwarzania danych osobowych oraz podstawy prawne przetwarzania danych i okresy retencji danych.

2.6. Administrator ewidencjonuje wszystkie czynności przetwarzania danych osobowych w **rejestrze czynności przetwarzania danych osobowych (RCPD) lub rejestrze kategorii czynności przetwarzania (RKCP)**. RCPD i RKCP prowadzony jest przez Administratora w formie elektronicznej według wzoru określonego w Załączniku nr 1A i 1B do Polityki. RCPD i RKCP stanowią dokument wewnętrzny i mogą być udostępniane wyłącznie na żądanie uprawnionych organów publicznych.

2.7. Ustalając okresy retencji przetwarzanych danych osobowych Administrator uwzględnia:

2.7.1. okresy przechowywania danych narzucone przez powszechnie obowiązujące przepisy prawa, a jeżeli przepisy nie regulują maksymalnego okresu przechowywania danych osobowych

2.7.2. niezbędność przechowywania danych osobowych dla realizacji wyznaczonych celów przetwarzania, w tym dla zabezpieczenia się przed roszczeniami.

3. UCZESTNICY PROCESU PRZETWARZANIA DANYCH (UPOWAŻNIENIA, POWIERZENIE, UDOSTĘPNIENIE)

3.1. Dane osobowe administrowane przez Administratora mogą być przetwarzane przez:

3.1.1. **organy Administratora** – w zakresie wynikających z kompetencji przyznanym ich przez ustawę lub akt założycielski (umowę spółki, statut),

3.1.2. **Pracowników** – w zakresie niezbędnym do realizacji ich obowiązków służbowych lub umownych i zgodnie z zakresem udzielonego upoważnienia,

3.1.3. **podmioty przetwarzające** – w zakresie danych powierzonych do przetwarzania takim podmiotom przez Administratora w oparciu o stosowną umowę powierzenia przetwarzania danych osobowych.

3.2. Administrator stosuje zasadę ograniczonego dostępu do danych osobowych, poprzez określanie zakresu danych osobowych, do których dostęp mają mieć poszczególne grupy Pracowników.

Upoważnienia do przetwarzania danych osobowych

3.3. Do przetwarzania danych osobowych u Administratora dopuszczani są jedynie Pracownicy, którzy:

3.3.1. ukończyli szkolenie podstawowe z zakresu ochrony danych osobowych oraz zaliczyli test wiedzy na temat ochrony danych osobowych,

3.3.2. uzyskali upoważnienie do przetwarzania danych nadane przez Administratora,

3.3.3. zobowiązali się do zachowania w tajemnicy danych osobowych, do których uzyskają dostęp w ramach realizacji obowiązków służbowych lub umownych, a także informacji o środkach zabezpieczających takie dane.

Szkolenie z zakresu ochrony danych osobowych

3.4. Szkolenie podstawowe z zakresu ochrony danych osobowych przeprowadzone może być w formie:

3.4.1. **samokształcenia Pracownika** – w oparciu o materiały szkoleniowe przekazane Pracownikowi w formie elektronicznej lub papierowej, niezwłocznie po zatrudnieniu, przez dział właściwy ds. kadr. W tym przypadku:

3.4.1.1. Pracownik w ciągu kolejnych 2 dni roboczych zapoznaje się z uzyskanymi materiałami szkoleniowymi, a także ma możliwość konsultacji z Inspektorem w sprawie wyjaśnienia niezrozumiałych kwestii poruszonych w materiałach,

3.4.1.2. W ciągu kolejnego dnia roboczego Pracownik podchodzi do testu wiedzy, który udostępniony zostanie mu w formie elektroniczne lub papierowej. Liczba pytań, treść pytań oraz próg zaliczeniowy ustalone zostaną przez Inspektora. Inspektor sprawdza wypełniony przez Pracownika test i przekazuje mu informację zwrotną,

3.4.1.3. W przypadku niezłożenia testu lub nieuzyskania minimalnej liczby punktów, Pracownik może kolejny raz podejść do testu. Po trzech

próbach zakończonych niepowodzeniem, Pracownik zobowiązany jest do ukończenia szkolenia z zakresu ochrony danych osobowych prowadzonego przez Inspektora,

3.4.2. **szkolenia sterowanego** – które realizowane jest przez Inspektora w formie zdalnej lub stacjonarnej (według jego wyboru), gdy liczba nowozatrudnionych Pracowników, którzy powinni zostać przeszkoleni jest nie mniejsza niż 10 osób. Po ukończeniu szkolenia prowadzonego przez Inspektora, Pracownicy kończą test wiedzy – postanowienia punktów 3.4.1.2. – 3.4.1.3. stosuje się odpowiednio.

3.5. Administrator we współpracy z Inspektorem organizuje szkolenia okresowe z zakresu ochrony danych osobowych, które powinny odbywać się regularnie, nie rzadziej niż raz w roku. Plan szkolenia okresowego przygotowuje Inspektor. Do przeprowadzenia szkolenia okresowego stosuje się pkt. 3.4.2.

Nadanie upoważnienia i zobowiązanie do zachowania tajemnicy

3.6. Upoważnienie do przetwarzania danych osobowych nadawane jest przez Administratora lub wyznaczoną przez niego osobę, w formie pisemnej lub elektronicznej, według wzoru określonego w Załączniku nr 2 do Polityki lub w innej formie przyjętej przez Administratora.

3.7. Upoważnienie udzielane jest na czas określony lub nieokreślony. Wygasa ono w każdym przypadku najpóźniej w momencie wygaśnięcia podstawy zatrudnienia lub współpracy z Pracownikiem.

3.8. Pracownik potwierdza, że został poinformowany o udzielonym mu upoważnieniu do przetwarzania danych osobowych, jego zakresie, a także że zobowiązuje się do zachowania tajemnicy danych osobowych oraz środków zabezpieczających takie dane.

3.9. Administrator może w dowolnym momencie cofnąć upoważnienie do przetwarzania danych osobowych przez Pracownika, a także zmodyfikować jego zakres. Czynności te podejmowane są, w szczególności w razie zmiany przez pracownika stanowiska pracy lub zmiany zakresu obowiązków umownych.

3.10. Administrator prowadzi rejestr upoważnień według wzoru określonego w Załączniku nr 3 do Polityki lub w innej formie przyjętej przez Administratora. Rejestr prowadzony jest w formie elektronicznej lub papierowej. Niezależnie od rejestru, Administrator przechowuje wszystkie udzielone upoważnienia w aktach osobowych pracowników lub innych wyznaczonym miejscu, w formie łatwo dostępnej.

Powierzenie przetwarzania danych osobowych

3.11. Administrator może korzystać z usług zewnętrznych podwykonawców, którym zlecać będzie przetwarzanie danych osobowych w swoim imieniu (powierzenie).

3.12. Powierzenie przetwarzania danych osobowych może nastąpić wyłącznie na rzecz podmiotu przetwarzającego, który zapewnia odpowiedni poziom bezpieczeństwa danych osobowych i wyłącznie na podstawie stosownej umowy powierzenia przetwarzania danych.

Weryfikacja podmiotu przetwarzającego dane osobowe

3.13. Przed powierzeniem przetwarzania danych osobowych, Administrator weryfikuje potencjalny podmiot przetwarzający, aby ustalić, czy zapewnia on odpowiedni poziom bezpieczeństwa danych osobowych. W tym celu Administrator lub wyznaczony przez niego dział odpowiedzialny za proces w ramach, którego ma dojść do powierzenia przetwarzania danych, w porozumieniu z Inspektorem, może:

3.13.1. zweryfikować ogólnodostępne informacje, w tym stronę internetową potencjalnego podmiotu przetwarzającą, jego kanały w mediach społecznościowych, czy opinie w Internecie,

3.13.2. zweryfikować dane znajdujące się w publicznych rejestrach, np. CEIDG, PRS, KRS,

3.13.3. zażądać przedłożenia przez potencjalny podmiot przetwarzający dokumentów związanych z gwarantowanym przez niego poziomem bezpieczeństwa danych osobowych, w tym, np. certyfikatów zgodności ISO, certyfikatu zgodności z przepisami o ochronie danych osobowych,

3.13.4. przeprowadzić weryfikację przy pomocy ankiety weryfikacji potencjalnego podmiotu przetwarzającego, poprzez przekazanie jej do potencjalnego podmiotu przetwarzającego, a także przeanalizowanie udzielonych przez ten podmiot odpowiedzi,

3.13.5. przeprowadzenie fizycznego audytu ochrony danych osobowych u potencjalnego podmiotu przetwarzającego.

3.14. W przypadku, gdy weryfikacja potencjalnego podmiotu przetwarzającego odbywa się w sposób określony w punktach 3.13.1 – 3.13.3. lub 3.13.5., osoba odpowiedzialna za dokonanie weryfikacji sporządza z niej notatkę lub raport. Dokument ten wskazywać musi na przeprowadzone czynności i poczynione w ich trakcie uzgodnienia. Dokument taki przechowywany jest przez okres 5 lat od momentu zakończenia współpracy z Podmiotem przetwarzającym, a jeżeli takiej współpracy nie nawiązano – przez okres do 1 roku od przeprowadzenia weryfikacji.

3.15. Jeżeli weryfikacja potencjalnego podmiotu przetwarzającego wskazuje, że nie zapewnia on należytej gwarancji bezpieczeństwa danych osobowych, Administrator nie powierza mu danych osobowych.

Zawarcie umowy powierzenia przetwarzania danych

3.16. Jeżeli weryfikacja potencjalnego podmiotu przetwarzającego wskazuje, że zapewnia on należyte gwarancje bezpieczeństwa danych osobowych, Administrator może powierzyć mu przetwarzanie danych osobowych. Powierzenie odbywa się po wcześniejszym zawarciu umowy powierzenia z Podmiotem przetwarzającym. Wzór umowy powierzenia przetwarzania danych osobowych stanowi Załącznik nr 4 do Polityki. Odstąpienie od wzoru umowy powierzenia przetwarzania danych osobowych wymaga akceptacji Inspektora.

3.17. Umowa powierzenia przetwarzania danych osobowych zawarta może być w formie pisemnej, elektronicznej, a także dokumentowej (np. przez akceptację regulaminu/umowy powierzenia udostępnionej w serwisie internetowym).

3.18. Administrator lub wyznaczona przez niego osoba prowadzi w rejestr wszystkich zawartych umów powierzenia przetwarzania danych osobowych, według wzoru stanowiącego Załącznik nr 5 do Polityki. Ponadto, skan każdej zawartej umowy powierzenia przetwarzania danych osobowych przekazywany jest przez Administratora lub wyznaczoną przez niego osobę do Inspektora w terminie 14 dni od dnia jej zawarcia.

Okresowa weryfikacja podmiotu przetwarzającego

3.19. Właściciel procesu, w którym dochodzi do powierzenia przetwarzania danych, dokonują okresowej weryfikacji Podmiotów przetwarzających z perspektywy utrzymywania odpowiedniego poziomu bezpieczeństwa danych. W tym celu stosuje się odpowiednio postanowienia punktów 3.13. – 3.15.

3.20. Z okresowej weryfikacji podmiotu przetwarzającego sporządza się notatkę lub raport, które przechowywane są wraz z umowa powierzenia przetwarzania danych osobowych, lub odnotowuje się przeprowadzenie tych czynności w rejestrze umów powierzenia przetwarzania danych osobowych.

Udostępnienie danych osobowych

3.21. Administrator może udostępnić dane osobowe podmiotu danych innemu podmiotowi (odbiorcy danych), który nie jest Podmiotem przetwarzającym, w tym uprawnionym organom publicznym oraz innym administratorom.

3.22. Udostępnienie danych osobowych odbywa się z poszanowaniem zasad określonych w pkt. 2.1. Polityki, a także w oparciu o co najmniej jedną z przesłanek legalizujących określonych w art. 6 ust. 1 lub art. 9 ust. 2 RODO, a w szczególności na podstawie:

3.22.1. przepisu prawa zobowiązującego Administratora do udostępnienia danych na rzecz określonego podmiotu,

3.22.2. zgody podmiotu danych na udostępnienie jego danych osobowych na rzecz oznaczonego odbiorcy,

3.22.3. prawnie uzasadnionego interesu Administratora lub strony trzeciej (np. wnioskodawcy),

3.22.4. konieczności realizacji umowy, której strona jest podmiot danych.

3.23. Jeżeli z żądaniem udostępnienia danych osobowych innemu podmiotowi występuje podmiot danych, powinien on złożyć w tym zakresie stosowny wniosek. Wniosek powinien zawierać dane identyfikujące podmiot danych, a także zakres danych osobowych, które mają być udostępnione, podmiot, któremu mają zostać udostępnione i formę ich udostępnienia. Administrator przed realizacją wniosku zobowiązany jest zweryfikować tożsamość podmiotu danych w sposób opisany w punkcie 5.12.

3.24. Jeżeli z żądaniem udostępnienia danych osobowych zwraca się inny wnioskodawca, zobowiązany jest on dostarczyć Administratorowi wniosek wskazujący na tożsamość wnioskodawcy, zakres żądanych danych osobowych, podstawę prawną żądania, sposób udostepnienia danych. Decyzję o udostepnieniu danych osobowych podejmuje Administrator lub wyznaczona przez niego osobę, konsultując się w razie potrzeby z Inspektorem.

3.25. Udostępnienie danych osobowych odbywa się w sposób zapewniający im odpowiednie bezpieczeństwo, w tym ochronę przed nieuprawnionym ujawnieniem. Dane w formie elektronicznej udostępniane są w formie plików zabezpieczonych hasłem, które przesłane zostanie odrębnym kanałem komunikacji (np. sms). Dane w formie pisemnej wydawane są osobiście za potwierdzeniem odbioru albo za pośrednictwem operatora pocztowego – w tym przypadku pakowane są one w dodatkową kopertę stanowiącą ochronę na wypadek uszkodzenia opakowania zewnętrznego.

3.26. Administrator lub wyznaczona przez niego osoba prowadzi rejestr wniosków o udostępnienie danych osobowych według wzoru określonego w Załączniku nr 6 do Polityki. W rejestrze nie odnotowuje się udostępnienia danych osobowych, które następuje z inicjatywy Administratora w ramach realizacji obowiązku prawnego (np. udostępnienia danych osobowych pracownika w ramach zgłoszenia do ubezpieczenia społecznego).

4. INSPEKTOR OCHRONY DANYCH

4.1. Administrator wyznacza Inspektora, a w miarę potrzeby również zastępcę Inspektora, który wspiera Inspektora i wykonuje poniższe zadania w razie nieobecności Inspektora.

4.2. Administrator podaje dane kontaktowe Inspektora na swojej stronie internetowej, a także ogłasza je Pracownikom w formie zwyczajowo przyjętej w swojej organizacji.

Status Inspektora

4.3. Inspektor podlega bezpośrednio Zarządowi i bezpośrednio do Zarządu raportuje swoją pracę.

4.4. Inspektor w wykonywaniu swoich zadań jest niezależny. Administrator ani jego Pracownicy nie mogą wydawać Inspektorowi instrukcji dotyczących wykonywania zadań, jak też nie mogą wywoływać u niego presji zajęcia określonego stanowiska w sprawie. O każdej zidentyfikowanej próbie naruszenia niezależności Inspektor niezwłocznie zawiadamia Zarząd.

4.5. Inspektor uprawniony jest do bezpośredniego kontaktu z Zarządem, a także ze wszystkimi Pracownikami.

4.6. Administrator zapewnia, aby Inspektor był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Dotyczy to informowania Inspektora przede wszystkim o:

- 4.6.1. planowanych, nowych procesach przetwarzania danych lub zmianach w obecnych procesach, np. zmiany formy gromadzenia danych z papierowej na elektroniczną,
- 4.6.2. planowaniu wdrożenia nowych narzędzi związanych z przetwarzaniem danych, np. nowego systemu informatycznego,
- 4.6.3. wpływie żądania od podmiotu danych w zakresie realizacji jego praw wynikających z RODO,
- 4.6.4. wpływie skargi podmiotu danych na nieprawidłowości w procesie przetwarzania danych,
- 4.6.5. każdym zidentyfikowanym naruszeniu ochrony danych osobowych lub podejrzeniu jego wystąpienia,
- 4.6.6. wszelkiej korespondencji od Prezesa Urzędu Ochrony Danych Osobowych, a także o wszelkich kontrolach związanych z procesami przetwarzania danych.

4.7. Inspektor uprawniony jest do wstępu do wszystkich pomieszczeń Administratora, w których dochodzi do przetwarzania danych osobowych, a także do dostępu do wszelkich danych osobowych oraz dokumentacji związanej z ich przetwarzaniem.

4.8. Administrator współpracuje z Inspektorem w zakresie realizacji jego zadań i udziela mu niezbędnego wsparcia, a także zapewnia taką współpracę i wsparcie ze strony Pracowników.

4.9. Inspektor nie może jednocześnie pełnić u Administratora innych funkcji, których pogodzenie mogłoby powodować konflikt interesów, w szczególności nie może on pełnić funkcji członka zarządu, dyrektora, audytora, głównego księgowego.

4.10. Inspektor zobowiązany jest do zachowania tajemnicy związanej z wykonywaniem swojej funkcji.

Zadania Inspektora

4.11. Inspektor realizuje zadania przewidziane w art. 39 ust. 1 RODO, a w szczególności:

4.11.1. informuje Administratora oraz jego Pracowników o obowiązkach, które spoczywają na nich na mocy RODO oraz prawa krajowego i regulacji wewnętrznych w obszarze ochrony danych osobowych, a także udziela im konsultacji i doradztwa w tych sprawach,

4.11.2. monitoruje przestrzeganie przez Administratora oraz Pracowników, przepisów o ochronie danych osobowych i regulacji wewnętrznych w obszarze ochrony danych osobowych, w tym przeprowadza zapowiedziane i niezapowiedziane audyty ochrony danych osobowych,

4.11.3. przeprowadza szkolenia z zakresu ochrony danych osobowych dla Pracowników, a także prowadzi inne działania edukacyjne związane z ochroną danych osobowych,

4.11.4. współpracuje z Prezesem Urzędu Ochrony Danych Osobowych w sprawach związanych z przetwarzaniem danych osobowych przez Administratora i pełni dla tego organu oraz dla osób, których dane dotyczą, funkcje punktu kontaktowego.

4.12. Inspektor odpowiada za przyjmowanie wewnętrznych i zewnętrznych zgłoszeń o naruszeniach ochrony danych osobowych u Administratora.

4.13. Pracownicy mogą kontaktować się bezpośrednio z Inspektorem we wszystkich sprawach związanych z ochroną danych osobowych – telefonicznie lub za pośrednictwem poczty e-mail, a także osobiście w czasie dyżurów Inspektora w siedzibie Administratora.

4.14. Inspektor może wykonywać inne zadania zlecone przez Administratora, o ile nie będą one powodowały konfliktu interesu. Jeżeli Inspektor identyfikuje możliwość takiego konfliktu, odmawia on realizacji zadania i wskazuje Administratorowi okoliczności, które świadczą o możliwości wystąpienia konfliktu interesu.

5. REALIZACJA PRAW PODMIOTÓW DANYCH

5.1. Administrator wdraża zasady realizacji praw podmiotów danych, celem zapewnia sprawnego i efektywnego ich realizowania.

5.2. Celem ułatwienia realizacji praw podmiotów danych i zapewnienia pełnej efektywności procesu, za koordynowanie rozpatrywania takich żądań odpowiada wyznaczona przez Administratora osoba, która:

5.2.1. przyjmuje żądania od podmiotów danych, w tym otrzymuje żądania skierowane do Administratora innymi kanałami komunikacji,

5.2.2. ewidencjonuje żądania podmiotów danych w rejestrze, o którym mowa w pkt. 5.7,

5.2.3. przekazuje żądania do realizacji właściwym działom Administratora, a także wskazuje termin udzielenia przez nie odpowiedzi w zakresie realizacji żądania,

5.2.4. w oparciu o informacje uzyskane od działu właściwego do realizacji żądania, przygotowuje on projekt odpowiedzi na żądanie podmiotu danych, który przekazuje do zatwierdzenia przez Zarząd, a po uzyskaniu akceptacji przekazuje podmiotowi danych.

5.3. Działania, o których mowa w pkt. 5.2. podejmowane są w porozumieniu z Inspektorem, który uprawniony jest do sprawowania nadzoru nad procesem realizacji żądań podmiotów danych.

5.4. Administrator realizuje prawa podmiotów danych bez pobierania opłat. Jeżeli jednak żądanie podmiotu danych ma charakter ustawiczny (np. podmiot danych zwraca się wielokrotnie, w krótkich odstępach czasu, o przekazanie mu kopii danych), Administrator może pobrać rozsądną opłatę wynikającą z administracyjnych kosztów udzielenia informacji, prowadzenia komunikacji oraz podjęcia żądanych działań albo odmówić podjęcia działań związanych z takim żądaniem.

Zasady przyjmowania wniosków podmiotów danych

5.5. Podmiot danych może kierować do Administratora wnioski w zakresie realizacji swoich uprawnień, następującymi kanałami:

5.5.1. **osobiście w siedzibie Administratora** – przez złożenie wniosku na piśmie w sekretariacie albo podanie go do notatki/protokołu sporządzonego przez Pracownika i podpisanego przez podmiot danych. Notatka lub protokół musi obejmować dane identyfikacyjne wnioskodawcy, a także przedmiot żądania oraz sposób, w jaki ma być udzielona odpowiedź,

5.5.2. **korespondencyjnie** – przez złożenie wniosku na adres siedziby Administratora,

5.5.3. **elektronicznie** – przez złożenie wniosku na adres e-mail Administratora lub Inspektora.

5.6. Pracownik lub Inspektor przyjmujący wniosek podmiotu danych niezwłocznie przekazuje go do osoby wyznaczonej przez Administratora, o której mowa w pkt. 5.2.

5.7. Osoba wyznaczona przez Administratora prowadzi rejestr wniosków podmiotów danych według wzoru określonego w Załączniku nr 7 do Polityki. Rejestr prowadzony jest w formie elektronicznej.

Sposób komunikacji z podmiotem danych

5.8. Komunikacja z podmiotami danych związana z przetwarzaniem ich danych osobowych oraz realizowaniem uprawnień przewidzianych w RODO, prowadzona jest przez Administratora w formie zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej, a także prostym i jasnym językiem. W celu zapewnienia takiej komunikacji Administrator dba o to, aby komunikaty do podmiotu danych:

5.8.1. formułowane były w miarę możliwości za pomocą zdań prostych,

5.8.2. nie zawierały zwrotów specjalistycznych, cytowani przepisów aktów prawnych,

5.8.3. dostosowane były do wieku podmiotu danych oraz jego wykształcenia, zawodu,

5.8.4. sporządzane były w estetycznej i łatwej do odczytu formie.

5.9. Administrator prowadzi komunikację z podmiotem danych z wykorzystaniem kanału wskazanego przez taką osobę we wniosku. Jeżeli we wniosku nie wskazano preferowanej formy kontaktu, Administrator prowadzi komunikację z wykorzystaniem tego kanału, przez który złożono wniosek (np. jeżeli wniosek wpłyną na adres e-mail, to komunikacja prowadzona jest drogą e-mail).

5.10. Podmiot danych może działać za pośrednictwem pełnomocnika. W takiej sytuacji pełnomocnik przy pierwszym kontakcie z Administratorem przedkłada pełnomocnictwo w formie oryginału lub uwierzytelnionej kopii.

Weryfikacja tożsamości wnioskodawcy

5.11. Przed realizacją żądania podmiotu danych, w przypadku, gdy brak jest możliwości dokonania jednoznacznej identyfikacji wnioskodawcy lub zaistnienia wątpliwości co do jego tożsamości, w celu zachowania bezpieczeństwa danych osobowych, Administrator zobowiązany jest do zweryfikowania tożsamości składającego żądanie, poprzez zażądanie przekazania przez niego dodatkowych informacji potwierdzających tożsamość.

5.12. Weryfikacja tożsamości może polegać, w szczególności na:

5.12.1. kontroli dokumentu tożsamości okazanego przez wnioskodawcę i porównaniu zawartych w nim danych z danymi posiadanymi przez Administratora,

5.12.2. żądaniu okazania określonych dokumentów,

5.12.3. żądaniu odpowiedzi na pytania weryfikacyjne, np. o numer klienta, numer telefonu powiązany w bazie Administratora z adresem e-mail, czy wysokości ostatniego opłaconego rachunku i formie płatności.

5.13. Jeżeli brak jest możliwości jednoznacznego potwierdzenia tożsamości wnioskodawcy, Administrator informuje go o negatywnej weryfikacji i o braku możliwości realizacji jego żądania.

Termin i treść odpowiedzi na żądanie podmiotu danych

5.14. Administrator rozpatruje wnioski podmiotów danych w terminie miesiąca od ich otrzymania.

5.15. Jeżeli żądanie podmiotu danych ma charakter skomplikowany lub występuje duża liczba żądań, Administrator, po konsultacji z Inspektorem, może przedłuży termin udzielenia odpowiedzi na wniosek o kolejne dwa miesiące. W takim przypadku w terminie miesiąca od otrzymania wniosku informuje on wnioskodawcę o przedłużeniu terminu, wskazując na przyczyny takiego przedłużenia.

5.16. Odpowiedź na żądanie podmiotu danych może polegać na:

5.16.1. zrealizowaniu żądania i poinformowaniu o tym osoby, której dane dotyczą,

5.16.2. poinformowaniu wnioskodawcy o braku możliwości zrealizowania jego żądania z uwagi na brak możliwości jednoznacznego potwierdzenia jego tożsamości,

5.16.3. poinformowaniu wnioskodawcy o odmowie realizacji jego żądania ze wskazaniem przyczyn takiej decyzji i pouczeniem o możliwości wniesienia skargi do Prezesa UODO oraz możliwości skorzystania ze środków ochrony prawnej przed sądem.

5.17. Administrator opracowuje szablony odpowiedzi na żądania podmiotów danych z uwzględnieniem zapewnienia zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formy oraz prostego i jasnego języka.

6. BEZPIECZEŃSTWO DANYCH OSOBOWYCH

6.1. Administrator przetwarza dane osobowe w sposób zapewniający im odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem, uszkodzeniem lub zmodyfikowaniem, za pomocą odpowiednich środków technicznych i organizacyjnych.

Analiza ryzyka

6.2. Administrator przeprowadza ogólna analizę ryzyka dla procesów przetwarzania danych osobowych w organizacji, uwzględniając w tym zakresie ryzyko dla praw lub wolności podmiotów danych, których dane są przetwarzane w ramach takich procesów.

6.3. Przy ogólnej analizie ryzyka Administrator uwzględnia stan wiedzy technicznej, charakter, zakres, kontekst oraz cele przetwarzania, a także ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie. W oparciu o ustalony wynik ryzyka pierwotnego Administrator dobiera adekwatne środki techniczne i organizacyjne, które pozwalają na utrzymanie akceptowalnego poziomu ryzyka lub minimalizacje poziomu nieakceptowalnego. Następnie Administrator ustala wpływ zastosowanych środków technicznych i organizacyjnych na zidentyfikowany poziom ryzyka, po czym podejmuje decyzję o postepowaniu z ryzykiem końcowym, które może zaakceptować, zmniejszyć przez zastosowanie odpowiednich środków lub odrzucić – przez rezygnację z procesu przetwarzania lub jego zmianę.

6.4. Szczegółowa metodyka analizy ryzyka określona jest w Metodyce analizy ryzyka, która stanowi załącznik nr 8 do Polityki.

Ocena skutków dla ochrony danych osobowych (DPIA)

6.5. Administrator przeprowadza ocenę skutków dla ochrony danych osobowych, jeżeli:

6.5.1. ogólna analiza ryzyka wskazuje na **wysokie ryzyko dla praw lub wolności podmiotów danych**, pomimo zastosowanych środków technicznych i organizacyjnych zabezpieczających dane osobowe,

6.5.2. obowiązek przeprowadzenia oceny skutków dla ochrony danych osobowych **wynika z Komunikatu Prezesa UODO** w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony,

6.5.3. planuje **przetwarzanie danych z użyciem nowych technologii**, które ze względu na swój charakter, zakres, kontekst i cele może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

6.6. Jeżeli przeprowadzona przez Administratora ocena skutków dla ochrony danych wykaże, że operacje przetwarzania powodują wysokie ryzyko, którego administrator nie może zminimalizować odpowiednimi środkami technicznymi lub organizacyjnymi, przed przetwarzaniem danych osobowych dokonuje on konsultacji z Prezesem Urzędu Ochrony Danych Osobowych.

Dobór i testowanie środków technicznych i organizacyjnych

6.7. Administrator wdraża techniczne i organizacyjne środki zapewniające bezpieczeństwo danych osobowych w stopniu adekwatnym do zidentyfikowanego ryzyka dla praw i wolności podmiotów danych występującego w procesach przetwarzania.

6.8. Wykaz konkretnych środków stosowanych przez Administratora ujmowany jest w analizie ryzyka.

6.9. Administrator zapewnia regularne testowanie, mierzenie i ocenianie skuteczności wdrożonych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych, a w tym celu:

6.9.1. Inspektor przeprowadza okresowe audyty ochrony danych osobowych i prezentuje ich wyniki Administratorowi,

6.9.2. Administrator zleca informatykowi okresowe przeprowadzenie audytów bezpieczeństwa IT, w tym weryfikowanie czy w wykorzystywanych urządzeniach (np. modemach, drukarkach sieciowych) nie są stosowane domyślne hasła, czy nie występują anomalia w działaniu systemów informatycznych, czy stosowane są najaktualniejsze bazy wirusów,

6.9.3. Administrator lub wyznaczony przez niego informatyk, przeprowadza okresowe kontrole oprogramowania zainstalowanego na urządzeniach służbowych pracowników, w tym weryfikuje ich aktualność i niezbędność do wykonywanych przez Pracownika obowiązków służbowych lub umownych,

6.9.4. Administrator lub Inspektor przeprowadzają wśród Pracowników okresowe ankiety potrzeb w obszarze ochrony danych osobowych, w których Pracownicy mogą ocenić stosowane dotychczas środki bezpieczeństwa i nakreślić problemy związane z ich stosowaniem w codziennej pracy.

Podstawowe zasady bezpieczeństwa IT

6.10. Za bezpieczeństwo systemów informatycznych odpowiada Administrator we współpracy z wyznaczonym informatykiem. Informatyk w porozumieniu z Inspektorem wdraża w organizacji zasady bezpieczeństwa informatycznego, w tym niezbędne procedury. W razie kolizji pomiędzy procedurami bezpieczeństwa informatycznego, a postanowieniami dalsze części punktu 6, pierwszeństwo zastosowania mają postanowienia tych pierwszych.

Użytkownicy systemu informatycznego

6.11. Dostęp do systemu operacyjnego oraz innych systemów informatycznych nadawany jest Pracownikowi (Użytkownikowi) przez informatyka, na wniosek Zarządu i we wskazanym przez Zarząd zakresie, który powinien ograniczony do tych systemów, które są niezbędne do realizacji obowiązków służbowych lub umownych Pracownika. Nadanie dostępu odbywa się przez ustalenie dla Użytkownika loginu i tymczasowego hasła, a także odnotowanie tego faktu w rejestrze upoważnień do przetwarzania danych.

6.12. Pracownikom nadawane są uprawnienia użytkownika zwykłego do systemu informatycznego. Uprawnienia administratora posiadać może jedynie informatyk zarządzający systemami IT w organizacji administratora oraz Zarząd lub wskazane przez niego osoby.

6.13. Użytkownik przy pierwszym logowaniu do systemu zobowiązany jest zmienić hasło tymczasowe. Administrator w miarę dostępnych możliwości wymusza automatyczną zmianę hasła tymczasowego przez system.

6.14. Administrator niezwłocznie odbiera uprawnienia do systemu informatycznego lub zleca ich odebranie informatykowi, w razie zakończenia współpracy z Pracownikiem, a także w razie zmiany zakresu jego obowiązków, które nie wymagają już dostępu do określonego systemu. Zakres dostępów weryfikowany jest przez Administratora lub wskazaną przez niego osobę nie rzadziej niż raz w roku.

Hasła użytkowników i uwierzytelnianie dwuskładnikowe

6.15. Użytkownicy zobowiązani są stosować bezpieczne hasła do systemów informatycznych, które powinny składać się z co najmniej 12 znaków, w tym małych i dużych liter, cyfr oraz znaków specjalnych. Hasła nie powinny zawierać prostych do odgadnięcia kombinacji, np. imienia i nazwiska pracownika, numeru telefonu, nazwy organizacji czy nazwy działu.

6.16. Użytkownicy zobowiązani są zapewnić poufność swoich haseł, a w szczególności nie ujawniać ich innym osobom i nie przechowywać zapisanych w pobliżu komputera lub innego urządzenia, do którego są przeznaczone. W razie utraty poufności hasła, Użytkownik niezwłocznie dokonuje jego zmiany i informuje o tym zdarzeniu informatyka, Administratora oraz Inspektora.

6.17. Użytkownicy stosują w miarę dostępnych funkcjonalności systemów informatycznych dwuskładnikowe uwierzytelnienie – przez włączenie dodatkowej weryfikacji, np. za pomocą hasła i kodu sms lub kodu w aplikacji uwierzytelniającej.

Zasady wykorzystania systemu informatycznego przez Użytkownika

6.18. Pracownicy zobowiązani są wykorzystywać narzędzia pracy udostępnione im przez Administratora, w szczególności służbowy komputer (laptop) oraz smartfon, wyłącznie do celów służbowych. Zabronione jest przechowywanie na takich urządzeniach prywatnych dokumentów lub informacji, a w szczególności informacji i danych niezwiązanych bezpośrednio z zajmowanym stanowiskiem pracy lub pełnioną funkcją.

6.19. Pracownicy zobowiązani są reagować na wszelkie nieprawidłowości w działaniu systemów informatycznych, w tym na pojawiające się komunikaty oprogramowania antywirusowego, poprzez zgłaszanie ich do informatyka współpracującego z Administratorem.

6.20. Pracownicy zobowiązani są zachować ostrożność przy korzystaniu z systemów informatycznych, w szczególności poczty elektronicznej, w tym do nieotwierania załączników nieznanego pochodzenia lub zapisanych w podejrzanych formach (np. .exe, .json). Użytkownicy nie mogą też wchodzić w linki niewiadomego pochodzenia, szczególnie pochodzące od nieznanych nadawców. W razie wątpliwości co do bezpieczeństwa pliku lub załącznika, Pracownik przekazuje wiadomość do informatyka współpracującego z Administratorem.

6.21. Użytkownicy nie mogą samodzielnie instalować, modyfikować ani dezinstalować (usuwać) oprogramowania na służbowych urządzeniach. Operacji takich dokonuje informatyk lub upoważniony pracownik.

6.22. Użytkownicy nie mogą wykorzystywać prywatnych nośników pamięci (np. pendrive) do przechowywania i przenoszenia służbowych plików zawierających dane osobowe. W razie konieczności przeniesienia takich plików, Pracownik wykorzystać powinien służbowy przenośny nośnik pamięci, który będzie zaszyfrowany/zabezpieczony hasłem.

6.23. Pracownik zobowiązany jest zgłaszać do Administratora lub Inspektora każdy przypadek awarii elektronicznego nośnika danych, a także zaginięcie lub kradzież wszelkich nośników danych (dokumentacji papierowej, laptopa, smartfona).

Korespondencja e-mail zawierająca dane osobowe

6.24. Wszelkie załączniki zawierające dane osobowe przesyłane przez Użytkowników za pośrednictwem poczty elektronicznej (e-mail), powinny być zabezpieczone hasłem. Sposób hasłowania plików ustalany jest przez Administratora, który ogłasza go Pracownikom w formie powszechnie przyjętej w swojej organizacji.

6.25. Hasło do zabezpieczonego pliku załączonego do wiadomości e-mail, przesyłane jest za pomocą innego kanału komunikacji, np. za pomocą SMS.

6.26. Użytkownik wysyłając wiadomość e-mail do wielu odbiorców spoza organizacji Administratora, zobowiązany jest wykorzystywać w tym celu opcję UDW (kopia ukryta) i wpisać w to miejsce wszystkie adresy odbiorców, celem nieujawniania ich innym odbiorcom wiadomości.

6.27. Za hasłowanie plików i przekazanie hasła odpowiada pracownik nadający wiadomość e-mail.

7. NARUSZENIE OCHRONY DANYCH OSOBOWYCH

7.1. Administrator wdraża system wykrywania naruszeń ochrony danych osobowych oraz zarządzania takimi naruszeniami, który opisany jest w poniższych postanowieniach.

7.2. Administrator lub wyznaczona przez niego osoba prowadzi w formie elektronicznej rejestr naruszeń ochrony danych osobowych. Wzór rejestru stanowi Załącznik nr 9 do Polityki. W rejestrze odnotowywany jest każdy zidentyfikowany przypadek naruszenia ochrony danych osobowych lub możliwości wystąpienia takiego naruszenia.

Zgłoszenie naruszeń ochrony danych

7.3. Każdy Pracownik jest zobowiązany do **reagowania na wszelkie przejawy negatywnych działań lub zaniechań, które mogą prowadzić do naruszeń ochrony danych osobowych**, w tym do zgłaszania takich działań/zaniechań Administratorowi lub Inspektorowi.

7.4. Jeżeli Pracownik jest świadkiem naruszenia ochrony danych osobowych, powinien on podjąć rozsądne działania celem **wyeliminowania naruszenia lub zminimalizowania jego skutków**, a następnie niezwłocznie powiadomić o nim bezpośredniego przełożonego oraz Inspektora.

7.5. Wszelkie zgłoszenia dotyczące naruszeń ochrony danych osobowych lub podejrzeń takich naruszeń, mogą być przekazywane do Administratora lub Inspektora, na adres poczty e-mail wskazany na stronie tytułowej. Pracownik, który uzyska informacje od osoby trzeciej o możliwości wystąpienia naruszenia ochrony danych, niezwłocznie przekazuje taką informację do Inspektora.

Postępowanie wyjaśniające

7.6. Niezwłocznie po otrzymaniu informacji o naruszeniu ochrony danych osobowych lub możliwości wystąpienia takiego naruszenia, Inspektor wraz z Administratorem podejmują **postępowanie wyjaśniające, którego celem jest ustalenie:**

7.6.1. czy doszło do zdarzenia objętego informacją?

7.6.2. czy zdarzenie dotyczy danych osobowych?

7.6.3. czy do zdarzenia doszło na skutek naruszenia bezpieczeństwa danych?

7.6.4. czy w wyniku zdarzenia doszło lub mogło dojść do utraty poufności, dostępności lub integralności przetwarzanych danych osobowych?

7.7. W przypadku negatywnej odpowiedzi, na którekolwiek z ww. pytań, Administrator podejmuje decyzje w przedmiocie postępowania ze zdarzeniem, w szczególności co do zakwalifikowania go jako **incydentu, czyli zdarzenia, które naruszyło wewnętrzne procedury administratora lub przepisy prawa, ale które nie doprowadziło do naruszenia ochrony danych osobowych.**

7.8. W przypadku pozytywnej odpowiedzi, na wskazane w pkt. 7.6. pytania, Administrator podejmuje dodatkową analizę, celem ustalenia:

7.8.1. jaka była skala naruszenia, w tym ilu osób ono dotyczyło, jakich kategorii danych osobowych, ile czasu trwało i co było jego źródłem, a także kto jest za nie odpowiedzialny i kto brał w nim udział?

7.8.2. jakie jest ryzyko naruszenia praw lub wolności podmiotów danych na skutek naruszenia?

7.8.3. czy zdarzenie jest następstwem czynu zabronionego, a jeżeli tak, to czy zachodzi uzasadnienie dla zawiadomienia o nim organów ścigania?

7.8.4. jakie środki zaradcze można podjąć, aby zminimalizować negatywne konsekwencje naruszenia ochrony danych osobowych?

7.8.5. jakie środki naprawcze i zapobiegawcze można wdrożyć, aby zmniejszyć ryzyko wystąpienia podobnego naruszenia w przyszłości?

7.9. Przy ocenie ryzyka, o którym mowa w pkt. 7.8.2. Administrator uwzględnia przede wszystkim:

7.9.1. kontekst przetwarzania danych, w tym kategorie danych osobowych oraz osób, których te dane dotyczą,

7.9.2. okoliczności naruszenia, w tym czy naruszenie objęło szeroki zakres danych oraz czy dane były wcześniej ogólnodostępne lub nieaktualne,

7.9.3. łatwość identyfikacji osoby, której dane zostały objęte naruszeniem,

7.9.4. okoliczności naruszenia, w tym rodzaj i charakter naruszenia atrybutów bezpieczeństwa danych (poufności, dostępności, integralności).

7.10. Każdy Pracownik zobowiązany jest do współpracy z Administratorem i Inspektorem w zakresie wyjaśniania przyczyn i okoliczności naruszenia ochrony danych, w tym do udzielania im niezbędnych informacji w wyznaczonych przez nich terminach.

7.11. W zależności od ustalonego poziomu ryzyka, o którym mowa w pkt. 7.8.2. Administrator:

7.11.1. jeżeli **nie występuje ryzyko** lub ustalone ryzyko naruszenia praw lub wolności podmiotów danych jest **niskie** – odnotowuje naruszenie w rejestrze, o którym mowa w pkt. 7.2.,

7.11.2. jeżeli **występuje ryzyko** naruszenia praw lub wolności podmiotów danych **(średnie)** – odnotowuje naruszenie w rejestrze, o którym mowa w pkt. 7.2., a także zgłasza naruszenie Prezesowi UODO niezwłocznie, jednak nie później niż w ciągu 72 godzin od momentu stwierdzenia naruszenia, w sposób wskazany w pkt. 7.14 – 7.16,

7.11.3. jeżeli **występuje wysokie ryzyko** naruszenia praw lub wolności podmiotów danych – poza czynnościami, o których mowa w pkt. 7.11.2., bez zbędnej zwłoki zawiadamia on o naruszeniu podmioty danych, których dane zostały objęte naruszeniem w sposób wskazany w pkt. 7.18 – 7.21.

7.12. Każdorazowo po stwierdzeniu naruszenia ochrony danych Administrator w porozumieniu z Inspektorem dokonuje przeglądu i w miarę potrzeby aktualizuje analizę ryzyka, weryfikując czy zagrożenie, które wywołało naruszenie zostało wcześniej zidentyfikowane i czy nie zachodzi potrzeba zwiększenia prawdopodobieństwa jego wystąpienia.

7.13. Inspektor ochrony danych sporządza dokumentację z przeprowadzonego postępowania wyjaśniającego, która obejmuje raport z obsługi naruszenia wraz z niezbędnymi załącznikami, np. notatką pracownika odpowiedzialnego za zdarzenie, dowodami.

Zgłoszenie naruszenia do Prezesa UODO

7.14. W sytuacji, o której mowa w pkt. 7.11.2. (średnie ryzyko naruszenia praw lub wolności podmiotów danych) Administrator w ciągu 72 godzin od momentu stwierdzenia naruszenia zgłasza jego wystąpienie do Prezesa UODO. Momentem stwierdzenia naruszenia jest chwila, w której Administrator zidentyfikował wystąpienie zdarzenia i nabrał wystarczającej pewności, że ma ono charakter naruszenia ochrony danych.

7.15. Administrator współpracuje z Inspektorem w zakresie opracowania treści zgłoszenia naruszenia do Prezesa UODO. Zgłoszenie opracowywane jest na formularzu udostępnionym przez Prezesa UODO na stronie www pod adresem: https://www.biznes.gov.pl/pl/opisy-procedur/-/proc/889 i przesyłane jest do Prezesa UODO w formie tradycyjnej (za pośrednictwem operatora pocztowego, listem poleconym) albo w formie elektronicznej (przez biznes.gov.pl lub ePUAP).

7.16. Jeżeli w ciągu 72 godzin od momentu stwierdzenia naruszenia Administrator nie ma możliwości przekazania Prezesowi UODO wszystkich informacji wymaganych w formularzu, o którym mowa w pkt. 7.15, dokonuje on zgłoszenia wstępnego zawierające ustalone dotychczas informacje, a następnie bez zbędnej zwłoki uzupełnia to zgłoszenie.

7.17. Treść zgłoszenia naruszenia do Prezesa UODO stanowi załącznik do raportu, o którym mowa w pkt. 7.13.

Zawiadomienie podmiotów danych o naruszeniu

7.18. W sytuacji, o której mowa w pkt. 7.11.3. (wysokie ryzyko naruszenia praw i wolności podmiotów danych) Administrator zawiadomią o wystąpieniu naruszenia ochrony danych osobowych podmioty danych, których dane osobowe objęte zostały naruszeniem.

7.19. Zawiadomienie podmiotów danych obejmuje, w szczególności:

7.19.1. nazwę i dane kontaktowe Administratora,

7.19.2. imię i nazwisko oraz dane kontaktowe Inspektora,

7.19.3. opis możliwych konsekwencji naruszenia ochrony danych,

7.19.4. opis środków zastosowanych lub proponowanych do zastosowania w celu zaradzenia naruszeniu ochrony danych osobowych, w tym opis środków w celu zminimalizowania negatywnych skutków naruszenia.

7.20. Administrator może odstąpić od zawiadomienia podmiotów danych o naruszeniu wyłącznie w sytuacji, gdy:

7.20.1. wdrożył on odpowiednie środki techniczne i organizacyjne oraz zastosował je do danych osobowych objętych naruszeniem, które minimalizują ryzyko negatywnych skutków, np. zaszyfrował dane osobowe uniemożliwiając ich odczyt osobom nieuprawnionym,

7.20.2. zastosował następczo środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności podmiotów danych,

7.20.3. wymagałoby to niewspółmiernie dużego wysiłku.

7.21. W sytuacji, o której mowa w pkt. 7.20.3. czyli gdy indywidualne zawiadomienie podmiotów danych o naruszeniu ochrony ich danych osobowych wymagałoby niewspółmiernie dużego wysiłku (np. z uwagi na znaczną liczbę osób albo brak danych kontaktowych), Administrator wydaje publiczny komunikat lub stosuje inny podobny środek, za pomocą którego podmioty danych zostają poinformowane w równie skuteczny sposób. Środkiem takim może być publikacja informacji na stronie internetowej Administratora, w jego mediach społecznościowych lub prasie.

7.22. Treść zawiadomienia podmiotów danych wraz z informacją o sposobie dokonania tego zgłoszenia, stanowi załącznik do raportu, o którym mowa w pkt. 7.13.

8. WSPÓŁPRACA Z ORGANEM NADZORCZYM

8.1. Administrator wdraża zasady współpracy z Prezesem UODO we wszelkich sprawach związanych z przetwarzaniem przez niego danych osobowych. Celem tych zasad jest zapewnienie skutecznego i efektywnego przepływu informacji oraz zapewnienie Prezesowi UODO możliwości efektywnego realizowania zadań wynikających z RODO.

8.2. Za koordynację współpracy z Prezesem UODO u Administratora odpowiada Inspektor. Pracownicy zobowiązani są do współpracy z Inspektorem w celu zapewnienia sprawnego obiegu informacji, przekazywania mu niezbędnych danych oraz udzielania niezbędnych wyjaśnień, a także stosowania się do jego rad i wskazówek związanych z realizacją zadań przez Prezesa UODO.

Komunikacja z Prezesem UODO

8.3. Wszelka korespondencja przychodząca od Prezesa UODO (listowna, mailowa, a także informacje o połączeniach telefonicznych), powinna być niezwłocznie przekazywana na adres e-mail Inspektora wskazany na stronie tytułowej, przez Pracownika przyjmującego taką korespondencję. Przekazanie korespondencji powinno nastąpić nie później niż w ciągu 24 godzin od jej otrzymania.

8.4. Inspektor ustala maksymalny termin udzielenia odpowiedzi na korespondencję Prezesa UODO, a także przygotowuje plan działań niezbędnych do przygotowania odpowiedzi i przekazuje go do Zarządu oraz podejmuje działania niezbędne do realizacji korespondencji.

8.5. Administrator lub wskazany przez niego Pracownik przekazuje Inspektorowi wszelkie informacje niezbędne do zrealizowania pisma Prezesa UODO. W oparciu o uzyskane informacje Inspektor przygotowuje projekt odpowiedzi na pismo Prezesa UODO, które przekazuje do zatwierdzenia i wysłania przez Zarząd.

8.6. Komunikacja z Prezesem UODO prowadzona może być w formie:

8.6.1. **tradycyjnej (papierowej)** – listem poleconym za potwierdzeniem odbioru na adres Urzędu Ochrony Danych Osobowych,

8.6.2. **elektronicznej** – za pośrednictwem ePUAP lub biznes.gov.pl na adres UODO.

8.7. Inspektor prowadzi ewidencję wszelkiej korespondencji prowadzonej z Prezesem UODO.

Kontrola Prezesa UODO

8.8. Administrator po uzyskaniu informacji o planowanej przez Prezesa UODO kontroli, niezwłocznie informuje o tym Inspektora i wspólnie zapewniają zasoby umożliwiające

Prezesowi UODO przeprowadzenie kontroli. W tym celu zapewniają oni Prezesowi UODO lub wyznaczonym przez niego kontrolującym:

8.8.1. wstępu na teren i do lokalu lub innych pomieszczeń Administratora,

8.8.2. w miarę możliwości odrębne pomieszczenie, w którym kontrolujący będzie mógł przeprowadzać czynności,

8.8.3. kopie lub wydruki wskazanych przez kontrolującego dokumentów lub informacji,

8.8.4. dostęp do wszelkich zasobów, które są wykorzystywane do przetwarzania danych.

8.9. W razie kontroli Prezesa UODO w biurze/siedzibie Administratora, Inspektor lub osoba wyznaczona przez Administratora do reprezentowania go w postępowaniu kontrolnym zobowiązana jest:

8.9.1. zażądać okazania przez kontrolującego imiennego upoważnienia wraz z legitymacją służbową, a także zweryfikować czy upoważnienie do kontroli zawiera informacje wymagane przez art. 82 ust. 2 u.o.d.o., t.j.:

8.9.1.1. wskazanie podstawy prawnej przeprowadzenia kontroli,

8.9.1.2. oznaczenie organu kontrolującego,

8.9.1.3. imię i nazwisko, stanowisko służbowe oraz numer legitymacji służbowej kontrolującego,

8.9.1.4. określenie zakresu przedmiotowego kontroli,

8.9.1.5. oznaczenie kontrolowanego (Administratora),

8.9.1.6. wskazanie daty rozpoczęcia i przewidywanego terminu zakończenia czynności kontrolnych,

8.9.1.7. podpis Prezesa UODO,

8.9.1.8. pouczenie kontrolowanego (Administratora) o jego prawach i obowiązkach,

8.9.1.9. datę i miejsce wystawienia upoważnienia,

8.9.2. uczestniczyć w prowadzonych czynnościach kontrolnych, w szczególności w dokonywaniu przez kontrolujących wizji lokalnej, rozmowie z pracownikami, dokonywaniu oględzin dokumentów lub systemów informatycznych,

8.9.3. zapewnienia niezbędnego wsparcia kontrolującemu, w tym realizacji czynności, o których mowa w pkt. 8.8.1. – 8.8.4.

8.10. Jeżeli w toku kontroli kontrolujący zażąda dostępu do danych lub informacji stanowiących tajemnicę przedsiębiorstwa, tajemnice zawodową lub inną tajemnicę prawnie chronioną, Administrator lub osoba reprezentująca go w toku kontroli powinna zazadać odnotowania tego w protokole. W przypadku przekazania kontrolującemu kopii lub odpisów dokumentów zawierających ww. informacje, Administrator przekazuje je w dwóch egzemplarzach:

8.10.1. **pierwszy egzemplarz** – zawierający pełną treść dokumentu, w tym dane/informacje objęte ww. tajemnicami. Egzemplarz ten przekazywany jest w odrębnej kopercie i oznaczany jest tekstem/napisem: „tajemnica przedsiębiorstwa/zawodowa/inna prawnie chroniona" – przy czym niewłaściwy rodzaj tajemnicy należy skreślić,

8.10.2. **drugi egzemplarz** – zanonimizowany o dane/informacje objęte ww. tajemnicami.

8.11. Jeżeli w trakcie kontroli powstaną wątpliwości czy żądanie lub polecenie kontrolującego lub inne podejmowane przez niego działania pozostają w związku z przedmiotem kontroli lub w zgodzie z przepisami prawa, a także, gdy Administrator odmawia spełnienia żądania lub polecenia kontrolującego, należy zadbać o umieszczenie przez niego odpowiedniej informacji w protokole kontroli ze wskazaniem uzasadnienia takiej decyzji.

9. POSTANOWIENIA KOŃCOWE

9.1. Wszelkie kwestie sporne związane z realizacją postanowień Polityki rozstrzygać będzie Zarząd w porozumieniu z Inspektorem. Zarząd jest też upoważniony do stosowania lub zezwalania na zastosowanie odstępstw od Polityki, co odbywać się może jedynie w uzasadnionych wypadkach i powinno być zgłoszone Inspektorowi.

9.2. Polityka wchodzi w życie z dniem przyjęcia jej uchwałą przez Zarząd. W uchwale Zarządu wskazane powinny być osoby wyznaczone do realizacji zadań wskazanych w Polityce. Uchwała wraz z Polityką podawana jest do wiadomości Pracowników w sposób przyjęty u Administratora.

9.3. Wszelkie zmiany Polityki wymagają przyjęcia ich uchwałą Zarządu i ogłoszenia ujednoliconej Polityki Pracownikom Administratora, w sposób przyjęty u Administratora.

9.4. W sprawach nieuregulowanych w Polityce i innych wewnętrznych procedurach, stosuje się przepisy RODO oraz inne przepisy powszechnie obowiązującego prawa.

9.5. Integralną częścią Polityki są następujące załączniki:

Załącznik nr 1A	–	Wzór rejestru czynności przetwarzania danych (RCPD)
Załącznik nr 1B	–	Wzór rejestru kategorii czynności przetwarzania danych (RKCP)
Załącznik nr 2	–	Wzór upoważnienia do przetwarzania danych osobowych
Załącznik nr 3	–	Wzór rejestru nadanych upoważnień do przetwarzania danych osobowych
Załącznik nr 4	–	Wzór umowy powierzenia przetwarzania danych osobowych

		4.1. wzór umowy powierzenia przetwarzania danych osobowych (RR Security Sp z o.o – Administrator) 4.2. wzór umowy powierzenia przetwarzania danych osobowych (RR Security Sp. z o.o. – Podmiot przetwarzający)
Załącznik nr 5	–	Wzór rejestru zawartych umów powierzenia przetwarzania danych osobowych
Załącznik nr 6	–	Wzór rejestru wniosków o udostępnienie danych osobowych
Załącznik nr 7	–	Wzór rejestru wniosków podmiotów danych
Załącznik nr 8	–	Metodyka analizy ryzyka
Załącznik nr 9	–	Wzór rejestru naruszeń ochrony danych osobowych

Załącznik nr 1A. Wzór rejestru czynności przetwarzania danych (RCPD)

L.P.	Nazwa czynności przetwarzania	Cel przetwarzania	Kategorie osób	Zakres danych	Planowany termin usunięcia kategorii danych (jeżeli jest to możliwe)	Kategorie odbiorców	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 (jeżeli jest to możliwe)	Transfer do kraju trzeciego lub organizacji międzynarodowej	
								transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	jeżeli transfer z art. 49 ust. 1 akapit drugi – dokumentacja odpowiednich zabezpieczeń
		Art. 30 ust. 1 pkt b	Art. 30 ust. 1 pkt c	Art. 30 ust. 1 pkt c	Art. 30 ust. 1 pkt f	Art. 30 ust. 1 pkt d	Art. 30 ust. 1 pkt g	Art. 30 ust. 2 pkt e	Art. 30 ust. 1 pkt e
Kolumna1	Kolumna2	Kolumna3	Kolumna4	Kolumna5	Kolumna6	Kolumna7	**Kolumna8**	**Kolumna9**	**Kolumna10**

Załącznik nr 1B. Wzór rejestru kategorii czynności przetwarzania danych (RCPD)

	1	2	3	4	5	6	7	8	9	10	11
L.P.	Kategorie przetwarzań	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Administrator				Czas trwania przetwarzania	Kategorie odbiorców, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi	Podprzetwarzający (podwykonawcy) – jeśli dotyczy	
			Identyfikacja Administratora	Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)	Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)	Inspektor ochrony danych administratora (jeśli powołano)				Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)	Kategorie podpowierzonych przetwarzań
	Art. 30 ust. 2 lit. b	Art. 30 ust. 2 lit. d, art. 32 ust. 1	Art. 30 ust. 2 lit. a					Art. 30 ust. 2 lit. c	Art. 30 ust. 2 lit. c		

Załącznik nr 2. Wzór upoważnienia do przetwarzania danych osobowych

pieczątka lub nazwa firmy

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

numer _____

(niniejsze upoważnienie stanowi polecenie Administratora zgodnie z art. 29 RODO)

....., dn. .....

.....

Zajmowane stanowisko .....

Podlega bezpośrednio .....

1. Niniejszym z dniem ..... nadaję Pani/Panu* ..... upoważnienie do przetwarzania danych osobowych gromadzonych w zbiorach, przetwarzanych w związku z wykonywaniem pracy na wskazanym stanowisku pracy.
2. Upoważnienie dotyczy danych osobowych:

	Zakres upoważnienia do przetwarzania danych osobowych *niepotrzebne wykreślić	Forma przetwarzania	
		Tradycyjna	Elektroniczna
	Nazwa czynności z RCPD lub RECP	wstawić x	wstawić x
1			
2			

3. Upoważnienie wygasa z chwilą rozwiązania umowy o pracę / umowy cywilno-prawnej lub zmiany stanowiska.
4. Jednocześnie zobowiązuje się Panią / Pana do zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobu ich zabezpieczenia.

.....

(data, podpis Administratora)

OŚWIADCZENIE OSOBY UPOWAŻNIONEJ

Niniejszym oświadczam, że:

a. zobowiązuję się do przestrzegania przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, innych przepisów lokalnych oraz wdrożonych wewnętrznych procedur, regulaminów i instrukcji w zakresie ochrony danych osobowych,
b. zobowiązuje się do zachowania poufności, integralności i dostępności danych osobowych do których przetwarzania zostałam/em upoważniona/y zapisanych w dowolnej formie (papier, klisza, nośniki elektroniczne, magnetyczne, optyczne itp.),
c. zostałam/em poinformowana/y, że udostępnianie danych osobowych lub umożliwianie dostępu do nich osobie nieuprawnionej podlega sankcjom przewidzianym w Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych, Ustawie Kodeks Pracy oraz Ustawie Kodeks Cywilny.
d. zobowiązuję się do przestrzegania obowiązujących zasad bezpieczeństwa w miejscu przetwarzania danych osobowych w tym szczegółowych zasad ustalonych w komórce organizacyjnej.
e. treść niniejszego dokumentu zrozumiałem co potwierdzam własnoręcznym podpisem.

.....

(data, podpis Pracownika)

Załącznik nr 3. Wzór rejestru upoważnień do przetwarzania danych osobowych

	1	2	3	4	5	6
Lp.	Nr upoważnienia	Imię i nazwisko osoby upoważnionej	Stanowisko	Data nadania upoważnienia	Data wygaśnięcia upoważnienia	Data wygaśnięcia upoważnienia
Kolumna 1	Kolumna2	Kolumna3	Kolumna4	Kolumna5	Kolumna6	Kolumna7

Załącznik nr 5. Wzór rejestru zawartych umów powierzenia przetwarzania danych osobowych

	1	2	3	4	5	6	7	8	9
Lp.	Data zawarcia umowy	Nazwa podmiotu	Podstawa powierzenia	Zakres powierzonych danych	Cel powierzenia	Czas trwania umowy	Sposób przekazywania danych	Data zakończenia umowy	Data usunięcia danych
Kolumna1	Kolumna2	Kolumna3	Kolumna4	Kolumna5	Kolumna6	Kolumna7	Kolumna8	Kolumna9	Kolumna10

Załącznik nr 6. Wzór rejestru wniosków o udostępnienie danych osobowych

	1	2	3	4	5	6	7	8
Lp.	Data wpłynięcia wniosku	Numer wniosku	Odbiorca danych	Podstawa udostępniania	Cel udostępniania	Zakres	Sposób udostępnienia	Data udostępnienia danych
Kolumna1	Kolumna2	Kolumna3	Kolumna4	Kolumna5	Kolumna6	Kolumna7	Kolumna8	Kolumna9

Załącznik nr 7. Wzór rejestru wniosków podmiotów danych

	1	2	3	4	5	6	7
Lp.	Numer rejestrowy	Data wpłynięcia żądania	Temat żądania	Numer rejestru sprzedaży	Data załatwienia	Sposób realizacji żądania	Kwalifikacja z kontroli zgodności
Kolumna1	Kolumna2	Kolumna3	Kolumna4	Kolumna5	Kolumna6	Kolumna7	Kolumna8

Załącznik nr 9. Wzór rejestru naruszeń ochrony danych osobowych

		Rejestr incydentów bezpieczeństwa i działań korygujących/ zapobiegawczych													
					Skutki			Podjęte działania							
L.p.	Numer	Rodzaj incydentu	Czy zdarzenie	Źródło zgłoszenia	Osoba zgłaszająca incydent	Osoba odpowiedzialna za rozwiązanie incydentu	Odpowiedzialność za wyjaśnienie incydentu	Zapobiegawcze	Korygujące	Dodatkowe uwagi	Data wystąpienia problemu/ incydentu	Data zakończenia problemu/ incydentu	Przyczyna incydentu	Zgłoszenie incydentu	Ocena skuteczności
		Jakiego rodzaju incydent	Czy zdarzenie miało miejsce	Źródło zgłoszenia incydentu	Imię i nazwisko	Imię i nazwisko	Imię i nazwisko	Opisać jakie podjęto działania, aby sytuacja nie powtórzyła się	Opisać jakie podjęto działania, aby zapobiec incydentowi	Opisać jakie podjęto działania zapobiegawcze	Wpisać datę d/m/r	Wpisać datę d/m/r	Podać przyczynę incydentu	Czy incydent został zgłoszony do PUODO	Opisać skuteczność podjętych działań