POLITYKA OCHRONY DANYCH OSOBOWYCH

(Privacy Policy)

SKYRISE SP. Z O.O.

Wersja uaktualniona z dnia 01.02.2019r.

DANE dotyczące rewizji dokumentu:

- Wersja 01. – z dnia 1 czerwca 2018r.

- Wersja 02. – z dnia 1 lutego 2019 r.

Słownik

1. **Administrator** (ADO) – oznacza Administratora Danych Osobowych, którym jest spółka Skyrise Sp. z o.o., prowadząca działalność pod adresem: Sobieskiego 2, 40-082 Katowice, wpisana przez Sąd Rejonowy w Katowicach VIII Wydział Gospodarczy KRS do rejestru przedsiębiorców pod numerem KRS 0000452810, posiadającą nr NIP: 954-274-19-69 oraz nr Regon: 243196124, kapitał zakładowy w całości wpłacony, z siedzibą w Gdańsku, jako podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
2. **Dane osobowe** - – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"), gdzie poprzez możliwą do zidentyfikowania osobę fizyczną rozumie się osobę, 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.
3. **DPIA** – ocena skutków dla ochrony danych osobowych (data protection impact assessment)
4. **Inspektor Ochrony Danych (IOD)** osoba wyznaczona przez Administratora, koordynująca procesy związane z przestrzeganiem zasad ochrony danych osobowych w ramach procesów przetwarzania danych osobowych zachodzących w strukturze Administratora Danych,
5. **Państwo trzecie** -państwo nienależące do Europejskiego Obszaru Gospodarczego
6. **Podmiot przetwarzający** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;
7. **Polityka ochrony** – niniejszy dokument ustanawiający zasady ochrony danych osobowych
8. **Pracownik** – osoba współpracująca z Administratorem na podstawie umowy o pracę lub umowy cywilnoprawnej;
9. **Przetwarzanie danych osobowych** - operacja 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,
10. **RODO** - 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),
11. **UE** – Unia Europejska
12. **Ustawa o ochronie danych** - Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000 ze zm.).

I. Wstęp

Niniejsza Polityka ochrony danych osobowych przedstawia **zasady i procedury przetwarzania danych osobowych w jednostce Administratora**. Określa reguły i wskazówki w sposobie zarządzania danymi oraz mechanizmy ich ochrony i udostępniania innym podmiotom współpracującym z Administratorem.

Wdrożenie niniejszej Polityki ochrony danych oznacza, iż stosuje się ją do wszelkich czynności, stanowiących w myśl RODO, przetwarzanie danych osobowych. W szczególności, bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady ujęte w Polityce.

Rygorowi Polityki podlegają zarówno dane, które Administrator przetwarza jako administrator w rozumieniu RODO, a także dane powierzone Administratorowi do przetwarzania na podstawie umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego oraz dane osobowe, które zostały Administratorowi Danych udostępnione.

Struktura organizacyjna w procesie przetwarzania

Osoby odpowiedzialne

Za przetwarzanie danych osobowych w organizacji i ich ochronę odpowiada Administrator. Zgodnie z postanowieniami RODO i Ustawy o ochronie danych osobowych, na dzień sporządzenia niniejszego dokumentu u Administratora nie powstaje obowiązek powołania IOD.

Za ochronę i bezpieczeństwo przetwarzania danych, w tym zarządzanie ryzykiem w zakresie utrzymania poziomu bezpieczeństwa oraz wprowadzanie mechanizmów kontroli, audytu oraz środków prewencyjnych i naprawczych, w jednostce Administratora odpowiada Dział IT, na czele którego stoi Pracownik: Łukasz Gruchała (lukasz.gruchala@skyrise.tech).

Wszelkie uwagi, pytania lub wątpliwości w zakresie ochrony danych osobowych należy kierować pod adres: it@skyrise.tech

Ponadto, Administrator wyznacza konkretne osoby wewnątrz jednostki odpowiedzialne za należyte zabezpieczenie ochrony w takcie przetwarzania danych oraz osoby upoważnione do podejmowania czynności przetwarzania danych osobowych.

W świetle obowiązujących przepisów, Administrator jest odpowiedzialny w szczególności za:

- zapewnienie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z określonymi zasadami przetwarzania danych osobowych (zgodnie z RODO)
- zapewnienie środków umożliwiających prawidłową realizację praw osób, których dane dotyczą
- prowadzenie rejestru przetwarzania danych osobowych
- wprowadzenie odpowiednich polityk, procedur
- wprowadzenie rejestru kategorii przetwarzania danych osobowych w imieniu innego administratora na podstawie umowy powierzenia
- współpracę z organem nadzorczym
- wdrożenie odpowiednich środków organizacyjnych i technicznych, aby zapewnić stopień bezpieczeństwa odpowiadający istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą,
- zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu oraz osobie, której dane dotyczą w sytuacji zaistnienia przesłanek
- nadawanie upoważnień Pracownikom do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych,
- dokumentowanie wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych.

Osoby upoważnione do przetwarzania danych osobowych

Osoby posiadające nadane przez Administratora danych upoważnienie do przetwarzania danych osobowych zobowiązane są do ich ochrony zgodnie z przepisami powszechnie obowiązującymi i niniejszym dokumentem. Ponadto osoba upoważniona zobowiązana jest do zachowania w tajemnicy informacji o danych osobowych oraz środkach, sposobach ich ochrony i zabezpieczeniach.

Naruszenie obowiązku ochrony danych osobowych m.in. obowiązku zachowania w tajemnicy skutkuje poniesieniem odpowiedzialności karnej oraz stanowi ciężkie naruszenie obowiązków pracowniczych.

Struktura danych w ramach systemu informatycznego Administratora

Administrator opracował usystematyzowany sposób ujęcia danych mieszczących się w systemie informatycznym Administratora (dalej jako „System"), rozumianym jako wszystkich danych dotyczących jednostki Administratora, w tym danych osobowych.

Struktura danych w ramach Systemu uwzględnia podział na kategorię danych oraz ujęcie ich w podsystemach, tj. ustalonych na wewnętrze potrzeby jednostki Administratora podsystemach wobec Systemu, w których znajdują się wykorzystywane przez Administratora usługi podmiotów trzecich, jako systemy zewnętrzne.

Struktura danych w ramach Systemu Administratora stanowi **Załącznik nr 1** do niniejszej Polityki (dokument poufny).

II. POSTANOWIENIA DOTYCZĄCE ZASAD PRZETWRZANIA DANYCH

Zasady przetwarzania danych osobowych

Dane osobowe w jednostce Administratora są przetwarzane zgodnie z zasadami przetwarzania danych osobowych, określonymi w art. 5 RODO, czyli:

- Zgodnie z prawem – tzn. w oparciu o odpowiednią przesłankę przetwarzania, spośród określonych w przepisie art. 6 lub 9 RODO;
- Zgodnie z zasadą rzetelności – tzn. z uwzględnieniem interesów podmiotu, którego dane dotyczą;
- Zgodnie z zasadą przejrzystości – tzn. z ujawnieniem szczegółów dotyczycących zakresu i procesu przetwarzania danych osobie, której dane dotyczą;
- Zgodnie z zasadą ograniczenia celu przetwarzania – tzn. tylko w konkretnych, wyraźnych i prawnie uzasadnionych celach przetwarzania;
- Zgodnie z zasadą minimalizacji danych – tzn. tylko stosowne dane i w zakresie adekwatnym w kontekście tego, co niezbędne dla celów, w których dane są przetwarzane;
- Zgodnie z zasadą prawidłowości – tzn. uwzględniając ich prawidłowość i uaktualnianie w razie potrzeby, usuwając dane nieprawidłowe lub je sprostowując;
- Zgodnie z zasadą ograniczonego przetwarzania – tzn. przechowując w formie umożliwiającej identyfikacje osoby przez okres nie dłuższy, niż ten, który jest niezbędny dla osiągnięcia celów przetwarzania;
- Zgodnie z zasadą integralności i poufności – tzn. zapewniając bezpieczeństwo i ochronę danych podczas każdej z czynności przetwarzania;

Zakres ochrony przetwarzania danych

Ochroną objęte są wszystkie dane osobowe przetwarzane przez Administratora i bez względu od przewidzianej formy (papierowo czy elektronicznie).

Wykaz zbiorów danych stanowi **Załącznik nr 2.** do niniejszej Polityki (dokument poufny).

Zgodnie z przepisami RODO Administrator prowadzi *Rejestr czynności przetwarzania danych osobowych*.

Dane zawarte w Rejestrze obejmują informacje, wymagane przepisami art. 30 RODO, w tym:

- nazwę oraz dane kontaktowe Administratora oraz wszelkich współadministratorów, jeśli tacy zostali ustaleni wobec danej kategorii danych,
- nazwę czynności przetwarzania i wewnętrznej jednostki organizacyjnej,
- cel przetwarzania,
- opis kategorii osób, których dane są przetwarzane, wraz z kategorią danych osobowych,
- podstawa prawna przetwarzania danych,
- wskazanie planowanego terminu usunięcia danych, jeśli jest to możliwe,
- kategorie odbiorców danych (innych niż podmiot przetwarzających),
- gdy dane są przekazywane do państwa trzeciego lub organizacji międzynarodowej, podać należy nazwę tego państwa trzeciego lub organizacji międzynarodowej,
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa wobec tych danych – jeśli jest to możliwe,
- czy na dana czynność przetwarzania danych wymaga przeprowadzenia analizy DPIA (ocena skutków dla ochrony danych) - jeśli tak, wskazać lokalizację raportu z tej analizy;
- dokumentacja odpowiednich zabezpieczeń

Powyższy rejestr prowadzony jest przez Administratora w formie elektronicznej i stanowi informację poufną w jednostce Administratora, ujawnianą jedynie w przypadkach określonych przepisami prawa lub obowiązujących Administratora umów (w szczególności umów w ramach których Administratorowi powierzono przetwarzanie danych osobowych, lub umów z podmiotami, którym Administrator powierzył dalsze przetwarzanie danych osobowych).

W szczególności, w przypadku żądania zgłoszonego przez organ nadzoru, Administrator niezwłocznie ujawnia prowadzony przez siebie rejestr.

Dopuszczenie osób do przetwarzania danych osobowych

Dostęp do danych osobowych w ramach wewnętrznej struktury jednostki Administratora, udzielany jest wyłącznie osobom, które uzyskały pisemne, uprzednie i stosowne upoważnienie do przetwarzania danych osobowych, w systemie informatycznym lub w ramach dokumentacji papierowej.

Upoważnienie do przetwarzania danych osobowych nadawane jest po przeprowadzeniu szkolenia lub zaznajomieniu w innej formie, osoby upoważnianej co do zasad ochrony danych osobowych obowiązującymi w strukturze Administratora Danych, ze szczególnym uwzględnieniem odniesienia się do danych, których dotyczy upoważnienie.

Upoważnienia do przetwarzania danych osobowych są indywidualne oraz wskazują zbiory danych objęte upoważnieniem.

Wzór upoważnienia do przetwarzania danych osobowych wraz z zobowiązaniem do zachowania poufności wraz z oświadczeniem o zapoznaniu się z zasadami ochrony danych osobowych stanowi **Załącznik nr 3.** do Polityki.

Upoważnienia do przetwarzania danych osobowych rejestrowane są **Ewidencji osób upoważnionych** do przetwarzania danych osobowych, która stanowi **Załącznik nr 4.** do niniejszej Polityki (dokument poufny).

Administrator może dopuścić do przetwarzania danych osobowych poza jednostką Administratora, w jednej z poniższych form:

1. Udostępnienia danych osobowych (Administrator jako administrator - administratorowi)
2. Powierzenia danych osobowych (Administrator jako administrator – podmiotowi przetwarzającemu „na zlecenie")
3. Dalszego powierzenia danych osobowych (Administrator jako podmiot, któremu powierzono przetwarza dane – dalszemu podmiotowi, który będzie przetwarzał te dane na takich samych warunkach, jak je pierwotnie powierzono)

Udostępnienie danych osobowych

Administrator realizując przepisy prawa i niniejszą Politykę dopuszcza, by dane osobowe, których jest administratorem były **przekazywane innym administratorom** w formie udostępnienia danych.

Udostępnienie danych osobowych może nastąpić tylko w oparciu o co najmniej jedną przesłankę spośród wskazanych w art. 6 RODO i/lub art. 9 RODO.

Podmioty lub kategorie podmiotów, którym udostępnia się dane osobowe muszą zostać obligatoryjnie wskazane w rejestrze czynności przetwarzania danych osobowych.

Powierzenie danych osobowych

Administrator może, na zasadach określonych przepisami RODO i Ustawy oraz niniejszej Polityki, **powierzyć dane osobowe, których jest administratorem do przetwarzania podmiotowi zewnętrznemu** na podstawie zawartej umowy powierzenia danych osobowych, jeśli następuje do w celach (i w interesie) przetwarzania przynależnych Administratorowi.

Przed powierzeniem przetwarzania danych osobowym Podmiotowi przetwarzającemu niezbędne jest poddanie tego podmiotu analizie pod kątem prawidłowości przetwarzania danych osobowych zgodnie z przepisami powszechnie obowiązującymi.

Umowa powierzenia przetwarzania danych osobowych powinna odpowiadać postanowieniom art. 28 RODO tj. winna określać:

- Przedmiot powierzenia
- Czas trwania powierzenia
- Charakter i cel przetwarzania danych
- Rodzaj powierzanych danych
- Kategorie osób, których danych dotyczą
- Warunki pod-powierzenia przetwarzania danych
- Obowiązki i prawa Administratora danych
- Obowiązki podmiotu przetwarzającego

Umowa powierzenia danych osobowych może zostać zawarta w formie pisemnej, w tym również elektronicznej. Umowa powierzenia przetwarzania danych osobowych podpisywana jest zgodnie z zasadami reprezentacji Administratora Danych lub udzielonymi pełnomocnictwami.

Powierzenie danych osobowych winno obligatoryjnie zostać odnotowane w rejestrze czynności przetwarzania danych osobowych Administratora.

Administrator Danych na prawo dokonać kontroli podmiotu przetwarzającego na zasadach określonych w umowie powierzenia danych osobowych.

Administrator Danych może również przetwarzać dane osobowe podmiotów, na rzecz których świadczy usługi. Przyjęcie danych winno również poprzedzać zawarcie umowy powierzenia danych osobowych oraz zostać odnotowane w rejestrze kategorii czynności przetwarzania danych osobowych.

Ponadto na zasadzie wskazanej w art. 28 ust 2. RODO podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora Danych na pod-powierzenie. Szczegółowe zasady ewentualnego podpowiedzenia winny zostać uregulowane w umowie powierzenia lub w osobnym dokumencie sporządzonym w formie pisemnej, w tym również elektronicznej.

Przekazywanie danych osobowych do państw trzecich

W przypadku przekazywania danych osobowych posiadanych przez Administratora do państwa trzeciego lub organizacji międzynarodowej konieczne jest wypełnienie warunków określonych w Rozdziale V RODO. Wskazany warunek dotyczy również podmiotu przetwarzającego dane.

Przekazanie danych do państw trzecich lub organizacji międzynarodowej może mieć formę udostępnienia danych, jak i powierzenia danych osobowych. Dla takich działań konieczne jest również wypełnienie zapisów niniejszego dokumentu.

Przekazanie danych osobowych, w posiadaniu których jest Administrator Danych do państwa trzeciego może nastąpić w sytuacji, jeżeli Komisja Europejska wydała decyzję, że dane państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.

W razie braku decyzji Komisji Europejskiej Administrator może przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie gdy podmiot ten zapewni iż posiada odpowiednie zabezpieczenia i pod warunkiem, że obowiązują prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej. Odpowiednie zabezpieczenia Administrator Danych może zapewnić, bez konieczności uzyskania zezwolenia ze strony organu nadzorczego, za pomocą:

- prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi,
- wiążących reguł korporacyjnych zatwierdzonych przez organ nadzorczy, mających zastosowanie do każdego z członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą,
- standardowych klauzul ochrony danych przyjętych lub zatwierdzonych przez Komisję Europejską,
- standardowych klauzul ochrony danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję Europejską,
- zatwierdzonego kodeksu postępowania wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą, lub
- zatwierdzonego mechanizmu certyfikacji wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą.

Z zastrzeżeniem zezwolenia właściwego organu nadzorczego odpowiednie zabezpieczenia, o których powyżej Administrator Danych może zapewnić w szczególności za pomocą:

- klauzul umownych między Administratorem Danych lub podmiotem przetwarzającym a Administratorem Danych, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej, lub

- postanowień uzgodnień administracyjnych między organami lub podmiotami publicznymi, w których przewidziane będą egzekwowalne i skuteczne prawa osób, których dane dotyczą.

W przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony wydawanej przez Komisję Europejską lub braku odpowiednich zabezpieczeń wskazanych powyżej, w tym wiążących reguł korporacyjnych, jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej jest możliwe jedynie pod warunkiem, że:

- osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którymi może się dla niej wiązać proponowane przekazanie, wyrazi na nie wyraźną zgodę,
- przekazanie jest niezbędne do wykonania umowy zawartej z osobą, której dane dotyczą,
- przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą,
- przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,
- przekazanie jest niezbędne ze względu na posiadane roszczenia,
- przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą lub
- przekazanie nastąpi z publicznego rejestru.

Współadministrowanie danymi osobowymi.

W zakresie swojej działalności Administrator Danych dopuszcza możliwość przyjęcia współadministrowania danymi osobowymi z innym podmiotem/podmiotami.

Współadministrowanie danymi zachodzi wówczas, gdy co najmniej dwóch administratorów podejmuje decyzje dotyczące celów i środków przetwarzania danych. Podmioty zarządzające danymi osobowymi na poziomie współadministrowania powinny spełniać trzy warunki:

- na zasadzie art. 4 pkt 7 RODO być administratorem danych
- wspólnie ustalać cele przetwarzania danych osobowych,
- wspólnie ustalać techniczne i organizacyjne sposoby przetwarzania danych osobowych.

Współadministratorzy danych w drodze wspólnych uzgodnień **określają w sposób przejrzysty zakresy swojej odpowiedzialności**, w odniesieniu do wypełniania obowiązków wynikających z RODO.

Obowiązek informacyjny

Każdorazowo wobec osób, których dane podlegają przetwarzaniu w jednostce Administratora wypełnia się obowiązek informacyjny, w formule Klauzuli Informacyjnej, przekazując dane zgodnie z przepisami RODO.

- Klauzula informacyjna dla pracownika – stanowi **Załącznik nr 5**
- Klauzula informacyjna dla zleceniodawcy- stanowi **Załącznik nr 6**
- Klauzula informacyjna dla klienta (użytkownika systemu Skyrise) - stanowi **Załącznik nr 7**

III. POSTANOWIENIA DOTYCZĄCE BEZPIECZEŃSTWA PRZETWRZANIA DANYCH

Ogólne zasady bezpieczeństwa ochrony danych osobowych

1. Dostęp do danych osobowych mają jedynie pracownicy lub osoby współpracujące z Administratorem Danych na podstawie stosunku prawnego innego niż umowa o pracę (dalej pracownicy) tylko i wyłącznie na podstawie udzielonego upoważnienia do przetwarzania danych.
2. Osoby nieuprawnione do przebywania w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne jedynie w obecności osoby posiadającej upoważnienie.
3. Pracownicy zobowiązani są do zachowania w tajemnicy wszelkich informacji o przetwarzanych danych osobowych w tym również o środkach stosowanych do zabezpieczeń i sposobach ich ochrony.
4. Pracownicy zobowiązani są do zabezpieczenia dokumentów, materiałów zawierających w swojej treści dane osobowe i nie udostępniania ich osobom nie upoważnionym. Ponadto zabronione jest udzielanie informacji dotyczących danych osobowych innym podmiotom na podstawie próśb w jakiejkolwiek formie (pisemnej, telefonicznej, ustnej itd.) bez ważnej podstawy prawnej.
5. Niedopuszczalnym jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych.
6. Hasła i identyfikatory służące pracownikowi do indywidualnego logowania do systemu informatycznego lub innego w miejscu pracy nie może być udostępnione innej osobie.
7. Wiadomości wysyłane do wielu osób wymaga zastosowania opcji „kopia ukryta”.
8. Pracownicy zobowiązani są w miejscu pracy do stosowania zasady tzw. „czystego biurka”, która cechuje się niepozostawianiem materiałów, dokumentów zawierających dane osobowe w miejscu, w którym osoby nieupoważnione mogą mieć dostęp do danych. Ponadto pracownicy zobowiązani są do niszczenia notatek na brudno, błędnych lub zbędnych kopii dokumentacji w sposób uniemożliwiający jej odtworzenie np. poprzez użycie niszczarki.
9. W czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe.
10. Po zakończeniu pracy w systemie informatycznym, w którym przetwarzane są dane osobowe należy się z niego skutecznie wylogować.

Audyt zgodności przetwarzania danych osobowych

Audyt zgodności przetwarzania danych osobowych przeprowadzany jest w celu sprawdzenia stosowanych w jednostce organizacyjnej Administratora rozwiązań technicznych i organizacyjnych służących przetwarzaniu i ochronie danych osobowych, pod kątem skuteczności oraz spełnienia wymogów wynikających z przepisów przez osobę wyznaczoną przez Administratora.

Audyt przeprowadzany jest raz do roku w pierwszym kwartale danego roku, przez osobę wybraną przez Administratora mającą stosowną wiedzę i kompetencje, na podstawie udzielanego upoważnienia. Audytor sporządza pisemny raport z dokonane sprawdzenia i zgodności przetwarzania danych osobowych w audytowanej jednostce.

Wzór Upoważnienia do przeprowadzenia audytu stanowi Załącznik nr 8.

Osoba upoważniona do przeprowadzenia audytu dokumentuje czynności przeprowadzone w toku sprawdzenia, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Dokumentowanie może polegać w szczególności na

utrwaleniu danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych na informatycznym nośniku danych lub dokonaniu wydruku tych danych oraz na:

- sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
- odebraniu wyjaśnień osoby, której czynności objęto sprawdzeniem;
- sporządzeniu kopii otrzymanego dokumentu;
- sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;
- sporządzeniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu;

Raport z przeprowadzonego audytu winien zostać sporządzony niezwłocznie po zakończeniu audytu, - nie później jednak niż w terminie 1 miesiąca - oraz zawierać co najmniej:

- oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania;
- datę i miejsce sprawozdania
- imię i nazwisko administratora bezpieczeństwa informacji (jeśli został powołany);
- wykaz czynności podjętych przez osobę upoważnioną do przeprowadzenia audytu w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach;
- datę rozpoczęcia i zakończenia audytu;
- określenie przedmiotu i zakresu audytu;
- opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
- stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem;
- rekomendacje do ulepszenia procesów przetwarzania danych lub zachowania bezpieczeństwa takiego przetwarzania;
- wyszczególnienie załączników stanowiących składową część Raportu;
- podpis osoby upoważnionej do przeprowadzenia audytu informacji,

Raport może być sporządzony w postaci elektronicznej albo w postaci papierowej.

W razie uwag zamieszczonych w Raporcie w zakresie stwierdzonych naruszeń, Administrator winien zapewnić niezwłoczne działania przywracające stan zgodny z prawem oraz wprowadzające środki zaradcze co do ponownego zaistnienia naruszenia, a po ich dokonaniu i Audytor winien otrzymać sprawozdanie z ich dokonania, oraz potwierdzić stan usunięcia naruszenia.

Osoba upoważniona do sporządzenia Raportu współpracuje z Administratorem aż do zakończenia działań naprawczych i zatwierdzenia stanu braku naruszeń, które winno być przekazane Administratorowi w takiej samej formie jak Raport, nie później niż w terminie 30 dni od zakończenia pierwotnego audytu.

Ocena skutków dla ochrony danych osobowych (Data Protection Impact Assessment)

Administrator na zasadach określonych przepisami RODO, oraz w wykazaniu wypełnienia obowiązku rozliczalności, dokonuje oceny skutków dla ochrony danych osobowych w celu opisania przetwarzania danych osobowych oraz oceny, konieczności i proporcjonalności.

Arkusz oceny skutków (DPIA) dla ochrony danych osobowych stanowi **Załącznik nr 9.** do niniejszej Polityki.

Incydent wobec ochrony danych osobowych

Administrator Danych osobowych jest podmiotem odpowiedzialnym za bezpieczeństwo przetwarzanych danych osobowych. Aby zapobiec naruszeniom Administrator czynnie przeciwdziała dostępowi osób niepowołanych do pomieszczeń oraz systemów, w których przetwarzane są dane osobowe oraz podejmowania działań w przypadku wystąpienia naruszeń ochrony danych osobowych.

- W przypadku podejrzenia naruszenia danych osobowych w jednostce Administratora uruchomiona zostaje **wewnętrzna procedura zaradcza**, mająca na celu podjęcie działań zaradczych i usunięciu zagrożenia naruszenia ochrony danych osobowych.

  Administrator przewiduje zastosowanie działań według ujednoliconej procedury działań zaradczych, jak opisano w **Załączniku nr 10** (dokument poufny).

- W przypadku naruszenia ochrony danych osobowych Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – **zgłasza je organowi nadzorczemu**. W przypadku przekroczenia 72 godzinnego terminu do zgłoszenia załącza się wyjaśnienie przyczyn opóźnienia.

  Zgłoszenie przypadku naruszenia ochrony danych powinno zawierać co najmniej:

  - opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorię i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
  - zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
  - opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
  - opisywać środki zastosowane lub proponowane przez Administratora Danych w celu zaradzeniu naruszenia ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków

Administrator może odstąpić od zgłoszenia przypadku naruszenia organowi nadzorczemu, w sytuacji gdy mało prawdopodobne jest, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

Wzór dla Rejestru przypadków naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania danych osobowych stanowi **Załącznik nr 11** (dokument poufny).

Realizacja paw osób, których dane dotyczą

Administrator Danych uwzględnia w zachodzących w jego strukturze procesach przetwarzania danych osobowych, procedury i zasady ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy przepisów RODO, w tym, w szczególności:

- prawo do wycofania wyrażonej zgody (art. 7 ust. 3 RODO),
- prawo dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO),
- prawo do sprostowania danych (art. 16 RODO),
- prawo do usunięcia danych (prawo do bycia zapomnianym) (art. 17 RODO),
- prawo do ograniczenia przetwarzania (art. 18 RODO),
- prawo do przenoszenia danych (art. 20 RODO),
- prawo sprzeciwu (art. 21 RODO),
- prawo do niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu (art. 22 RODO).

Mając na względzie profesjonalne działanie i należyte wykonywanie praw wobec osób, które się zgłaszają do Administratora, przewiduje się zastosowanie działań według ujednoliconej wewnętrznie procedury działań dla wykonania praw osób, które wniosły o realizację przysługującego im prawa, jak opisano w Załączniku nr 12 (dokument poufny).

Ochrona danych osobowych w fazie projektowania oraz domyślna ochrona danych osobowych

Administrator Danych uwzględnia ochronę danych osobowych i prywatności na każdym etapie tworzenia oraz istnienia technologii obejmującej ich przetwarzanie. Oznacza to, iż zasady ochrony prywatności będą „wbudowane" w każdy projekt zakładający przetwarzanie danych osobowych w taki sposób, aby od samego początku jego istnienia ochrona prywatności stanowiła jego część składową. Dodatkowo ustawienia aplikacji czy systemów przetwarzających dane domyślnie powinny udostępniać minimalną ilość informacji o użytkowniku.

Wdrażając odpowiednie środki techniczne i organizacyjne Administrator Danych uwzględnia

- stan wiedzy technicznej
- koszt wdrożenia
- charakter, zakres, kontekst i cele przetwarzania danych
- ryzyko naruszenia praw lub wolności osób fizycznych o różnych prawdopodobieństwie wystąpienia i wadze zagrożenia wynikającego z przetwarzania.

Zastosowane środki techniczne i organizacyjne zapewniają również aby dane osobowe nie były udostępniane nieokreślonej licznie osób.

Administrator Danych wykazuje iż spełnia swoje obowiązki odpowiednio je dokumentując np. w formie notatki, maila, raportu, wydruku z systemu.

Przeglądy i aktualizacji Polityki Ochrony Danych Osobowych

Osoba upoważniona przez Administratora Danych dokonuje raz w roku okresowego przeglądu niniejszej Polityki pod kątem jej adekwatności w stosunku do procesów funkcjonujących w strukturach Administratora Danych oraz obowiązujących przepisów prawa odnoszących się do ochrony danych osobowych. W ramach przeglądu uwzględnia się:

1. wyniki Raportu z corocznego audytu;
2. rekomendacje wynikające z odnotowanych przypadków zagrożenia wystąpienia naruszenia ochrony danych oraz przypadków zaistniałego naruszenia ochrony danych osobowych;

Ponadto weryfikacji Polityki dokonuje się niezwłocznie w przypadku zmian przepisów prawa, a także w innych okolicznościach uzasadnionych specyfiką funkcjonowania jednostki Administratora.

Załączniki

Załącznik nr 1 Struktura danych (poufne)

Załącznik nr 2 Wykaz zbiorów danych (poufne).

Załącznik nr 3 Wzór upoważnienia do przetwarzania danych osobowych ze zobowiązaniem do zachowania poufności

Załącznik nr 4 Ewidencja osób upoważnionych do przetwarzania danych osobowych (poufne)

Załącznik nr 5 Klauzula informacyjna dla pracownika (poufne)

Załącznik nr 6 Klauzula informacyjna dla zleceniobiorcy (poufne)

Załącznik nr 7 Klauzula informacyjna dla klienta (poufne)

Załącznik nr 8 Wzór upoważnienia do przeprowadzenia audytu zgodności przetwarzania danych i sporządzenia Raportu

Załącznik nr 9 Wzór Arkusza oceny skutków dla ochrony danych osobowych (DPIA)

Załącznik nr 10 Procedura działań zaradczych w przypadku zagrożenia naruszenia (poufne)

Załącznik nr 11 Wzór Rejestru przypadków naruszeń lub zagrożenia naruszeń ochrony przetwarzania

Załącznik nr 12 Wzór Raportu z audytu

Załącznik nr 13 Procedura wykonania praw osób, które wniosły o realizację przysługującego im prawa (poufne).

Załącznik nr 3

....
(oznaczenie pracodawcy) (miejscowość i data)

UPOWAŻNIENIE
do przetwarzania danych osobowych

1. Niniejszym z dniem . . . . . nadaję Pani/Panu*). . . . . zatrudnionemu przez Administratora danych tj. . . . . . na stanowisku . . . . . w zakresie pełnionych obowiązków służbowych, upoważnienie do przetwarzania danych osobowych gromadzonych w następujących zbiorach:
   - .....
   - .....
   - .....
   - .....

   Upoważnienie dotyczy danych osobowych w zakresie następujących kategorii danych:
   - .....
   - .....
   - .....
   - .....
2. Upoważnienie wygasa z chwilą rozwiązania umowy o pracę lub zmiany stanowiska pracy.
3. Jednocześnie zobowiązuję Panią/Pana*) do zachowania w tajemnicy informacji o przetwarzanych danych osobowych oraz sposobach ich zabezpieczenia.

....
podpis osoby reprezentującej Administratora Data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi u Administratora Danych osobowych. Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

.....
Data i podpis osoby upoważnionej

Załącznik nr 8

....
(oznaczenie Administratora) (miejscowość i data)

Upoważnienie do przeprowadzenia audytu zgodności przetwarzania danych osobowych w jednostce organizacyjnej Administratora oraz sporządzenia Raportu z audytu

Administrator Danych osobowych .....
(dane Administratora)

.....

upoważnia .....
(imię i nazwisko, stanowisko)

Do przeprowadzenia audytu zgodności przetwarzania danych osobowych u Administratora danych osobowych zgodnie z zasadami określonymi w Polityce Ochrony Danych Osobowych obowiązującej u Administratora.

Upoważnienie jest ważne przez okres zatrudnienia osoby upoważnionej/Upoważnienie jest jednorazowe.

.....
Data i podpis Administratora

Załącznik nr 12

…… ……
(oznaczenie Administratora) (miejscowość i data)

Raport ze sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w Skyrise Sp. z o.o.

……

(podać pełną nazwę oraz adres)

Imię i nazwisko osoby upoważnionej do przeprowadzenia audytu zgodności przetwarzania danych osobowych i sporządzenia sprawozdania:

……

1. Wykaz czynności podjętych przez osobę upoważnioną w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach:

……

……

……

……

……

……

……

……

……

……

……

……

……

……

2. Datę rozpoczęcia i zakończenia sprawdzenia:

……

3. Określenie przedmiotu i zakresu sprawdzenia:

……

……

4. Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych:

……

……

……

……

……

……

……

……

……

……

……

……

5. Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem:

……

……

……

……

6. Wyszczególnienie załączników stanowiących składową część Raportu:

……

……

……

……

Data, podpis osoby upoważnionej do przeprowadzenia audytu

Załącznik nr 11

Administrator: *Skyrise Sp. z o.o.*

REJESTR

przypadków naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania danych osobowych

Data zgłoszenia Naruszenia (dzień i godzina)	Zgłaszający	Rodzaj naruszenia	Miejsce naruszenia	Opis naruszenia	Skutki naruszenia	Czy naruszenie podlega zgłoszeniu do organu nadzorczego	Czy naruszenie podlega zgłoszeniu osobie, której dane dotyczą	Podjęte działania – sposób usunięcia naruszenie	Data zakończenia czynności