POLITYKA OCHRONY DANYCH OSOBOWYCH

ADMINISTRATOR:

TREVI APARTMENTS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Adres siedziby: ul. Bukowa 24, 43-100 Tychy

wpisana do KRS za numerem 0000937417, NIP 6462992743, Regon 520634216

Data wprowadzenia:	01.2025r.
Wersja:	1/2025r.
Daty aktualizacji:	co 12 miesięcy
Zatwierdził:	Martin Mokwa-Prezes Zarządu

rodo@mq.energy; www.bukowa.tychy.pl

SPIS TREŚCI

1. CEL I ZAKRES STOSOWANIA POLITYKI OCHRONY DANYCH OSOBOWYCH

Polityka ochrony danych osobowych (*dalej PODO)* została zatwierdzona przez Zarząd Spółki i wdrożona niezwłocznie do przestrzegania firmie od 01 stycznia 2025 r.

Polityka ochrony danych osobowych w przedsiębiorstwie **MQ Energy Spółka z ograniczoną odpowiedzialnością,** Adres siedziby: ul. Bukowa 24, 43-100 Tychy, wpisana do KRS za numerem 0000937417, NIP 6462992743, Regon 520634216 (*dalej Administrator),* została wprowadzona celem dostosowania zasad, technik, metod i sposobów ochrony danych osobowych zgodnie z obowiązującymi przepisami prawa krajowego i unijnego.

Celem wprowadzonej regulacji jest stworzenie dokumentu zawierającego spójne, całościowe, pełne i aktualne zestawienie stosowanych metod ochrony danych osobowych w procesie ich przetwarzania lub powierzenia.

2. OBOWIĄZYWANIE POLITYKI

Zakres danych:

Polityka ochrony danych osobowych dotyczy wszystkich danych, które są przetwarzane przez Administratora niezależnie od formy i sposobu ich uzyskania. Dotyczy w szczególności danych bezpośrednio przetwarzanych (zbieranych, gromadzonych), powierzonych na mocy umów powierzenia oraz takich, które Administrator uzyskał z innego źródła (nawet w sposób nieuprawniony, z jawnych rejestrów, poprzez podanie przez podmioty trzecie). Bez względu na źródło pochodzenia danych osobowych Polityka obowiązuje Administratora co do wszystkich danych, także tych uzyskanych przed dniem nowelizacji przepisów o ochronie danych z maja 2018r i wejściem w życie RODO.

Do kogo stosujemy:

Polityka ochrony danych osobowych obowiązuje wszystkie podmioty (osoby, podmioty współpracujące), które przetwarzają dane osobowe administrowane lub procesowane przez Administratora, bez względu na charakter zatrudnienia lub współpracy tych osób (umowa o pracę, zlecenie, współpracę, dzieło).

Wszystkie podmioty (osoby, przedsiębiorstwa), z którymi nie zawarto umowy powierzenia danych osobowych, a wykonujące swoje działania na podstawie upoważnienia do przetwarzania danych osobowych lub upoważnienia do przebywania w miejscu przechowywania danych osobowych, mają obowiązek stosowania Polityki.

Zakres stosowania:

Polityka ochrony danych osobowych obowiązuje do wszystkich procesów przetwarzania danych osobowych u Administratora. Bez względu na formę działań dokonywanych na danych osobowych, PODO jest obligatoryjnie stosowana i wdrożona. Nawet działania zmierzające do incydentalnego, jednorazowego, działania na danych osobowych (np. usunięcia trwałego danych osobowych) są objęte Polityką.

Słowniczek pojęć:

1. Administrator – osoba fizyczna lub prawna który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych - w rozumieniu art. 4 pkt. 7 Rozporządzenia,
2. Administrator Systemów Informatycznych (ASI) – osoba wyznaczona przez Administratora, koordynująca działania związane z zapewnieniem bezpieczeństwa systemów informatycznych, w tym również odpowiadająca za nadzór nad zabezpieczeniem danych osobowych przetwarzanych w systemach informatycznych wykorzystywanych przez Administratora,
3. Dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej - w rozumieniu art. 4 pkt. 1 Rozporządzenia,
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,
5. Naruszenie ochrony danych osobowych - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do danych osobowych- w rozumieniu art. 4 pkt. 12 Rozporządzenia,
6. Organ nadzorczy – niezależny organ publiczny w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii, powołany w każdym państwie członkowskim Unii, którego podstawowym zadaniem jest monitorowanie stosowania RODO,
7. Państwo trzecie – państwo nienależące do Europejskiego Obszaru Gospodarczego.
8. Podmiot przetwarzający – osoba fizyczna lub prawna, która przetwarza dane osobowe w imieniu Administratora - w rozumieniu art. 4 pkt. 8 Rozporządzenia,
9. Przetwarzanie – operacja lub zestaw operacji wykonywanych na danych osobowych, lub na zestawach danych osobowych w sposób zautomatyzowany lub nie - w rozumieniu art. 4 pkt. 2 Rozporządzenia,
10. Rozporządzenia- rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024),
11. Rozporządzenie – Rozporządzenie PE i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) - Dz. Urz. UE L 119, z dnia 4.5.2016r.
12. Ustawa - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000 ze zm.),
13. Współadministratorzy – podmioty, które wspólnie określają cele i sposoby przetwarzania danych osobowych jako Administratorzy i w związku z prowadzeniem wspólnej polityki ochrony danych osobowych, wykonują razem zadania Administratora,

14. Zbiór danych – uporządkowany zestaw danych osobowych dostępny wedle określonych kryteriów- w rozumieniu art. 4 pkt. 6 Rozporządzenia.

STRUKTURA ORGANIZACYJNA OCHRONY DANYCH OSOBOWYCH

3. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

Administrator

Administratorem danych osobowych jest TREVI APARTMENTS Spółka z ograniczoną odpowiedzialnością.

Jest on odpowiedzialny za:

1) przygotowanie zaplecza organizacyjnego i technicznego do zgodnego z prawem i PODO przetwarzania danych osobowych, w tym wykazania i zapewnienia przetwarzania na najwyższym poziomie bezpieczeństwa;
2) ustalenie, przyjęcie i wdrożenie procedur ochrony danych osobowych na najwyższym poziomie z wdrożeniem odpowiednich środków organizacyjnych i technicznych zapewniających bezpieczeństwo odpowiadające ryzyku naruszenia praw i wolności osób, których dotyczą;
3) ustalenie, przyjęcie i wdrożenie mechanizmów umożliwiających realizację przez osoby uprawnione praw gwarantowanych prawem krajowym i unijnym w zakresie ochrony danych osobowych (w szczególności możliwości zgłoszenia: zastrzeżenia co do przetwarzania danych, zapytania o dane osobowe, żądanie usunięcia, zmiany i innych);
4) ustalenie, przyjęcie i wdrożenie do prowadzenia i aktualizowania rejestrów:
   4.1. przetwarzania danych osobowych,
   4.2. kategorii przetwarzania danych osobowych jako procesor,
   4.3. rejestru wydanych kart i kluczy dostępu,
   4.4. rejestru zgłoszeń zapytań, żądania usunięcia/zmiany/ danych osobowych i cofnięcia zgody na przetwarzanie danych osobowych,
   4.5. rejestru zgłoszeń naruszeń ochrony danych osobowych i sposobu postępowania, w tym prowadzonym środkom zapobiegawczym i prewencyjnym,
5) prowadzenie stałej i koniecznej współpracy z organem nadzoru;
6) zgłoszenie naruszeń danych osobowych organowi nadzorczemu i jeżeli konieczne policji (prokuraturze), oraz w przypadku wystąpienia takiej konieczności zawiadomienia osób, których dane zostały naruszone z opisem naruszenia;
7) zapewnienie odpowiednich środków w celu dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w sytuacji, jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym, jeżeli zajdą ku temu odpowiednie przesłanki konsultację z organem nadzorczym;
8) jeśli uzna to za konieczne, stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji, jako element dla stwierdzenia przestrzegania przez Administratora ciążących na nim obowiązków;

9) nadawanie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
10) zapewnienie legalności przekazywania danych osobowych do podmiotów trzecich;

W stosunku do IOD, kiedy zostanie powołany:

11) ustalenie, stworzenie i wdrożenie mechanizmów umożliwiających stałe włączenie IOD do wszystkich spraw związanych z ochroną danych osobowych;
12) zapewnienie niezbędnego zaplecza organizacyjno – technicznego do wykonywania zadań zleconych przez IOD oraz przekazania pełnego dostępu do danych osobowych i operacji przetwarzania, a także umożliwienie podnoszenia kwalifikacji i szkolenia;
13) zapewnienie niezależności IOD w podejmowaniu działań związanych z ochroną danych osobowych;
14) publikacja danych kontaktowych IOD i powiadomienie organu nadzorczego;

W stosunku do ASI, kiedy zostanie powołany:

15) ustalenie, stworzenie i wdrożenie mechanizmów umożliwiających stałe włączenie ASI do wszystkich spraw związanych z ochroną danych osobowych w procesach telekomunikacyjnych;
16) zapewnienie niezbędnego zaplecza organizacyjno – technicznego do wykonywania zadań zleconych ASI oraz przekazania pełnego dostępu do danych osobowych i operacji przetwarzania w procesach informatycznych, a także umożliwienie podnoszenia kwalifikacji i szkolenia;
17) zapewnienie niezależności ASI w podejmowaniu działań związanych z ochroną danych osobowych w procesach informatycznych.

Administrator:

Nadzorują działania IOD, ASI oraz wydają im zalecenia, co do sposobu wykonywania obowiązków wynikających z Polityki, które nie naruszają prawa do bezstronności i niezależności IOD w kreowaniu polityki ochrony danych osobowych oraz wyrażają zgodę i ostateczną akceptację na takie działania IOD oraz ASI, w które zaangażowane są podmioty trzecie.

Do zaakceptowania działań, zlecenia czynności, procedur sprawdzających, wskazania wytycznych i złożenia zapytań wystarczająca jest komunikacja w formie wiadomości e-mail.

Administrator wyznacza IOD i ASI na mocy powołania.

Dokument powołania i odwołania stanowią **Załącznik numer 1 i 2 do PODO**.

Inspektor ochrony danych (IOD)

Inspektora ochrony danych osobowych ustanawia Administrator, poprzez powołanie. Odwołanie następuje w tej samej formie (dokumenty powołania i odwołania IOD stanowią Załącznik nr 1 do PODO).

Inspektor ochrony danych:

1. musi spełniać kryterium wiedzy teoretycznej i praktycznej z zakresu ochrony danych osobowych;
2. posiadać doświadczenie w pełnieniu funkcji IOD (jako poprzedni IOD, lub na podstawie dotychczasowego przebiegu zatrudnienia i kwalifikacji zawodowych daje rękojmie prawidłowego wykonywania obowiązków);
3. być nieposzlakowanej opinii;
4. IOD może być powołany bezpośrednio i zostaje zawierana umowa o pracę, współpracę, lub może zostać wyznaczony przez firmę zewnętrzną, której zleci się obsługę ochrony danych. Delegowanie przez firmę zewnętrzną IOD do wykonywania tej funkcji u Administratora odbywa się na podstawie imiennego wskazania. Osoba ta nie może być zmieniona bez wiedzy i zgody Administratora. O każdej zmianie firma zewnętrzna zawiadamia z 1 (*jedno*) miesięcznym wyprzedzeniem. Na czas nieobecności IOD firma zewnętrzna może wskazać imiennie zastępcę IOD. Wskazania odnoszące się do IOD obowiązują zastępcę bezpośrednio.

Zadania IOD:

1. bieżące monitorowanie prawodawstwa unijnego i krajowego związanego z ochroną danych osobowych, aktualizowanie obowiązujących u Administratora dokumentów, procedur, rozwiązań do zgodności z nowelizowanymi lub nowo ustanawianymi przepisami prawa w zakresie ochrony danych osobowych;
2. informowanie i szkolenie pracowników, współpracowników z zakresu ochrony danych osobowych, w tym o konsekwencjach nieprzestrzegania ochrony danych osobowych;
3. monitorowanie przestrzegania prawa krajowego i unijnego w zakresie ochrony danych osobowych, ustalonych i wdrożonych procedur ochrony danych osobowych oraz stosowanych rozwiązaniach u Administratora, raportowanie spostrzeżonych uchybień, wdrażanie procedur naprawczych, tworzenie mechanizmów zapobiegających naruszeniom w przyszłości;
4. podnoszenie kwalifikacji i świadomości pracowników, współpracowników w zakresie ochrony danych osobowych;
5. wdrażanie i ustalanie podziału obowiązków w zakresie ochrony danych osobowych (prowadzenie polityki upoważnień do przetwarzania danych osobowych – ustalanie kto jakie działanie, na których danych może podejmować, w jakim zakresie);
6. prowadzenie polityki podziału obowiązków w związku z ochroną danych osobowych co do kontrahentów Administratora (zakres umów powierzenia, konieczność powierzenia danych osobowych, zakres procesowania danych osobowych);
7. przeprowadzanie audytów w zakresie przestrzegania RODO i wdrożonych procedur ochrony danych osobowych;

8. udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania;
9. współpraca z organem nadzorczym i bezpośrednie kontaktowanie się z organem nadzorczym w kwestiach związanych z przetwarzaniem danych;
10. kontakt dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

Administrator Systemów Informatycznych

Administratora Systemów Informatycznych ustanawia Administrator, poprzez powołanie. Odwołanie następuje w tej samej formie (dokumenty powołania i odwołania ASI stanowią Załącznik numer 2 do PODO).

1. musi spełniać kryterium wiedzy teoretycznej i praktycznej z zakresu procesów informatycznych i ochrony danych osobowych;
2. posiadać doświadczenie w pełnieniu funkcji ASI (jako poprzedni ASI, lub na podstawie dotychczasowego przebiegu zatrudnienia i kwalifikacji zawodowych daje rękojmie prawidłowego wykonywania obowiązków);
3. być nieposzlakowanej opinii;
4. ASI może być powołany bezpośrednio i zostaje zawierana umowa o pracę, współpracę, lub może zostać wyznaczony przez firmę zewnętrzną, której zleci się obsługę informatyczną Administratora.

Zadania ASI:

1. prowadzenie rejestru nadanych uprawnień do systemów informatycznych;
2. opracowywanie oraz aktualizacja Polityki Bezpieczeństwa Systemów Informatycznych *(dalej PBSI)*, która stanowi ogólny opis technicznych środków bezpieczeństwa wdrożonych w firmie,
3. nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów;
4. podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń;
5. identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych;
6. sprawowanie nadzoru nad kopiami zapasowymi;
7. inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych;
8. podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemach informatycznych;
9. dokonywanie cyklicznych przeglądów aktualności i stosowania procedur z zakresu przetwarzania danych w systemach informatycznych, na podstawie opracowanego planu przeglądów;

10. ścisła współpraca z IOD w zakresie bezpieczeństwa i zasad przetwarzania danych osobowych w systemach informatycznych.

4 ZAKRES KOMPETENCJI I ZALEŻNOŚCI IOD, ASI, ADMINISTRATORA

Administrator powołuje IOD i ASI. Oba te podmioty w ramach kompetencji związanych z ochroną danych osobowych są od siebie niezależne, co do zakresu wykonywanych obowiązków. Są to także podmioty niezależne od Administratora w zakresie władczych decyzji, które podejmują w ramach zleconych czynności.

ASI podlega IOD co do tego zakresu czynności, który wykracza poza PBSI, a wiąże się z ochroną danych osobowych. Także IOD może przeprowadzić kontrolę wykonywania obowiązków przez ASI w formie audytu, o którego rezultacie zawiadamia ASI i Administratora. ASI może udzielić wyjaśnień do audytu lub złożyć zastrzeżenia.

ASI w zakresie wykonywania PBSI jest niezależny. Raportuje IOD stopień ochrony danych osobowych i wprowadzane rozwiązania. Przekazuje także na koniec każdego roku kalendarzowego, w terminie do 31 stycznia roku następnego, zaktualizowaną listę upoważnień do systemów informatycznych, wprowadzanych zmianach w systemach, modyfikacji zabezpieczeń. Jeżeli tego wymaga proces ochronny (w szczególności dokonano zmiany systemów informatycznych w ciągu roku, rozszerzono znacząco zakres upoważnień do systemów informatycznych, odebrano komuś upoważnienie, zauważono naruszenia o stopniu poważnym lub znacznym) lub dobro osób, których dane dotyczą ASI składa raport co do tych okoliczności niezwłocznie po ich wystąpieniu do IOD, z kopią do Administratora.

Administrator może na każdym etapie procesu przetwarzania danych osobowych żądać raportu z dokonywanych czynności, procesów bezpieczeństwa, wdrażanych procedur przez IOD I ASI. IOD i ASI w terminie 7 (*siedmiu)* dni składają raport, chyba że potrzeba jest więcej czasu do jego sporządzenia o czym informują Administratora z podaniem daty wykonania.

ZAKRES ODPOWIEDZIALNOŚCI IOD, ASI

IOD i ASI nie są odpowiedzialni za te działania drugiego podmiotu, które należą wyłącznie do jego zakresu czynności. Odpowiedzialność za ten obszar ponosi osoba, która miała wykonywać zlecone czynności. W szczególności ASI odpowiada za PBSI i działanie ochrony systemów informatycznych, IOD za dalszą ochronę danych osobowych i realizację PODO.

5. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

Administrator, a także jeżeli takie upoważnienie otrzyma IOD i ASI, mają prawo i obowiązek nadać:

1) upoważnienie do przetwarzania danych osobowych (wzór stanowi Załącznik numer 3 do PODO),
2) upoważnienie do przebywania w miejscu przechowywania danych osobowych (wzór stanowi Załącznik numer 3 do PODO).

Upoważnienie:

1) zawiera określenie osoby, której je nadano (imię, nazwisko, stanowisko służbowe),
2) okres nadania,
3) termin cofnięcia upoważnienia ze wskazaniem przyczyny,
4) wskazanie danych osobowych, których upoważnienie dotyczy,
5) zakres upoważnienia (rodzaj czynności, których może dokonywać upoważniony),
6) pouczenie o obowiązku przestrzegania zasad ochrony danych osobowych (PODO, PBSI, innych procedur, ustawodawstwa krajowego i unijnego),
7) wskazanie odpowiedzialności za naruszenie ochrony danych osobowych,
8) podpis upoważniającego,
9) zgoda na przyjęcie upoważnienia z oświadczeniem o przestrzeganiu polityki ochrony danych osobowych,
10) podpis upoważnionego.

Osoba upoważniona:

1. ma obowiązek przestrzegać polityki ochrony danych osobowych (PODO i prawa krajowego i unijnego),
2. wykorzystywać upoważnienie jedynie do tych kategorii danych, których upoważnienie dotyczy,
3. dokonywać działań na danych osobowych jedynie w zakresie upoważnienia i w czasie jego trwania,
4. wystąpić o upoważnienie do działań na danych osobowych lub na kategorii danych osobowych, przed ich podjęciem, a których nie obejmuje upoważnienie z podaniem przyczyny to uzasadniającej,
5. stosować się zaleceń, wytycznych, procedur wdrażanych przez IOD, ASI, Administratora,
6. informować IOD i Administratora niezwłocznie:
   6.1. o dokonaniu działań na danych osobowych z poza upoważnienia z podaniem przyczyny to uzasadniającej,
   6.2. dokonanie działań na danych osobowych nie wskazanych kategorii z podaniem przyczyny to uzasadniającej,
   6.3. o problemach z przetwarzaniem danych osobowych z opisem problemu,
   6.4. o naruszeniu ochrony danych osobowych z opisem naruszenia, zakresem danych i kategorią danych, stosowanym środkom zapobiegawczym i minimalizującym naruszenie, informować także o możliwości wystąpienia naruszenia,
   6.5. zgłoszonych żądaniach osób, których dane dotyczą – usunięcia, zmiany, poprawienia danych osobowych i innych.

7. Przestrzegać bezwzględnie zasad bezpieczeństwa ochrony danych osobowych i informować o każdej możliwości ich naruszenia, a jeżeli naruszenie wystąpi o stosowanych procedurach.

Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.

Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jedn. Dz.U. z 2018 r., poz. 108 ze zm.), bądź rozwiązania stosunku cywilnoprawnego

6. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Wprowadzenie - zasady ogólne

Dane osobowe u Administratora przetwarzane są zgodnie z RODO i ustawodawstwem krajowym. Administrator w procesie przetwarzania danych osobowy stosują zasady wyartykułowane w art. 5 RODO, tj.:

Zasady przetwarzania danych osobowych

1. **Legalności przetwarzania danych**: wszystkie dane osobowe przetwarzane przez Administratora są przetwarzane, w oparciu o jedną lub więcej, przesłanek legalności wskazanych w art. 6-9 RODO. Podstawa przetwarzania danych osobowych jest każdorazowo podana do wiadomości osoby, której to dotyczy, w klauzuli informacyjnej.
2. **Minimalizacji danych:** dane osobowe przetwarzane przez Administratora są konieczne do realizacji uprawnień, obowiązków lub praw (osób, których dotyczą i Administratora). Administrator nie przetwarza danych niekoniecznych lub zbędnych. Takie dane są niepobierane a pobrane niezwłocznie usuwane.
3. **Ograniczonego celu:** dane są przetwarzanie jedynie w konkretnym, zindywidualizowanym celu, zgodnie z zasadą legalności i minimalizacji.
4. **Rzetelności i przejrzystości:** dane osobowe są przetwarzane w sposób przejrzysty dla osoby, której dotyczą i rzetelnie w zgodnie z słusznym interesem Administratora i osoby, której dotyczą.
5. **Integralności, poufności i prawidłowości:** zapewnione jest odpowiednie bezpieczeństwo przetwarzanych danych, w zgodności z ich treścią. Dane są uaktualniane.
6. **Ograniczonego przechowywania:** dane osobowe są przechowywane jedynie przez niezbędny czas, który także podawany jest do wiadomości osób, których dotyczą w formie obowiązku informacyjnego.
7. **Sprawdzalności:** Administrator prowadzi politykę ochrony danych osobowych w taki sposób, w którym możliwa jest kontrola wykonywania przez nich obowiązków, praw i zadań.

Administrator na bieżąco monitorują zgodność procesów przetwarzania danych osobowych z ww. zasadami.

7 ZGODNOŚĆ PRZETWARZANIA DANYCH Z PRAWEM

1) **Przetwarzanie jest zgodne z prawem wyłącznie, gdy spełniony jest co najmniej jeden z poniższych warunków** (art.6 RODO):

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

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

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze,

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

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi,

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem.

2) Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona:

a) w prawie Unii

lub

b) w prawie państwa członkowskiego, któremu podlega Administrator.

Cel przetwarzania musi być określony w tej podstawie prawnej lub w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) – musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

Jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani prawa Unii lub prawa krajowego, Administrator - aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane - bierze pod uwagę między innymi:

a) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania;

b) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem;

c) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 RODO lub dane osobowe dotyczące wyroków skazujących i czynów zabronionych zgodnie z art. 10 RODO;

d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą;

e) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.

Warunki wyrażenia zgody

Jeżeli przetwarzanie odbywa się na podstawie zgody, Administrator jest zobligowany wykazać zgodę tej osoby.

Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

Przetwarzanie szczególnych kategorii danych osobowych

Zabrania się przetwarzania danych osobowych szczególnych kategorii, w szczególności:

a) ujawniających pochodzenie rasowe lub etniczne,
b) poglądy polityczne,
c) przekonania religijne lub światopoglądowe,
d) przynależność do związków zawodowych,
e) przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej,
f) danych dotyczących zdrowia, seksualności lub orientacji seksualnej osoby.

Warunek przetwarzania danych szczególnych kategorii:

ii) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo zabrania przetwarzania takich danych nawet za zgodą osoby,
iii) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub osobę, której dane dotyczą (np. w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem krajowym),

iv) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody,
v) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą,
vi) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy,
vii) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa krajowego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą,
viii) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa krajowego,
ix) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego,
x) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Dane osobowe, o których mowa powyżej, mogą być przetwarzane do celów, o których mowa pod lit. h), jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa krajowego lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa krajowego.

Przetwarzanie danych osobowych dotyczących wyroków skazujących i czynów zabronionych

Przetwarzania danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 RODO wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem krajowym przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących nie są prowadzone przez Administratora.

Przetwarzanie niewymagające identyfikacji

Jeżeli cele, w których Administrator przetwarza dane osobowe, nie wymagają lub już nie wymagają zidentyfikowania przez niego osoby, której dane dotyczą, Administrator nie ma obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do niniejszego rozporządzenia.

8. INFORMACJE PODAWANE DO WIADOMOŚCI OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE

Dane uzyskane bezpośrednio od osoby, której dane dotyczą

Zakres informacji podawanych przez Administratora:

a) tożsamość Administratora, dane kontaktowe oraz gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela,
b) dane kontaktowe inspektora ochrony danych,
c) cele przetwarzania danych osobowych,
d) podstawa prawna przetwarzania,
e) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO – prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią,
f) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
g) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia.

Poza informacjami wskazanymi pod literą a-g powyżej, podczas pozyskiwania danych osobowych Administrator podają osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:

h) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
i) informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
j) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
k) informacje o prawie wniesienia skargi do organu nadzorczego,
l) informację czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
m) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

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

Pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą Administratora podaje osobie, której dane dotyczą, informacje jak wyżej opisane w punkcie I oraz:

źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;

Termin podanie informacji, sposób

W rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych.

Jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą lub, jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

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

Informacje podaje się: ustnie, pisemnie, elektroniczne. Sposób zależy od kontaktu osoby, której dotyczą. Zaleca się przekazanie informacji w sposób umożliwiający zweryfikowanie wykonanie tego obowiązku (z datą przekazanie i zakresem udzielonych informacji).

Nie podaje się informacji (nie spełnia obowiązku), jeżeli:

a) osoba już posiada te informacje,
b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1 RODO, lub o ile obowiązek informacyjny może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach Administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie,
c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem krajowym, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą,
d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie krajowym, w tym ustawowym obowiązkiem zachowania tajemnicy.

9. ZAKRES PRZETWORZANIA DANYCH OSOBOWYCH

Rejestry

Wszystkie dane osobowe przetwarzane przez Administratora są objęte polityką ochrony danych osobowych. Niezależnie od źródeł ich pozyskania, formy przetwarzania (papierowa, elektroniczna) i kategorii danych do wszystkich danych osobowych stosuje się tożsame zasady ochrony.

Administrator prowadzi rejestry:

I. Czynności przetwarzania danych osobowych.

Rejestr czynności przetwarzania danych osobowych – Załącznik numer 14 do PODO.

Dzieli się na zakładki:

1. Określenie administratora,
2. Rejestr czynności przetwarzania,
3. Rejestr naruszeń danych osobowych,
4. Rejestr zapytań,
5. Rejestr przetwarzającego,
6. Rejestr przetworzeń – współadministrowanie,
7. Rejestr upoważnień,
8. Rejestr kluczy i nośników dostępu.

W rejestrze czynności przetwarzania danych osobowych znajdują się pozycje:

1. Wskazanie liczby porządkowej,
2. Kategoria czynności przetwarzania (cel główny),
3. Cel przetwarzania – szczegółowy,
4. Podstawa przetwarzania,
5. Właściciel procesu,
6. Kategorie osób,
7. Kategorie danych,
8. Dane osobowe szczególnych kategorii,
9. Odbiorcy danych osobowych – kategorie,
10. Sposób przetwarzania danych osobowych,
11. Sposób pozyskiwania danych osobowych,
12. Okres przechowywania danych,
13. Opis środków bezpieczeństwa,
14. DPIA,
15. Transfer do Państwa Trzeciego,
16. Kategorie transferowanych danych,
17. Odbiorca danych,
18. Państwo trzecie/organizacja międzynarodowa,
19. Podstawa prawna transferu,
20. Dokumentacja dotycząca odpowiednich zabezpieczeń,

21. Data ostatniej aktualizacji.

II. Rejestr naruszeń:

1. Naruszenie (stypizowany opis naruszenia),
2. Data i godzina zgłoszenia podejrzenia naruszenia,
3. Data oraz godzina stwierdzenia naruszenia,
4. Data naruszenia/okres, którego dotyczy,
5. Kategoria i ilość osób, których dotyczy naruszenie,
6. Zakres danych i/lub kategorie danych, których dotyczy naruszenie,
7. Osoba/źródło informacji o zdarzeniu,
8. Miejsce naruszenia,
9. Okoliczności naruszenia - opis charakteru naruszenia, analiza zdarzenia, przyczyny wystąpienia,
10. Opis skutków/konsekwencji naruszenia,
11. Osoba/jednostka odpowiedzialna za naruszenie,
12. Podjęte działania - opis środków zastosowanych lub proponowanych do wdrożenia w celu zaradzenia naruszeniu, w tym zastosowane środki w celu zminimalizowania jego negatywnych skutków,
13. Rezultat działań naprawczych,
14. Osoba odpowiedzialna za wdrożenie działań naprawczych,
15. Czy zachodzi obowiązek poinformowania Urzędu Ochrony Danych Osobowych (Jeśli tak - data i godzina zgłoszenia; w przypadku wystąpienia opóźnienia w powiadomieniu - wyjaśnienie przyczyn opóźnienia,
16. Czy powiadomiono organy ścigania (data zawiadomienia),
17. Czy zachodzi obowiązek poinformowania osoby/osób, których naruszenie dotyczy oraz sposób przekazania informacji wraz opisem zaleceń dla podmiotów danych,
18. Monitoring działań naprawczych.

III. Rejestr zapytań:

1. Lp,
2. Data zgłoszenia,
3. Dane osoby przyjmującej,
4. Data przekazania os. upoważnionej,
5. Podjęte czynności,
6. Inne.

IV. Rejestr przetwarzającego:

1. Lp,
2. Nazwa powierzonego procesu biznesowego,
3. Nazwa i dane kontaktowe Administratora, któremu powierzono przetwarzanie danych,
4. Departament Przetwarzającego odpowiedzialny za przetwarzanie (IT, HR itp.),
5. Kategorie czynności przetworzeń,

6. Transfer do Państwa Trzeciego,
7. Nazwa Państwa Trzeciego/ Organizacji międzynarodowej,
8. Dokumentacja Dotycząca Odpowiednich Zabezpieczeń,
9. Opis środków minimalizacji,
10. Czy zawarta umowa powierzenia - do kiedy,
11. Data zawarcia umowy powierzenia.

V. Rejestr powierzenia danych przez Administratora:

1. nazwa powierzonego procesu biznesowego,
2. Nazwa i dane kontaktowe Administratora, który powierzył przetwarzanie danych,
3. Departament Przetwarzającego odpowiedzialny za przetwarzanie (IT, HR itp.),
4. Kategorie czynności przetworzeń,
5. Transfer do Państwa Trzeciego,
6. Nazwa Państwa Trzeciego/ Organizacji międzynarodowej,
7. Dokumentacja Dotycząca Odpowiednich Zabezpieczeń,
8. Opis środków minimalizacji,
9. Czy zawarta umowa powierzenia - do kiedy,
10. Data zawarcia umowy powierzenia.

VI. Rejestr wydanych upoważnień:

1. Osoba, której wydano upoważnienie,
2. Data wydania upoważnienia,
3. Zakres upoważnienia,
4. Data wygaśnięcia upoważnienia (czas określony, nieokreślony),
5. Data wygaśnięcia upoważnienia.

VII. Rejestr wydanych kluczy i kart dostępu:

1. Wydany dostęp - numer ewidencyjny,
2. Osoba, której wydano klucze/ dostęp,
3. Data wydania/ nadania dostępu,
4. Zakres wydanego dostępu,
5. Data wygaśnięcia dostępu,
6. Data pozbawienia dostępu.

10 ZAKRES UPOWAŻNIENIA, DZIAŁANIE BEZ UPOWAŻNIENIA

Upoważnienia nadawane są osobom, które przetwarzają dane osobowe. Opis upoważnienia (co zawiera) wskazano w punkcie o osobach upoważnionych - powyżej wiersz: (Upoważnienie), Załącznik numer 3 do PODO stanowi wzór upoważnienia.

Do przetwarzania danych osobowych nowy pracownik/ współpracownik może przystąpić: po nadaniu upoważnienia i jego podpisaniu, przeprowadzeniu szkolenia i przekazaniu do zapoznania się Polityki ochrony danych osobowych, wpisaniu osoby do rejestru upoważnień, jeżeli wymaga się po nadaniu dostępu lub wydaniu kluczy.

Osoba nieupoważniona do przetwarzania danych osobowych (pracownik, współpracownik) lub nieposiadająca upoważnienia do niektórych działań lub kategorii osób, jeżeli wymagają tego przepisy bezpieczeństwa, jest to konieczne dla ochrony danych osobowych i ważnego interesu Administratora lub osób, których dane dotyczą (klientów) może podjąć się działań na danych osobowych zawiadamiając niezwłocznie IOD i Administratora (jeżeli to możliwe). IOD i Administrator niezwłocznie wydają upoważnienie do tych działań, lub odmawiają wydania i zabraniają dokonywania działań na danych osobowych. Co do działań już wykonanych osoba ta otrzymuje upoważnienie i rozlicza się ją niezwłocznie z zachowania zasad polityki ochrony danych osobowych, oraz sprawdza czy dane osobowe były należycie przetwarzane.

11. UMOWA POWIERZENIE DANYCH OSOBOWYCH

Dopuszcza się przekazanie w części lub w całości, danych osobowych kategorii (lub danych kategorii osób) do przetwarzania przez podmioty trzecie – firmy i osoby zewnętrzne. Zawsze przekazanie danych osobowych do przetwarzania przez podmioty trzecie wymaga zawarcia umowy powierzenia danych osobowych.

Wzór umowy powierzenia danych osobowych stanowi Załącznik numer 5 do PODO.

Umowa powierzenia danych osobowych musi być zgodna z art. 28 RODO, tj. w szczególności określać:

1. przedmiot powierzenia,
2. czas trwania powierzenia,
3. charakter i cel przetwarzania,
4. rodzaj powierzanych danych osobowych,
5. kategorie osób, których dane dotyczą,
6. warunki podpowierzenia przetwarzania danych
7. obowiązki i prawa ADO,
8. obowiązki podmiotu przetwarzającego.

Warunki zawarcia umowy powierzenia i jej wykonania:

1. weryfikacja podmiotu przetwarzającego pod kontem zgodności przetwarzania przez niego danych w zgodzie z polityką ochrony danych osobowych i prawa krajowego i unijnego ochrony danych osobowych,
2. wdrożenia przez podmiot przetwarzający odpowiednich zabezpieczeń i polityki bezpieczeństwa,
3. wybór najlepszego podmiotu, dającego gwarancję należytego wykonania obowiązków i ochrony danych osobowych powierzonych.
4. Umowa może być zawarta w formie elektronicznej lub pisemnej.
5. Przed zawarciem umowy powierzenia wymaga się analizy i akceptacji treści umowy przez IOD.
6. IOD wprowadza zmiany w umowie powierzenia, a jeżeli uważa, że umowa jest nieodpowiednia lub nie gwarantuje zasad ochrony danych osobowych odmawia jej akceptacji.
7. Umowa zostaje zawarta oddzielnie lub może stanowić element umowy głównej świadczenia usług, jeżeli umowa główna zawierać będzie wszystkie elementy wskazane powyżej.
8. Umowę powierzenia po akceptacji IOD podpisują osoby upoważnione.
9. Okoliczność zawarcia umowy powierzenia odnotowuje się w rejestrze umów powierzenia.
10. Jeżeli to możliwe to Administrator przedstawia umowę własną powierzenia do podpisu, dopuszcza się zawarcie umowy powierzenia sporządzonej przez podmiot trzeci.
11. Każda zmiana umowy powierzenia lub umowy głównej wpływającej na ochronę danych osobowych wymaga nowej zgody i akceptacji IOD.
12. Administrator kontroluje przestrzeganie przez procesorów zasad ochrony danych osobowych w procesie przetwarzania powierzonych im danych (audyt, wezwanie do

wyjaśnień). Jeżeli procesor narusza zasady PODO Administrator bezzwłocznie odstępuje od umowy powierzenia i żąda zwrotu powierzonych danych osobowych wraz z załącznikami.

13. Po odstąpieniu od umowy powierzenia IOD sprawdza prawidłowość przeprowadzonych czynności przez procesora, stan bezpieczeństwa danych osobowych i niezwłocznie, jeżeli jest konieczne, wprowadza procesy naprawcze.

Administrator może przetwarzać dane pozyskane od podmiotów przekazującym im te dane umową powierzenia, jeżeli dopuszcza to ta umowa powierzenia.

12. **UDOSTĘPNIENIE DANYCH OSOBOWYCH**

Administrator jest uprawniony do przekazania – udostępnienia danych osobowych innym podmiotom, jeżeli jest to konieczne i na podstawie wskazanej w art. 6-9 RODO.

Wymaga się kontroli prawidłowości udostepnienia i przestrzegania przez ten podmiot ochrony danych osobowych.

Podejmuje się działania służące uniemożliwieniu udostępnienia danych niekoniecznych, podmiotom nieuprawnionym, których legitymacja wygasła.

Udostępnienie odnotowuje się w rejestrze czynności przetwarzania.

Administrator może również przyjąć udostępnione dane od innego Administratora. Zakres, cel i odpowiedzialność Administratora określa wówczas umowa.

Wzór umowy o udostępnienie danych osobowych jest załącznikiem nr 18 do PODO.

Udostepnienia danych do państw trzecich

Przekazywanie danych, których administratorem jest Administrator do państw trzecich i organizacji międzynarodowych, może się odbywać wyłącznie po spełnieniu warunków przewidzianych w Rozdziale V RODO.

Przekazywanie danych do państw trzecich może mieć formę zarówno powierzenia przetwarzania danych osobowych oraz udostępnienia danych osobowych, co oznacza, że w zależności od rodzaju przekazania, należy wziąć również pod uwagę postanowienia podrozdziałów PODO w zakresie umowy powierzenia lub udostępnienia danych.

Przekazanie danych osobowych 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 przypadkach braku decyzji Komisji Europejskiej, o której mowa powyżej, dokonanie przekazania danych osobowych do państwa trzeciego jest możliwe, gdy samodzielnie zapewni odpowiednie zabezpieczenia i pod warunkiem, że będą obowiązywały egzekwowalne prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej.

Odpowiednie zabezpieczenia można zapewnić za pomocą:

1) prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi,
2) wiążących reguł korporacyjnych zatwierdzonych przez organ nadzorczy, mających zastosowanie do każdego z członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą,
3) standardowych klauzul ochrony danych przyjętych lub zatwierdzonych przez Komisję Europejską,
4) standardowych klauzul ochrony danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję Europejską,
5) 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
6) 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 mowa powyżej można zapewnić w szczególności za pomocą:

i) klauzul umownych między Administratorem lub podmiotem przetwarzającym a Administratorem, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej,
   lub
ii) postanowień uzgodnień administracyjnych między organami lub podmiotami publicznymi, w których przewidziane będą egzekwowalne i skuteczne prawa osób, których dane dotyczą.

W szczególnych przypadkach, dopuszcza się przekazanie danych osobowych do państwa trzeciego pomimo braku decyzji Komisji Europejskiej, o której mowa wyżej oraz bez zapewnienia odpowiednich zabezpieczeń wyżej opisanych. Do tych szczególnych przypadków zalicza się przekazanie danych pod warunkiem, że:

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

Administratora przed planowanym przekazaniem danych do państwa trzeciego, jest zobowiązany poinformować o tym IOD oraz skonsultować z nim warunki przekazania tych danych. Przekazanie danych może odbyć się wyłącznie na podstawie warunków i postanowień zaakceptowanych przez IOD.

13. **WSPÓŁADMINISTROWANIE**

Dopuszcza możliwość przyjęcia modelu współadministrowania danymi osobowymi zgodnie z art. 26 RODO.

Współadministrowanie danymi może zachodzić wówczas, jeżeli co najmniej dwa podmioty wspólnie ustalają cele i sposoby przetwarzania danych osobowych. Oznacza to, że w danym procesie spełnione są łącznie warunki:

1) podmioty są administratorami w rozumieniu RODO,
2) wspólnie ustalają cele przetwarzania danych,
3) wspólnie ustalają sposoby (techniczne i organizacyjne) przetwarzania danych osobowych.

Jeżeli spełnione są powyższe warunki podmioty te stają się Współadministratorami w danym procesie przetwarzania (nie musi dotyczyć wszystkich kategorii przetwarzania i kategorii danych osobowych).

Przy współadministrowaniu:

1) w drodze wspólnych uzgodnień, w przejrzysty sposób Współadministratorzy określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO,
2) prowadzą wspólną politykę ochrony danych osobowych,
3) są zobowiązani informować się wzajemnie o naruszenie PODO.

Współadministrowanie wymaga zgody IOD. IOD ocenia czy dane procesy są objęte współadministrowaniem i w jakim zakresie.

IOD, przy udziale IOD lub administratora drugiego podmiotu, wspólnie ustala zasady współadministrowania danymi osobowymi podmiotów. Sporządza stosowne dokumenty i nadzoruje jakość wykonania współadministrowania. O współadministrowaniu zawiadamia się osoby, których dane są współadministrowane w klauzuli informacyjnej.

Wzór umowy o współadministrowanie jest załącznikiem nr 17 do PODO.

OCHRONA DANYCH OSOBOWYCH I REALIZACJA PRAW OSÓB, KTÓRYCH DOTYCZĄ

14. **AUDYTY**

Audyty zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz wdrożonymi procedurami przeprowadzane są przez IOD.

IOD przygotowuje plan audytów, co najmniej jeden audyt rocznie. Plan audytów przedstawia IOD Administratorowi nie później niż do 31 stycznia każdego roku.

Plan audytów zawiera:

1) przedmiot, zakres oraz termin przeprowadzenia poszczególnych audytów oraz sposób i zakres ich dokumentowania,
2) procesy przetwarzania danych osobowych objęte audytem,
3) konieczność weryfikacji zgodności przetwarzania danych osobowych z:
   3.1. zasadami przetwarzania danych osobowych,
   3.2. zasadami dotyczącymi zabezpieczenia danych osobowych,
   3.3. zasadami przekazywania danych osobowych.

IOD raportuje audyty. Wskazuje w raporcie:

1. zakres audytu,
2. termin wykonania,
3. spostrzeżenia,
4. wnioski,
5. środki naprawcze (jeżeli wymaga),
6. dalsze wytyczne.

Raport przedkłada się Administratorowi do 30 dni od dnia jego zakończenia.

Wzór raportu z audytu stanowi Załącznik numer 6 do PODO.

Administrator prowadzi również rejestr audytów. Załącznik nr 6a.

15. REALIZACJA PRAW OSÓB, KTÓRYCH DOTYCZĄ

Administrator wdrożył procedury i zasady ułatwiające osobie, której dane dotyczą, wykonywanie praw ochrony danych osobowych, w tym, w szczególności:

1) prawo do wycofania wyrażonej zgody na przetwarzanie danych osobowych (art. 7 ust. 3 RODO),
2) prawo dostępu do danych osobowych przysługujące osobie, której dane dotyczą (art. 15 RODO),
3) prawo do sprostowania danych osobowych (art. 16 RODO),
4) prawo do usunięcia danych osobowych czyli prawo do bycia zapomnianym (art. 17 RODO),
5) prawo do ograniczenia przetwarzania danych osobowych (art. 18 RODO),
6) prawo do przenoszenia danych osobowych (art. 20 RODO),
7) prawo sprzeciwu wobec przetwarzania danych osobowych (art. 21 RODO),
8) prawo do niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu danych osobowych (art. 22 RODO).

I) Procedura realizacji praw osób, których dane osobowe dotyczą – *dalej Procedura realizacji praw.*

i) Podmioty uprawnione do złożenia wniosku o wdrożenie procedury realizacji praw.

Każda osoba, której dane są przetwarzane może złożyć do Administratora wniosek o realizację praw ochronnych dotyczących jej danych osobowych.

W szczególności dotyczy to danych osobowych usługobiorców, użytkowników systemu i aplikacji, klientów, kontrahentów, pracowników, zleceniobiorców, usługodawców.

Nie tylko obecnie korzystający usługobiorca, użytkownik czy pracownik posiada takie uprawnienie. Bez względu na okres współpracy z Administratorem, do czasu posiadania Twoich danych przez Nas, możesz złożyć wniosek dotyczący Twoich danych osobowych.

Szczególną kategorią osób zainteresowanych złożeniem żądań np. ograniczenia przetwarzania ich danych osobowych są kandydaci do pracy, którzy nie zostali zatrudnieni. Takie osoby mogą żądać np. usunięcia swoich danych z bazy rekrutacyjnej..

ii) Wszczęcie procedury.

Każde zgłoszenie w wersji e-mailowej, telefonicznej czy listownej, zawierające w swojej treści wniosek dotyczący danych osobowych osoby, której te dane dotyczą, podlega rozpoznaniu. Bez znaczenia jest tytuł wniosku i jego treść, jeżeli można na jej podstawie uznać czego żąda wnioskujący w zakresie swoich danych osobowych. Jeżeli treść wniosku jest nieprecyzyjna, niepełna, nie ma informacji, które są konieczne do wszczęcia lub kontynuowania procedury realizacji praw, zawiadamia się osobę uprawnioną o konieczności uzupełnienia, poprawienia lub złożenia nowego wniosku, wskazując zakres koniecznych do zmiany lub uzupełnienia danych.

Wniosek nie zawierający danych nadawcy lub nieuzupełniony pomimo wezwania, nie będzie rozpatrzony. Takie wnioski odnotowuje się w Rejestrze zapytań wskazując przyczynę odmowy jego realizacji. Jednocześnie, jeżeli to możliwe, zawiadamia się o powyższym uprawnionego.

Wniosek może być złożony powtórnie, podlegając tym samym zasadom co wniosek pierwotny.

iii) Wstępna weryfikacja wniosku.

Osoba upoważniona do przyjęcia i rozpoznania wniosków dotyczących danych osobowych dokonuje wstępnej kontroli złożonego wniosku i weryfikuje czy wskazano:

1. dane nadawcy wniosku,
2. dane osoby, której dane osobowe dotyczą,
3. zakres żądania czynności od Administratora,
4. zakres danych osobowych, których dane dotyczą,

I ocenia:

1. poprawność danych kontaktowych,
2. czy osoba zgłaszająca żądanie lub osoba, której dane osobowe dotyczą, jest ujęta w zbiorze danych osobowych Administratora,
3. możliwość złożenia wniosku przez wnioskującego, jeżeli dotyczy on danych osobowych innej osoby np. rodzic w imieniu małoletnich,
4. zakres żądania i zakres danych objętych wnioskiem – czy jest zgodny z zakresem posiadanych danych osobowych a żądanie mieści się w ustawowym katalogu uprawnień osoby, której dane osobowe dotyczą.

Następnie wniosek przekazywany jest do osoby zajmującej się obsługą RODO, celem dalszej realizacji z adnotacją i zaznaczeniem wyników wstępnej kontroli.

iv) Forma, sposób złożenie zapytania/roszczenia przez uprawnionego.

A1. Pisemna

Administrator stworzył wzór wniosku do Procedury realizacji praw, który stanowi Załącznik do tego dokumentu. Wzór wniosku załączono także na stronie internetowej www.mq.energy/rodo, przy wzorach informacji o administrowaniu danymi osobowymi.

Formularz jest wzorem, stworzonym dla ułatwienia realizacji praw osób uprawnionych. Nie wyłącza się złożenia wniosku przez osobę uprawnioną w innej formie, z pominięciem formularza. Każde zgłoszenie w wersji papierowej zawierające w swojej treści żądanie dotyczące danych osobowych osoby, której dotyczą, podlega rozpoznaniu.

A2. E-mailowa

Wniosek można złożyć e-mailowo załączając formularz, stanowiący wzór udostępniony na stronie www.bukowa.tychy.pl/rodo, lub w każdej innej formie.

Adres: rodo@mq.energy

Przesłanie wniosku na inny adres e-mailowy Administratora wszczyna procedurę realizacji praw. Wniosek przekazuje się niezwłocznie, zgodnie z kompetencjami.

A3. Ustna

Wniosek może zostać złożony także ustnie – telefoniczne. Osoba odpowiedzialna za Procedurę realizacji praw, przyjmując wniosek, sporządza notatkę służbową pobierając od osoby zgłaszającej informacje:

1. dane osoby zgłaszającej,
2. dane osoby, której dane dotyczą,
3. zakres żądania,
4. zakres danych osobowych.

Celem zweryfikowania tożsamości osoby zgłaszającej i osoby, której dane osobowe dotyczą, przesyła się do akceptacji przez zgłaszającego treści potwierdzonej rozmowy ustnej (telefonicznej), e-mailem. Po prawidłowej weryfikacji tożsamości osób wnioskujących, nadaje się wnioskowi dalszy bieg.

v) Realizacja wniosku.

Po wstępnej analizie wniosku specjalista ds. RODO lub upoważniony przez niego pracownik, dokonuje realizacji wniosku. Realizacja wniosku odbywa się zgodnie z żądaniem osoby wnioskującej, jeżeli jest to zgodne z powszechnie obowiązującymi przepisami prawa oraz nie sprzeciwia się celom przetwarzania danych osobowych. Przykładowo realizacja prawa osób wnioskujących może doprowadzić do:

1. wycofania wyrażonej zgody na przetwarzanie danych osobowych i zaprzestanie przetwarzania tych danych osobowych,
2. udzielenie dostępu, informacji o posiadanych danych osobowych przez Administratora,
3. sprostowanie danych osobowych,
4. usunięcie danych osobowych,
5. ograniczenie przetwarzania danych osobowych zgodnie z wnioskiem,
6. przeniesienie danych osobowych, udostępnienie danych osobowych zgodnie z wnioskiem,
7. uwzględnienie/odmowa uwzględnienia sprzeciwu z uzasadnieniem odmowy,
8. wyłączenie automatycznego profilowania danych osobowych.

Jeżeli nie jest możliwa realizacja wniosku zgodnie z żądaniem osoby uzasadnia się powyższe z przekazaniem informacji o możliwych sposobach zakończenia sprawy, dalszym postępowaniu, możliwości zgłoszenia zastrzeżeń, możliwością odwołania się od decyzji osoby rozpatrującej wniosek do Administratora, zgłoszenia organowi nadzorczemu.

O sposobie realizacji wniosku zawiadamia się osobę zgłaszającą pisemnie lub e-mailowo.

II) Terminy, rejestry, opłaty

Wpływ wniosku (także niekompletnego, lub któremu nie nadano biegu) wpisuje się rejestru zapytań ze wskazaniem sposobu załatwienia.

Termin realizacji wniosku – niezwłocznie, nie później niż w terminie 30 (*trzydziestu)* dni od dnia wpływu wniosku.

W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania informuje się osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.

Informacje i działania podejmowane w ramach Procedury realizacji praw są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, Administrator może:

a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań, albo

b) odmówić podjęcia działań w związku z żądaniem.

Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na Administratorze.

III) Odwołanie

Osoba zgłaszająca żądania a niezadowolona ze sposobu realizacji wniosku lub odmowy jego realizacji może złożyć odwołanie do Administratora w terminie 14 (*czternastu)* dni od dnia wpływu informacji o sposobie realizacji wniosku w formie pisemnej lub e-mailowej. Wyłącza się prawo ustnego odwołania. O powyższym informuje się zainteresowanego w toku procedury.

Informuje się także o możliwości złożenia informacji do organu nadzorczego ze wskazaniem danych adresowych i z pouczeniem o prawach osób, których dane osobowe dotyczą.

Administrator w terminie 14 (*czternastu)* dni od dnia wpływu odwołania udziela odpowiedzi i jeżeli widzi podstawy do uwzględniania wniosku przekazują informację specjaliście ds. RODO ze swoją opinią.

Specjalista ds. RODO powtórnie rozpatruje wniosek i jeżeli podtrzymuje swoje wcześniejsze stanowisko informuje o tym Administratora i osobę zgłaszającą wraz uzasadnieniem decyzji.

Jeżeli uwzględnia odwołanie postępuje zgodnie z wnioskiem, niezwłocznie podejmując czynności.

O sposobie rozpatrzenia odwołania powiadamia się osobę zgłaszającą.

16. OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH (DATA PROTECTION IMPACT ASSESSMENT)

Administrator dokonuje oceny skutków dla ochrony danych w celu opisania przetwarzania danych osobowych oraz oceny jego konieczności i proporcjonalności, a także w celu wspomagania zarządzania ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania ich danych osobowych.

W strukturze Administratora ocena skutków dla ochrony danych osobowych stanowi narzędzie rozliczalności ułatwiające przestrzeganie wymogów określonych w RODO, a także wykazanie, że podjęto odpowiednie środki w celu zapewnienia przestrzegania przepisów RODO.

Procedura oceny skutków dla ochrony danych osobowych (data protection impact assessment) stanowi Załącznik numer 15 do PODO.

Ocena zawiera co najmniej

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez Administratora,
b) ocenę czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,
c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

W stosownych przypadkach Administrator zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania.

Nie tworzy się oceny, jeżeli przetwarzanie ma podstawę prawną w prawie Unii lub w prawie krajowym i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej – chyba że uznaje się za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych.

W razie potrzeby, przynajmniej, gdy zmienia się ryzyko wynikające z operacji przetwarzania, Administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.

Uprzednie konsultacje

Jeżeli ocena skutków dla ochrony danych, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania należy skonsultować się z organem nadzorczym.

Organ nadzorczy, jeżeli uzna, że zamierzone przetwarzanie stanowiłoby naruszenie przepisów RODO lub prawa krajowego – w szczególności, gdy Administrator niedostatecznie zidentyfikował lub zminimalizował ryzyko – organ nadzorczy w terminie do ośmiu tygodni od wpłynięcia wniosku o konsultacje udziela Administratorowi, gdy ma to zastosowanie także podmiotowi przetwarzającemu pisemne zalecenia i może skorzystać z dowolnego ze swoich uprawnień, o których mowa w art. 58 RODO. Okres ten można przedłużyć o sześć tygodni ze względu na złożony charakter zamierzonego przetwarzania. Organ nadzorczy informuje o takim przedłużeniu w terminie miesiąca od wpłynięcia wniosku o konsultacje, z podaniem przyczyn tego opóźnienia. Bieg tych terminów można zawiesić, do czasu aż organ nadzorczy uzyska wszelkie informacje, których zażądał do celów konsultacji.

Konsultując się z organem nadzorczym, Administrator przedstawia mu:

a) gdy ma to zastosowanie – odpowiednie obowiązki Administratora oraz podmiotów przetwarzających uczestniczących w przetwarzaniu, w szczególności w przypadku przetwarzania w ramach grupy przedsiębiorstw,
b) cele i sposoby zamierzonego przetwarzania,
c) środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą, zgodnie z RODO,
d) dane kontaktowe inspektora ochrony danych,
e) ocenę skutków dla ochrony danych,
f) wszelkie inne informacje, których żąda organ nadzorczy.

17. BEZPIECZEŃSTWO PRZETWARZANIA

Administrator celem zapewnienia bezpieczeństwa danych osobowych wdrożył:

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

Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Podsumowanie:

1) Przestrzegamy zasady czystego biurka, zasady minimalizacji danych, ograniczonego dostępu osób trzecich,
2) Realizujemy politykę ochrony danych osobowych, politykę nadawania upoważnień, wydawania kluczy/haseł/kart dostępu.
3) Prowadzimy rejestry i protokoły zdawania danych osobowych i ich nośników.

4) Chronimy dane osób nam powierzonych. Minimalizujemy możliwość zidentyfikowania osoby, której dane dotyczą. Prowadzimy szyfrowanie dokumentów, anonimizację.
5) Preferujemy korespondencję listowną poleconą, za zwrotnym potwierdzeniem odbioru, pocztę elektroniczną na skrzynki służbowe (imienne, tematyczne), nie na ogólne.
6) Weryfikujemy osoby, którym podajemy dane osobowe i inne dane dotyczące usługi. Zasada sprawdzenia osoby, która chce uzyskać informację.
7) Zabezpieczamy nośniki danych osobowych, prowadzimy politykę ochrony dostępu. Nie wynosimy nośników danych poza miejsce realizacji obowiązków służbowych, minimalizujemy ryzyko przypadkowej utraty lub uszkodzenia.
8) Zawsze informujemy osoby, których dane dotyczą o administrowaniu tymi danymi.
9) Realizujemy uprawnienia osób, których dane dotyczą.
10) Każdy przypadek naruszenie PODO lub zauważoną niedostateczną ochronę danych zgłaszamy jako incydent naruszenia polityki ochrony danych osobowych.

18. NARUSZENIE OCHRONY DANYCH OSOBOWYCH

Osobami odpowiedzialnymi za bezpieczeństwo danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do pomieszczeń oraz systemów, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia incydentów ochrony danych osobowych są: Administrator, IOD oraz ASI (w odniesieniu do danych przetwarzanych w systemach informatycznych).

PROCEDURA POSTĘPOWANIA Z INCYDENTAMI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

I) Istota naruszenia danych osobowych

Incydentem w zakresie danych osobowych jest utrata:

1) poufności,
2) integralności,
3) dostępności przetwarzanych danych,

Naruszeniem danych osobowych jest zawsze każda stwierdzona okoliczność:

1) nieuprawnionego ujawnienia danych,
2) udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym,
3) skopiowania (przejęcie) danych przez osobę nieupoważnioną,
4) uszkodzenia elementu systemu informatycznego, w tym włamanie do programu, sieci Administratora.

Takie naruszenia mogą polegać w szczególności na:

5) nieautoryzowanym dostępie do danych lub części danych,
6) modyfikacjom lub zniszczeniom danych bez zezwolenia/upoważnienia,
7) udostępnienie danych podmiotom nieupoważnionym,
8) nielegalnym ujawnienie danych lub nośników danych,
9) pozyskiwanie danych z nielegalnych źródeł lub bez zgody osoby, której dotyczą.

II) Procedura postępowania

Każda osoba zobowiązana do przestrzegania PODO i ochrony danych osobowych administrowanych, powierzonych Administratorowi, która stwierdziła lub podejrzewa możliwość naruszenia polityki ochrony danych osobowych, **jest zobowiązana niezwłocznie zgłosić ową okoliczność** IOD, ASI, Administratorowi.

Przykładowe sytuacje wymagające zgłoszenia zauważone przez zgłaszającego:

1) ślady włamania lub próby włamania do miejsca przechowywania danych osobowych, nośników danych osobowych,
2) udostępnienie kluczy, kart dostępu osobom nieupoważnionym lub pozostawienie ww. rzeczy w miejscach ogólnie dostępnych, niezabezpieczonych,
3) pozostawianie dokumentów – nośników danych osobowych, telefonów i sprzętu elektronicznego (komputer, laptop, tablet i innych) Administratora w miejscach publicznych lub niezabezpieczonych,
4) niszczenie dokumentów w sposób nienależyty (bez niszczarki, w niewyznaczonym miejscu, przez wrzucenie do śmieci,
5) otwarte drzwi do pomieszczeń, szaf i innych miejsc z przechowywaną dokumentacją zawierającą dane osobowe,
6) przebywanie osób nieuprawnionych w miejscach, w których obowiązuje zasada posiadania upoważnienia do przebywania,
7) niewylogowanie się przed opuszczeniem stanowiska pracy,
8) pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem,
9) niewykonanie w określonym terminie kopii bezpieczeństwa,
10) prace na dokumentach służbowych w celach prywatnych,
11) ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe;
12) wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia,
13) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej,
14) próbę modyfikację danych lub ich zmiany w strukturze danych bez odpowiedniego upoważnienia lub zgody IOD,
15) telefoniczne próby uzyskania danych osobowych przez osoby nieupoważnione,
16) kradzież nośników danych osobowych,
17) utrata kontroli nad nośnikiem, kopią danych osobowych;
18) otrzymywanie korespondencji listownej, e-mailowej, telefonicznej z próbą uzyskania dostępu do nośników danych osobowych (systemów informatycznych),
19) zawirusowanie komputera i innych nośników danych osobowych,
20) nieprzestrzeganie zasady „czystego biurka”,
21) rozmowy w miejscach publicznych (telefoniczne, ustne, za pomocą Internetu) na tematy służbowe z podaniem danych osobowych, osób których dane dotyczą,
22) nielegitymowanie rozmówców przed podaniem danych osobowych, o które wnoszą,
23) nieraportowanie możliwości naruszenia danych osobowych,
24) przekazanie danych bez umowy powierzenie, przed jej podpisaniem,

25) przyjęcie danych osobowych, które nie są konieczne/żądane,
26) przekazywanie swoich loginów, haseł dostępu, nośników danych osobowych osobom nieuprawnionym.

Każda osobowa zobowiązana do ochrony danych osobowych u Administratora, która stwierdzi fakt naruszenia danych osobowych lub możliwości wystąpienia naruszenia danych osobowych, ma obowiązek niezwłocznie podjąć czynności niezbędne do powstrzymania skutków naruszenia, zabezpieczyć dowody umożliwiające ustalenie przyczyn i skutków naruszenia.

Zawiadamia się także IOD i Administratora. Jeżeli to konieczne do zapobieżenia skutkom naruszenia przywołuje się do współdziałania osoby trzecie przebywające w miejscu naruszenia, chyba że osoby te nie mogą mieć wglądu w dane osobowe naruszane.

Osoby, które zauważyły naruszenie lub możliwość naruszenia danych osobowych:

1. Są zobowiązane podjąć działania wyżej opisane,
2. Nie ponoszą odpowiedzialności karnej, dyscyplinarnej i cywilnej za zgłoszenie naruszenia.

Nie można w żaden sposób – wytycznymi, procedurami, zaleceniami, dążyć do ograniczenia praw osób zajmujących się danymi osobowymi i zobowiązanymi do przestrzegania PODO, do złożenia informacji o naruszeniu/możliwości naruszenia danych osobowych.

Osoby utrudniające zgłoszenie naruszenia/możliwości naruszenia danych osobowych są odpowiedzialne karnie, cywilnie i dyscyplinarnie za powstałą szkodę.

Po zauważeniu naruszenia/możliwości naruszenia danych osobowych należy:

1. Zabezpieczyć miejsce zdarzenia,
2. Podjąć czynności niezbędne do minimalizacji skutków naruszeń lub ich wystąpienia (w tym powołać osoby do czynności),
3. Zgłosić IOD, ASI, Administratorowi,
4. Czekać do momentu przybycia IOD, ASI, Administratora (jednej z osób) na miejsce zdarzenia,
5. Nie podejmować niekoniecznych czynności, które mogą utrudnić proces analizy naruszenia/możliwości naruszenia i jego skutków,
6. IOD podejmuje dalsze decyzje co do postępowania w związku z tym naruszeniem/możliwością naruszenia. Jeżeli nie ma IOD czynności może podjąć odpowiednio ASI lub Administrator,
7. ASI i inne osoby współpracują z IOD przy ustaleniu przyczyn incydentu,
8. ASI sprawdza wpływ sieci informatycznych na to naruszenie i wpływ naruszenia na sieci informatyczne, zgłasza uwagi i wyniki kontroli niezwłocznie IOD,
9. IOD tworzy protokół poincydentalny, z wpisaniem do rejestru naruszeń.
10. Jeżeli potrzeba IOD zawiadamia organ nadzoru i osoby, których dane naruszono.

III) <u>Zabezpieczenie systemów informatycznych przed naruszeniem</u>

Pełny opis zabezpieczeń zawiera IBSI, załącznik numer 12 do PODO.

W szczególności zaś ochrona systemów informatycznych przy naruszeniach, ułatwieniu oceny naruszenia/możliwości naruszenia to:

1. okresowe przeglądy logów gromadzonych w systemie informatycznym,
2. centralną usługę NTP (synchronizacja czasu w systemie informatycznym w celu jednoznacznej identyfikacji czasowej incydentu naruszenia),
3. kontrola polityki haseł,
4. kontrola przeciwwirusowa,
5. aktualizacje danych i zapór systemu,
6. okresowe kontrole wykonywania obowiązków upoważnionych przez ASI,
7. audyty ASI,
8. audyt procesorów dostarczających usługi informatyczne.

IV) Protokół pokontrolny naruszenia

Inspektor ochrony danych tworzy protokół kontroli naruszenia, w którym:

1. Opisuje incydent,
2. Osobę zgłaszającą,
3. Opis zastosowanych do czasu jego przybycia czynności,
4. opis dalszego postępowania uwzględniający zagrożenie w prawidłowości i ciągłości pracy,
5. protokół przesłuchania osób, które mogą posiadać informacje w związku z zaistniałym naruszeniem,
6. jeżeli potrzeba powołuje specjalistów zewnętrznych do oceny naruszenia.

Możliwe działania IOD dot. ograniczenia skutków naruszeń/możliwości wystąpienia naruszenia:

Z pomocą ASI:

1. rekonfiguracja systemu informatycznego z pomocą ASI,
2. usunięcie przyczyny problemu np. złośliwego oprogramowania, wyłączenie systemu lub jego części,
3. odcięcie połączenia systemu z siecią publiczną,
4. zablokowanie dostępu do konta użytkownika.

Samodzielnie:

5. zabezpieczenie szaf, pomieszczeń,
6. zlecenie wymiany zamków, szyfrów, loginów, kart dostępu,
7. zabezpieczenie nośników danych,
8. kontrola wejść i wyjść do strefy z upoważnieniami do przebywania,
9. zlecenie zdania do depozytu po zakończeniu pracy narzędzi służbowych (telefon, laptop, tablet),
10. zlecenie uprzątnięcia miejsca pracy, zabezpieczenia danych (nośników danych),
11. cofnięcie upoważnień,
12. polecenie ograniczenia dostępu do danych, zwolnienie pracownika,
13. zawiadomienie policji lub innych służb,
14. zawiadomienie osób, których dane naruszono.

Zasadniczym celem usunięcia skutków jest przywrócenie stanu bezpieczeństwa systemu informatycznego oraz informacji sprzed wystąpienia incydentu. Należy przy tym pamiętać o niezacieraniu dowodów związanych z wystąpieniem incydentu naruszenia bezpieczeństwa informacji.

IDO prowadzi rejestr incydentów naruszeń. IDO cyklicznie przeprowadza analizę zebranych danych w rejestrze, wyniki analizy wraz z wnioskami przedstawia Administratorowi.

IOD wprowadzając działania naprawcze wskazuje terminy dalszego przetwarzania danych osobowych, uruchomienia systemu.

19. **ZGŁOSZENIE NARUSZENIA DANYCH**

Po naruszeniu danych osobowych IOD zawiadamia organ nadzoru:

1) bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia UODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
2) Jeżeli zgłoszenia organowi nadzoru dokonano po czasie dołącza się opis przyczyn opóźnienia.

Zgłoszenie:

1) Opisuje charakter naruszenia z podaniem osób (kategorii) i danych, których naruszenie dotyczy,
2) Zawiera opis kategorii wpisów danych
3) Wskazanie IOD lub innej osoby kontaktowej,
4) Opis konsekwencji naruszenia i jego zakresu,
5) Zastosowane środki zapobiegawcze i kontrolne,
6) Przesyła na wniosek organu kopię pełnej, wyczerpującej dokumentacji naruszenia,
7) IOD udziela informacji na każde wezwanie organu,
8) IOD stosuje się do zaleceń organu w zakresie zgłoszonego incydentu.

Zgłoszenie osobom, których dane naruszono:

1. Dokonuje się zgłoszenia, jeżeli to powoduje wysokie ryzyko wystąpienia naruszenia praw lub wolności osób fizycznych,
2. bez zbędnej zwłoki,
3. opis charakteru naruszeń wraz informacją o wdrożonych procedurach naprawczych, kontrolnych i minimalizujących,
4. informacja o zgłoszeniu organowi nadzoru, policji, innemu podmiotowi,
5. zakres danych i zakres informacji o danych,
6. dane kontaktowe do IOD.

Zgłoszenia nie wykonuje się, jeżeli Administrator:

1. wdrożył odpowiednie środki szyfrowania uniemożliwiające odczytanie danych osób osobom nieuprawnionym,

2. zgłoszenie wymagało by niewspółmiernie wysokiego wysiłku – dokonuje się publicznego ogłoszenia o incydencie naruszenia z opisem kategorii danych i danych osób, których może to dotyczyć,
3. zastosowane środki naprawcze spowodowały zminimalizowanie skutków wystąpienia naruszeń i naruszenia praw i wolności osób, których dane dotyczą.

20. MONITORING

1. Podmiot stosuje monitoring:

- monitoring wizyjny,
- monitoring GPS,

2. W przedmiocie stosowanego monitoringu, Podmiot wdrożył:

- obowiązki informacyjne monitoringu wizyjnego, zgodnie z przyjętą procedurą – załącznik nr 19
- obowiązki informacyjne monitoringu GPS, zgodnie z przyjętą procedurą – załącznik nr 20

21. ANALIZA RYZYKA

1) Podmiot wdraża zasadę analizowania ryzyka naruszenia praw lub wolności osób, których dane osobowe podlegają przetwarzaniu.
2) Szacowanie ryzyka odbywać się będzie na warunkach ustanowionych w załączniku.
3) Zabrania się wdrażania nowych czynności przetwarzania danych osobowych, wdrażania nowych zasobów służących do ich przetwarzania, a także zmian środków ochrony danych osobowych, bez uprzedniego wykonania analizy ryzyka lub jej aktualizacji
4) Podmiot zobowiązuje się do aktualizacji analizy ryzyka, znajdującej się w załączniku.

Podmiot przechowuje dokumentację szacowania ryzyka w załączeniu do niniejszej Polityki Ochrony Danych. Załączniki nr 15

22. OGÓLNE ZASADY BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

1) dostęp do danych osobowych mogą mieć tylko pracownicy posiadający upoważnienie do ich przetwarzania;
2) przebywanie osób nieuprawnionych do przetwarzania danych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem;
3) osoby mające dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem,
   w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych;

4) osoby przechowujący dane osobowe zobowiązani są do zabezpieczenia materiałów zawierających dane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym;
5) niedopuszczalnym jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony;
6) nikomu nie należy udostępniać indywidualnych haseł i identyfikatorów do systemów informatycznych;
7) wysyłanie seryjnych wiadomości e-mail wymaga zastosowania opcji kopia ukryta;
8) nie można udzielać informacji dotyczących danych osobowych innym podmiotom na podstawie prośby o takie dane skierowanej w formie zapytania telefonicznego, e-mailowego bez wyraźnej zgody IOD lub innego ważnego upoważnienia. IOD akceptuje zgodę na ich udostępnienie każdorazowo;
9) w miejscu przetwarzania danych osobowych utrwalonych w formie papierowej osoby są zobowiązane do stosowania zasady tzw. czystego biurka, która oznacza niepozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników. Nie należy pozostawiać danych osobowych w miejscach ogólnodostępnych takich jak np. biurka, blaty, parapety;
10) niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe odbywać się musi w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek;
11) za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych;
12) 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;
13) klucze do pomieszczeń, w których przetwarzane są dane osobowe nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia kluczy przed udostępnieniem ich osobom nieupoważnionym;
14) przed wyjściem z pomieszczenia, w którym przechowywane są dane osobowe należy upewnić się, że zostało ono odpowiednio zabezpieczone (zamknięte okna, drzwi);
15) po zakończeniu pracy w systemie informatycznym, w którym przechowywane są dane osobowe, należy wylogować się z systemu;
16) osoba użytkująca komputer przenośny zawierający dane osobowe zobowiązana jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe;
17) na pracowniku pracującym zdalnie spoczywa obowiązek odpowiedniego zabezpieczenia danych tak, aby osoby trzecie nie miały dostępu do danych osobowych;
18) dane osobowe przesyłane elektronicznie powinny być zabezpieczone hasłem. Hasło to powinno być wysyłane oddzielnym kanałem telekomunikacyjnym.

<u>Zabrania się:</u>

1) Udostępniania nośników danych osobom nieupoważnionym, nawet innym współpracownikom, co tych danych, które są przetwarzane z upoważnienia przez daną osobę,
2) Rozmów telefonicznych, za pośrednictwem Internetu dotyczących obowiązków służbowych z podaniem danych osobowych, w miejscach publicznych (dostępnych osobom nieupoważnionym),
3) Niezabezpieczenia kluczy, karty dostępu, nośników danych i ich pozostawianie w miejscach dostępnych osobom nieupoważnionym,
4) Wprowadzanie na teren przechowywania danych osobowych (nośników danych) osób nieupoważnionych,
5) Odwracanie monitora komputera umożliwiając odczytanie danych na nim zapisanych w trakcie pracy,
6) Przekazywanie dokumentów osobom nieupoważnionym zawierającym dane osobowe innych osób,
7) Wykonywanie pracy zawodowej na narzędziach służbowych (także poczcie firmowej e-mail) poza miejscem wskazanym, bez upoważnienia,
8) Przedstawianie dokumentów do kontroli bez odebrania podstaw kontroli danych osobowych (dokumentów je zawierających).

23. **DELEGACJA UPRAWNIEŃ**

Administrator może delegować swoje uprawnienia i obowiązki na osoby zatrudnione, współpracujące. Delegacja uprawnień/obowiązków szczegółowo określa zakres delegowanych obowiązków, datę delegacji, czas jej trwania (jeżeli jest oznaczony), odebranie/cofnięcie, jeżeli odebrano/cofnięto uprawnienia.

Jeżeli nie powołano IOD lub ASI Administrator może delegować obowiązki/uprawnienia, które zgodnie z PODO wykonuje IOD lub ASI, na pracowników/współpracowników. Nie oznacza to, że osoba ta staje się IOD lub ASI, chyba że w rzeczywistości wykonuje wszystkie obowiązki i uprawnienia IOD lub ASI. Konieczne jest wtedy zgłoszenie takiej osoby jako IOD, ASI. Delegacja nie może służyć obejściu przepisów o powołaniu IOD, ASI. W razie wątpliwości uważa się, że osoba delegowana o pełnym zakresie upoważnienia została powołana jako IOD lub ASI.

24. **ZAŁĄCZNIKI**

1) Powołanie, odwołanie IOD,
2) Powołanie, odwołanie ASI,
3) Upoważnienia do przetwarzania danych,
4) Upoważnienie do przebywania,
5) Umowa powierzenia danych osobowych,
6) Audyt,
7) Wniosek o dokonanie czynności,
8) Realizacja praw,
9) Klauzule informacyjne,
10) Ankieta dla procesorów,

11) Polityka prywatności,
12) Regulamin przetwarzania,
13) Instrukcja ZSI (Zarządzanie Zasobami Informatycznymi),
14) Rejestr czynności przetwarzania danych osobowych,
15) Analiza ryzyka + DPIA
16) Termin usunięcia danych osobowych poszczególnych rodzajów
17) Umowa o współadministrowanie
18) Umowa udostępnienia danych osobowych
19) Procedura stosowania monitoringu wizyjnego
20) Procedura stosowania monitoringu GPS

Dokument podpisany przez Martin Mokwa
Data: 2025.04.28 11:58:15 CEST