Regulamin przetwarzania danych osobowych

Administrator celem zapewnienia bezpieczeństwa danych osobowych wdrożył nw. zasady:

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 naruszenia ochrony danych osobowych,
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.

Stosowane zabezpieczenia danych Administratora:

1. **Zabezpieczenie pomieszczeń, w których są przechowywane dane osobowe:**

TREVI APARTMENTS Spółka z ograniczoną odpowiedzialnością, Adres siedziby ul. Bukowa 24, 43-100 Tychy

wpisana do KRS za 0000937417, NIP 6462992743, Regon 520634216, email: rodo@mq.energy

Opis budynku i powierzchni biurowych Administratora ogólny: budynek wielolokalowy, zlokalizowany w miejscowości Tychy. Lokal jest wynajmowany. Na parterze zlokalizowane jest biuro firmy. W osobnych pokojach, zamykanych na klucz pokoje biurowe. Prowadzony jest monitoring części wspólnych i otoczenia budynku. Alarm budynku z czujkami ruchu w pomieszczeniach biurowych. Parking ogólny, niemonitorowany. Archiwum zlokalizowane w budynku. Serwerownia znajduje się w drugim budynku, którego właścicielem jest współadministrator: MQ Energy Sp. z o.o. w pomieszczeniu Prezesa Zarządu, w oddzielnym budynku, zamykanym na noc. Klucz tylko z dostępem dla upoważnionych osób. Dostęp do biura wspólny – każdy pracownik ma klucz. Wejścia i wyjścia z budynku monitorowane. Wejście do pokojów biurowych ogólnodostępne. Wyposażenie pokoju zabezpieczone zamkiem z kluczem dedykowanym posiadaczowi dokumentów.

1. **Zabezpieczenia zewnętrzne:**
2. Alarm budynku – alarm załączany od godzin wieczornych;
3. monitoring alarmu – właściciel + upoważniona osoba ;
4. drzwi wejściowe: antywłamaniowe, zabezpieczone zamkiem antywłamaniowym,
5. Monitoring wizyjny na okolicę zewnętrzną budynku, monitorowanie wejść i wyjść z budynku, punktów newralgicznych takich jak korytarz, okna, wejście do budynku, parking ogólnodostępny.

- w razie konieczności patrole na zlecenie (po uruchomieniu alarmu) lub z własnej inicjatywy.

2. **Pomieszczenia wewnętrzne, wyposażenie:**

2.1. pokój przechodni

- pomieszczenie wewnętrzne zlokalizowane na parterze budynku głównego,

- pokój przechodni połączony z korytarzem,

- w pomieszczeniu biurka, przy których pracują pracownicy współadministratora MQ Energy Sp. z o.o.. Pracownicy TREVI APARTMENTS Sp. z o.o. przebywają w oddzielnym pomieszczeniu.

- szafy, w których przechowywane są segregatory z innych podmiotów (z grupy kapitałowej)- nie zamykane. Część znajduje się w innym pomieszczeniu,

- monitoring w korytarzu

2.2. pokoje służbowe – zlokalizowane na parterze. Dostęp z poziomu korytarza. Drzwi nieprzeszklone, nie zamykane na klucz. Załączenie alarmu po opuszczeniu całego budynku, włącza ostatnia osoba wychodząca z biura. Dostęp do pomieszczeń ogólnodostępny dla wszystkich pracowników budynku, bez względu na rodzaj wykonywanej pracy.

W pokoju, 2 stanowiska pracy, wyposażone w:

- szafki podblatowe zamykane na klucz, komputer przyporządkowany do jednego stanowiska pracy, szafki nablatowe w postaci kuwet niezabezpieczone do przechowywania dokumentów w trakcie pracy, na dokumenty niezawierające danych osobowych,

- drukarka

- niszczarka:

- wyposażenie biurowe pozostałe:

- szafy częściowo zamykane na klucz: na dokumenty kadrowe, osobowe. Dokumenty kadrowe i inne posiadające dane osobowe w osobnych segregatorach, nazwane z zastosowaniem zasady anonimizacji. Dostęp ograniczony. Klucz posiadają wyłącznie pracownicy Administratora.

- w pomieszczeniu sprzęty: monitor komputera, stacja dysków przynależna do danego stanowiska pracy, zabezpieczona hasłem

2.3. pozostałe pokoje: kuchnia, łazienka, nie stanowi miejsca przechowywania danych osobowych i miejsca, w których dane te mogą się znajdować. Pokoje służbowe do czynności techniczno – organizacyjnych.

Zasady przetwarzania danych osobowych – PROCEDURY.

Procedura Przechowywania danych osobowych	
numer procedury: 1	
dotyczy:	wszystkich osób przetwarzających dane osobowe
osoby odpowiedzialne:	Upoważnieni do przetwarzania danych osobowych

1) Dane osobowe i ich nośniki danych przechowywane są w: szafach zamykanych na klucz, zwykłych lub wzmocnionych, poza dostępem osób trzecich, w pokojach zabezpieczanych wejściem na klucz. Minimalizuje się możliwość dostępu osób trzecich. Zabrania się współdzielenia miejsca biurowego w szafach z innymi podmiotami niepowiązanymi z Administratorem.
2) Szafy z danymi osobowymi szczególnych kategorii są przechowywane w szafach zamykanych na klucz lub zabezpieczonych w innych sposób - szyfrem, z ograniczonym odstępem osób trzecich i pracowników.
3) Dokumenty niepotrzebne archiwizuje się w wydzielonym pomieszczeniu. O archiwizacji w procedurze osobnej.
4) Pracownik ma obowiązek przed rozpoczęciem świadczenia pracy i bezpośrednio po zakończeniu protokolarnie sprawdzić stan nośników danych osobowych i miejsca ich przechowywania, dokonując adnotacji wyłącznie o spostrzeżonych uchybieniach lub odchyleń od normy.

Procedura Upoważnień	
numer procedury: 2	
dotyczy:	wszystkich osób przetwarzających dane osobowe
osoby odpowiedzialne:	Upoważnieni do przetwarzania danych osobowych

1. Każdy pracownik/współpracownik upoważniony do działań na danych i danych szczególnych kategorii otrzymuje upoważnienie, na podstawie którego odbiera: hasło i komplet kluczy do pokoju/szaf/biurka (inne), uzyskuje możliwość dostępu do biura.
2. Uzupełnia się rejestr wydanych upoważnień, imiennie.
3. Odebranie kluczy, haseł, kart dostępu odnotowuje się w rejestrze.
4. Miejsca przechowywania danych szczególnych kategorii – danych wrażliwych, jest zabezpieczone dodatkowym upoważnieniem, rodzajowym.
5. Wyłącza się prawo do przetworzenia danych bez upoważnienia. Czynności nagłe podejmowane przez osobę nieupoważnioną na danych osobowych są dopuszczalne wyłącznie w sytuacji nadzwyczajnej, grożącej utratą lub uszkodzeniem danych osobowych Administratora.

Procedura : Dostęp do miejsc przechowywania danych, procedura kluczy

numer procedury: 3	
dotyczy:	wszystkich osób przetwarzających dane osobowe
osoby odpowiedzialne:	Upoważnieni do przetwarzania danych osobowych

1. Klucze wejściowe do pomieszczeń koniecznych do wykonywania obowiązków (do drzwi wejściowych, do pomieszczenia miejsca świadczenia pracy) nie są zdawane na koniec dnia roboczego. Zdawane są po zakończeniu współpracy protokolarnie, lub w trakcie długich planowanych nieobecności (np. urlop zdrowotny, urlop macierzyński, urlop wychowawczy).
2. Zabrania się pozostawiania w czasie pracy kluczy do budynków i pomieszczeń w zamkach.
3. Zabrania się pozostawiania kluczy w szafach, szufladach i biurkach podczas nieobecności w pomieszczeniu osób upoważnionych do przetwarzania danych osobowych.
4. Poza godzinami pracy, klucze do szaf, szuflad oraz biurek przechowuje się w kasetach lub skrzynkach zamykanych na szyfr.
5. Klucze do szaf z nośnikami danych nie są zwracane na koniec dnia roboczego. Prowadzi się rejestr, w którym nie trzeba odnotowywać każdego wydania kluczy, tylko w momencie przekazania i zbycia. Odnotowuje się nietypowe sytuacje – niezwrócenia klucza na koniec umowy, niezwrócenia hasła dostępu, zwrot klucza przez inną osobę niż osoba, której go wydano, z wykazaniem okoliczności uzasadniających i jeżeli trzeba opisem zastosowanych środków naprawczych i prewencyjnych.
6. Jeżeli wystąpiła inna szczególna okoliczność wskazująca, że dostęp do wydzielonych miejsc przechowywania danych szczególnych kategorii miały osoby nieupoważnione lub mogły mieć dostęp, należy bezwzględnie sprawdzić stan zabezpieczeń, stan posiadanych akt i nośników danych, kompletność zbioru danych, możliwość ich nieuprawnionego powielenia, dostępu, wykazanie osób odpowiedzialnych za sytuację i zastosowanych metod naprawczych i prewencyjnych. Postępowanie jak w przypadku incydentu naruszenia danych osobowych.

ZASADY PRZEBYWANIA W POMIESZCZENIACH ZWYKŁYCH

7. Przebywanie w budynkach lub pomieszczeniach Podmiotu, jest dozwolone w godzinach pracy, przez osoby upoważnione do przetwarzania danych osobowych, przetwarzanych w tych budynkach lub pomieszczeniach.
8. Z zastrzeżeniem punktu poniżej, zabrania się przebywania w budynkach lub pomieszczeniach zwykłych Podmiotu poza godzinami i dniami pracy.
9. Przebywanie w budynkach lub pomieszczeniach zwykłych Podmiotu poza godzinami i dniami pracy, wymaga zgody Administratora.
10. Przebywanie osób nieupoważnionych do przetwarzania danych osobowych, wewnątrz pomieszczeń zwykłych, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych lub za zgodą Administratora.
11. Po zakończeniu pracy, poprzez użycie kluczy, osoby sprawujące nadzór nad nimi, zobowiązane są zabezpieczyć miejsca przechowywania dokumentów z danymi osobowymi (budynki, pomieszczenia, szafy, biurka, szuflady) i inne zbiory ewidencyjne przed dostępem osób trzecich, a także przed zniszczeniem i kradzieżą.
12. Klucz do serwerowni posiada jedynie ASI i Zarząd. W tych pomieszczeniach nie mogą przebywać osoby trzecie, bez nadzoru.

13. Klucz do archiwum posiada jedynie osoba upoważniona i archiwiści. W tych pomieszczeniach nie mogą przebywać osoby trzecie, bez nadzoru.
14. Administrator lub ASI za uprzednią zgodą Administratora, może upoważnić pisemnie inne osoby, imiennie wskazane, do przebywania lub dostępu do kluczy i miejsc przechowywania danych szczególnych kategorii. Osoby te mogą czasowo wykonywać obowiązki, o których mowa w punktach powyżej. Upoważniony nie może nadawać dalszych upoważnień.

Procedura: Zabezpieczenie miejsca pracy i nośników danych w trakcie i po pracy	
numer procedury: 4	
dotyczy:	wszystkich osób przetwarzających dane osobowe
osoby odpowiedzialne:	Upoważnieni do przetwarzania danych osobowych

1) Każdy pracownik ma przypisane miejsce pracy,
2) Do każdego miejsca pracy przypisano: jedną szafkę służącą do przechowywania nośników danych osobowych w trakcie pracy - *dalej szafka podblatowa zamykana na klucz*
3) Każde miejsce pracy jest wyposażone w komputer zabezpieczony hasłem, ustawiony w sposób uniemożliwiający wgląd w treści znajdujące się na pulpicie komputera osobom trzecim (przez okno)i innym pracownikom.
4) Jeżeli monitor znajduje się w pozycji umożliwiającej wgląd w dane na pulpicie zabronione jest wejście osób trzecich do tego pomieszczenia. Wstęp mają jedynie pracownicy wykonujący tam obowiązki. Na monitorach powinny być zamontowane filtry uniemożliwiające dostęp do danych przez okna.
5) Każdy pracownik posiada własne miejsce pracy, które nie jest innym udostępniane (chyba, że w trakcie zastępstwa pracownika za upoważnieniem).
6) Każdy pracownik ma własne narzędzia pracy: telefon komórkowy (jeżeli jest taka potrzeba), komputer stacjonarny i/lub laptop, nośniki danych takie jak: pendrive, mp3, materiały papiernicze, kalendarz papierowy i książkowy, notatnik, organizer. Zabroniona jest praca na własnym sprzęcie pracownika.
7) Narzędzia pracy elektroniczne są hasłowane, zgodnie z polityką haseł.
8) Narzędzia pracy po zakończeniu pracy lub w trakcie jej przerw, jeżeli zawierają dane osobowe a są przenoszalne, są zamykane w szafce podblatowej. Zabrania się wynoszenia narzędzi pracy poza miejsce pracy, chyba, że Administrator wyraził na to zgodę (służbowy laptop).
9) Monitor komputera/laptopa i inne narzędzia danych z wyświetlaczem są ustawione w sposób uniemożliwiający wgląd osób trzecich w treść danych.
10) Jest ogólnie dostępne Ksero i skaner, na którym wykonuje się kopie dokumentów firmowych i potrzebnych do realizacji umowy. Skan zapisuje się na dedykowanym dla danego działu folderze, do którego dostęp mają pracownicy zgodnie z udzielonymi upoważnieniami.
11) Przestrzega się zasady czystego biurka – po skończonej pracy nośniki danych osobowych i inne materiały są przenoszone do wskazanego przez Administratora miejsca przechowywania. W trakcie pracy nie pozostawia się na biurku nośników danych i innych materiałów niekoniecznych do wykonywania obowiązków. W trakcie przerwy dane i ich nośniki są zabezpieczane przed

wglądem i dostępem osób trzecich: zamykane w szafce podblatowej, przenoszone na miejsce przechowywania, zwracane nadawcy. Zabrania się pozostawiania danych osobowych i ich nośników także w trakcie pracy w sposób umożliwiający odczytanie danych przez osoby trzecie (zewnątrz).

12) Przyjmując osobę trzecią lub innego pracownika, przy stanowisku pracy należy zabezpieczyć miejsce pracy w sposób uniemożliwiający odczytanie danych z nośników danych przez te osoby (nie pozostawiać na widoku, tekstem na wierzchu).
13) Po skończonej pracy lub w trakcie przerw należy zawsze wylogować się z systemu, wyłączając wszystkie aplikacje, pozostawiając komputer wyłączony z zabezpieczeniami lub w trybie wygaszacza ekranu z hasłem.
14) W trakcie chwilowych przerw, opuszczenia stanowiska pracy, zawsze należy włączyć wygaszacz ekranu z hasłem, zabezpieczyć stanowisko pracy przez osobami trzecimi, usunąć nośniki danych osobowych z biurka i je zabezpieczyć w szafkach podblatowych.
15) Po skończonej pracy lub jeżeli tego wymaga dłuższa przerwa w pracy zdać kierownikowi: klucze do pomieszczeń i szaf z ograniczonym dostępem i podlegających zwrotowi, rozliczyć się z wydanych nośników danych osobowych i narzędzi pracy pozostawionych w miejscu pracy, zwłaszcza jeżeli zawierają dane szczególnych kategorii i podlegają szczególnej ochronie.
16) W przypadku pracy na danych szczególnych kategorii należy: rozliczyć się każdego dnia na zakończenia pracy z nośników danych, zanieść i zamknąć we wskazanych szafach do przechowywania tych danych. Zdać informacje kierownikowi o zakończeniu pracy. Zabrania się przechowywać nośniki danych z danymi osobowymi szczególnych kategorii poza wydzielonym miejscem ich przechowywania w zamkniętych szafach. Niedozwolone jest pozostawienie tych nośników danych w szafkach podblatowych.
17) Dokumenty niepotrzebne, błędne, przeznaczone do zniszczenia są niszczone w niszczarkach firmowych. Zabrania się wyrzucania dokumentów (nośników danych osobowych) do kosza, nawet po zamazaniu, zniszczeniu treści. Jeżeli dokumenty zawierają dane szczególnych kategorii i są obszerne i nie można ich zniszczyć w niszczarce zawiadamia się Administratora i ww. osoby dokonują zamówienia usługi niszczenia dokumentów przez wyspecjalizowane firmy. Do czasu realizacji zlecenia dopuszcza się składowanie dokumentów do zniszczenia we wskazanym przez Administratora miejscu uniemożliwiającym ich zabranie lub nieuprawniony dostęp osób trzecich.

Procedura: Pracy na danych osobowych i nośnikach danych nieelektronicznych	
numer procedury: 5	
dotyczy:	wszystkich osób przetwarzających dane osobowe
osoby odpowiedzialne:	Upoważnieni do przetwarzania danych osobowych

1) Pliki papierowe – segregatory, nagłówki, widoczne dla osób trzecich zapisujemy w sposób uniemożliwiający identyfikację osoby, której dane dotyczą – **szyfrowanie.**
2) Nazwa nagłówków segregatorów, widoczna dla osób trzecich jest zapisywana: cyfrą, skrótem literowym, hasłowo lub w inny sposób.

3) Pliki znajdujące się w segregatorze, zbiorze dokumentów papierowych mogą być nazywane w sposób umożliwiających identyfikację osoby, której dotyczą, jeżeli jest to konieczne dla realizacji obowiązków/zadań (np. dokumenty kadrowe).
4) Zbiory danych osobowych kompletuje się w jednym miejscu w zakresie tego samego rodzaju dokumentów. Dane szczególnych kategorii są przechowywane zgodnie z zapisami powyżej.
5) Dane niekonieczne, po terminie obowiązku ich przechowywania czy na żądanie osoby, której dotyczą są usuwane trwale po zgłoszeniu Administratorowi, chyba że nie mogą być usunięte. Można nadać upoważnienie imienne pracownikowi do ich usuwania.
6) Nie tworzy się kopii dokumentów, jeżeli nie są konieczne. Kopie są tworzone dla celów realizacji zadań. Kopie dokumentów są przechowywane jak oryginały z zaznaczeniem, że to kopie lub „podpinane" pod oryginały.
7) Kopiowanie dokumentów odbywa się pod nadzorem pracownika. Nie można pozostawić kopiowanych danych w urządzeniu bez nadzoru, także w procesie drukowania. Po skończonym kopiowaniu sprawdza się stan (sztuki) wykonanych kopii i oryginał. Jeżeli nie ma odpowiedniej liczby kopii lub oryginału zgłasza się to jako incydent ochrony danych osobowych zgodnie z procedurą.
8) Zniszczenie lub trwałe zatrzymanie danych w drukarce, kopiarce zgłasza się zgodnie z procedurą incydentu ochrony danych osobowych.
9) Zapiski w kalendarzach ogólnodostępnych nie mogą stanowić podstawy identyfikacji osoby, której dotyczą, nie mogą zawierać danych osobowych.
10) Nie wolno zapisywać informacji z danymi osobowymi na kartkach typu post-it, naklejkach i innych dokumentach, które nie stanowią dokumenty końcowego, zwłaszcza zabrania się pozostawienia takich notatek na miejscu ogólnodostępnym (np. przy biurku).
11) Prowadzenie organizera, kalendarza osobistego jest dozwolone. Dane tam zapisywane nie powinny dotyczyć danych osobowych, chyba że jest to konieczne z uwagi na specyfikę pracy (np. praca sekretariatu). Takie dokumenty są chronione jak dane szczególnych kategorii. Dostęp do nich ma wyłącznie osoba upoważniona.

Procedura: Prowadzenia książki korespondencyjnej, dziennika wejść i wyjść	
numer procedury: 6	
dotyczy:	Osoby prowadzącej książkę korespondencyjną, dziennik wejść i wyjść
osoby odpowiedzialne:	Upoważnieni do przetwarzania danych osobowych

1) Książkę korespondencyjną prowadzi się jak kalendarz, organizer. Dostęp ma wyłącznie osoba upoważniona do wprowadzania w niej danych. W miarę możliwości zapisuje się wyłącznie dane konieczne, minimalizując ich zakres.
2) Każdy list naruszony (otwarty, uszkodzony) odnotowuje się wskazując zakres naruszenia i zawiadamia nadawcę o powyższym. Jeżeli naruszenie jest istotne zawiadamia się Administratora i postępuje zgodnie z wytycznymi w sprawie incydentu naruszenia danych osobowych.

Procedura: Przyjmowanie interesantów, obsługa zamówień i zapytań

numer procedury: 7	
dotyczy:	wszystkich osób przetwarzających dane osobowe
osoby odpowiedzialne:	Upoważnieni do przetwarzania danych osobowych

1) Realizuje się zasadę poinformowania o administrowaniu danymi osobowymi przy pierwszym kontakcie w formie e-mailowej, papierowej, nagrania głosowego, zawierające informację o miejscu przechowywania dokumentów RODO w formie elektronicznej w stopce e-maila, na dokumentach źródłowych pierwszego kontaktu, na dokumentach projektowych lub w inny przyjęty sposób.
2) Zamówienia, zapytania elektroniczne, wnioski i inna korespondencja elektroniczna jest przyjmowana jak każda poczta przychodząca. W miarę możliwości poczta ze skrzynki ogólnej jest przesyłana zgodnie z właściwością na skrzynki imienne lub rodzajowe. Usuwa się kopię ze skrzynki ogólnodostępnej. Usuwa się dane wrażliwe, niezanonimizowane i nie szyfrowane ze skrzynki ogólnej. Ze skrzynek rodzajowych dane wrażliwe są usuwane z poczty i zapisywane w miejscu docelowym do realizacji w pliku pdf lub innym, szyfrowane. Jeżeli wiadomość e-mailowa zawiera dane niekonieczne, lub których Administrator nie może przetwarzać, informuje się o tym nadawcę wiadomości, której dane dotyczą i dane te są usuwane (zanonimizowane).
3) Zamówienia i zapytania elektroniczne są realizowane bezpośrednio po zweryfikowaniu osoby, której zapytanie dotyczy. Zawsze dokonuje się weryfikacji tożsamości, chyba że tożsamość nadawcy nie budzi wątpliwości a także wiadomość e-mailowa nie spełnia przesłanek podrobienia, spamu, kradzieży danych osobowych. Odmawia się realizacji zapytania, jeżeli zachodzi obawa nieuprawnionego ujawnienia danych osobowych. Powiadamia się osobę o powyższym i o możliwość złożenia zapytania pisemnie lub w innej formie.
4) Nie udziela się informacji telefonicznych co do danych osobowych i szczegółów zamówienia, usługi, chyba że osoba – rozmówca potwierdzi swoją tożsamość w sposób umożliwiający jej pełną i dokładną identyfikację a Administrator posiada możliwość dokonania tej weryfikacji bez uszczerbku dla osoby, której dane dotyczą i z zapewnieniem ochrony danych osobowych przez nią przekazywanych. Zaleca się nagrywanie weryfikacji tożsamości i pouczenia o administrowaniu danymi osobowymi. Odpowiedzialność za odpowiednią identyfikację spoczywa na udzielającym wyjaśnień. Jeżeli identyfikacja nie jest możliwa, rozmówca odmawia identyfikacji lub nie można zweryfikować prawdziwości danych a także zawsze, kiedy zachodzi obawa nieupoważnionego dostępu do danych osobowych, nie udziela się wyjaśnień wskazując możliwość złożenia zapytania e-mailowego lub pisemnego.
5) Można prowadzić rejestr rozmów telefonicznych o czym zawiadamia się rozmówce przed rozmową, który wyraża zgodę na powyższe.
6) Przyjmowanie zamówień, zgłoszeń osobiście w biurze, wymaga zachowania zasad bezpieczeństwa i poufności. Osoba – klient, nie może podawać danych osobowych w obecności osób trzecich, które mogą je usłyszeć, zobaczyć. Należy zapewnić komfort i bezpieczeństwo podawania danych osobowych. Najlepiej przyjmować koniecznie dane w formie papierowej, na formularzu, bez ingerencji osób trzecich.
7) Przyjmowanie danych od klientów odbywa się w sposób uniemożliwiający dostęp osobom nieupoważnionym. Należy ograniczyć do minimum zakres osób, które mają kontakt z danymi.

8) Udostępnienie danych procesorom lub Administratorowi danych, gdy Spółka jest procesorem, odbywa się z wykorzystaniem komunikacji bezpiecznej, szyfrowanej. Zabrania się udostępniania innych danych, niż te które procesor uzyskał od Administratora lub osoby, której dane dotyczą a ona wyraziła zgodę na ich powierzenie. Należy ograniczyć zakres zbieranych danych do minimum.

Procedura: Obsługa zgłoszeń	
numer procedury: 8	
dotyczy:	wszystkich osób przetwarzających dane osobowe
osoby odpowiedzialne:	Upoważnieni do przetwarzania danych osobowych

1) Zgłoszenia przyjmuje się e-mailowo, osobiście lub pisemnie.
2) Zgłoszenia telefoniczne nie obejmują zbierania danych osobowych.
3) Umowy zawiera się papierowo i elektroniczne, jeżeli jest to możliwe.
4) Dane szczególnych kategorii pozyskuje się po zawarciu umowy od osób, których dane dotyczą. Dane te są przesyłane listownie lub z wykorzystaniem bezpiecznych kanałów komunikacji szyfrowanej.
5) Dane szczególnych kategorii są przesyłane listami poleconymi wyłącznie, pocztą kurierską lub e-mailem z szyfrowaniem danych na skrzynki pocztowe imienne lub rodzajowe. Zabrania się przesyłania listami zwykłymi niepoleconymi.
6) Możliwe jest przesłanie danych osobowych elektroniczne na skrzynkę pocztową pracownika uprawnionego, nie na ogólną pocztę firmową.
7) Korespondencję dotyczą organizacji usługi z danymi osobowymi przesyła się wyłącznie pocztą poleconą i przez uprawnione podmioty za pośrednictwem poczty służbowej e-mailowej, imiennej.

Procedura : Rekrutacji, składania ofert	
numer procedury: 9	
dotyczy:	wszystkich osób przetwarzających dane osobowe
osoby odpowiedzialne:	Upoważnieni do przetwarzania danych osobowych

1) Ogłoszenia zamieszcza się na portalach branżowych, na stronie internetowej Administratora.
2) Ogłoszenie zawiera opis rekrutacyjny z klauzulą RODO i zgodami dobrowolnymi i koniecznymi.
3) Rekrutacja odbywa się za pośrednictwem poczty firmowej z dostępem wyłącznie osób upoważnionych, nie poczty ogólnej lub listownie i osobiście.
4) Zgłoszenia nie zawierające klauzul koniecznych są usuwane. Nie podlegają rozpatrzeniu i archiwizacji.
5) Zgłoszenia zawierające dane osobowe niekonieczne do rekrutacji, bez zgód na ich wykorzystanie, są poddawane obróbce i zanonimizowane. Dane niekonieczne są usuwane (zakrywane trwale). Jeżeli jest zgoda kandydata to dane te nie są ukrywane, chyba że to dane szczególnych kategorii, co do których nie można ich przetwarzać nawet za zgodą i podlegają trwałemu usunięciu.

6) O czynności z ustępów 4-5 zawiadamia się osoby, których dane dotyczą, chyba że nie ma takiej możliwości.
7) Po rekrutacji dane są niszczone lub archiwizowane, w zależności do zgód osób, których dotyczą.
8) Po zrekrutowaniu podbiera się dalsze dane zgodnie z formą zatrudnienia i wyłącznie te dane, które są konieczne w ramach danej umowy.
9) W zakresie rekrutacji projektowej, w oparciu o przepisy ustawy prawo zamówień publicznych i inne ustawy szczególne w zapytaniu ofertowym w trybie nie przetargowym zamieszcza się informację o koniecznych dokumentach i wymogach oferty. Załącza się wzór umowy i inne konieczne postanowienia. W wyniku realizacji przetargu, zapytania ofertowego lub konkursu ofert wybór najkorzystniejszej oferty publikuje się na portalu konkurencyjności lub w innym wskazanym ustawą prawo zamówień publicznym miejscu. Wyłącznie publikuje się dane wymagane ustawą, w zakresie w niej określonym a oferent nie może wyrazić sprzeciwu co do publikacji, przyjmując w ofercie obowiązek spełnienia warunków ustawowych trybu wyboru oferty.
10) Jeżeli Administrator przetwarza dane zebrane nie od osoby, których dane przetwarza, należy w momencie pierwszego kontaktu poinformować daną osobę o sposobie pozyskania i celu przetwarzania.

Procedura: Obiegu dokumentów szczególnej kategorii (płacowo- kadrowych)	
numer procedury: 10	
dotyczy:	wszystkich osób przetwarzających dane osobowe
osoby odpowiedzialne:	Upoważnieni do przetwarzania danych osobowych

1) Akta osobowe prowadzi się zgodnie z kodeksem pracy, w zgodzie z przepisami ubezpieczeń społecznych i skarbowych.
2) Kadrami zajmują się osoby upoważnione. Zabrania się korzystania z danych osobowych podawanych w dokumentach kadrowych innych pracownikom. Są to dane uważane za dane szczególnej kategorii, zawierające również dane wrażliwe – dotyczące stanu zdrowia, oraz dane innych osób np. małoletnich dzieci.
3) Biuro kadrowo – rachunkowe prowadzi własną politykę ochrony danych osobowych na najwyższym poziomie i w zgodzie z prawem unijnym i krajowym w tym zakresie. Zawarto umowę powierzenia danych osobowych. Prowadzone są audyty spełniania obowiązków kadrowych i rachunkowych, zgodnie z procedurą ochrony danych osobowych.
4) Korespondencja kadrowa odbywa się pocztą poleconą lub za pośrednictwem poczty służbowej, imiennej lub rodzajowej, szyfrowanej i w miarę możliwości zanonimizowanej co do przedmiotu korespondencji.
5) Postępowanie z przekazaniem dokumentów kadrowo- płacowych reguluje polityka ochrony danych osobowych biura rachunkowego. Administrator weryfikuje czy stopień zabezpieczenia przesyłu danych w formie elektronicznej (e-mailowo) lub za pośrednictwem bezpiecznych kanałów komunikacji szyfrowanej, hasłowanej, spełniają podstawowe wymogi Administratora.
6) Dane szczególnych kategorii są dodatkowo chronione upoważnieniem do ich przetwarzania rodzajowego, upoważnieniem do przebywania w miejscu ich przechowywania, polityką wydania

kluczy i kart dostępu, ochroną przesyłania i hasłowania plików, katalogów danych, polityką nadawania przesyłek poleconych.

7) Dane osobowe na nośnikach danych wydawane są pracownikom, po przeszkoleniu w zakresie ochrony tych danych.
8) Dane szczególnych kategorii są przesyłane elektronicznie, hasłowane i szyfrowane, jeżeli jest to możliwe. Nie wydaje się kopii dokumentów zawierających te dane na nośnikach nieelektronicznych, chyba że wymaga tego przepis prawa lub nadzwyczajne okoliczności. Wydanie kopii dokumentów w wersji papierowej (np. zaświadczeń lekarskich) wymaga sporządzenia notatki służbowej zawierającej te informacje ze wskazaniem przyczyn sporządzenia i wydania takiego dokumentu danej osobie (imiennie). Notatki służbowej nie sporządza się, jeżeli jest to wymagane przepisem prawa (przesłanie do odpowiednich urzędów) i odnotowuje się w treści korespondencji.
9) Dokumenty zawierające dane osobowe przekazuje się zawsze w zalakowanej lub trwale zamkniętej kopercie. Wgląd w dokumenty w czasie od ich otrzymania do zdania, posiadają tylko osoby upoważnione i tylko w uzasadnionych wypadkach.
10) Zabrania się przekazywania dokumentów zawierających dane kadrowe, płacowe i inne dane szczególnie wrażliwe, osobom nieupoważnionym, nawet innym współpracownikom.
11) Dokumenty w czasie od wydania do zdania osoba upoważniona przechowuje w bezpiecznym miejscu, chroniąc przed dostępem osób trzecich. Jeżeli jest to konieczne dla bezpieczeństwa przewożonych danych Administrator zapewni bezpieczny transport.
12) Każdy przypadek utraty nośników danych lub możliwości ich nieupoważnionego udostępnienia zgłasza się Administratorowi, zgodnie z procedurą postępowania w przypadku incydentu ochrony danych osobowych.
13) Dokumenty zwracane kontrahentom zdaje się osobie upoważnionej i potwierdza protokołem zdania. Pozostała dokumentacja częściowa lub pełna w zależności od sytuacji, jest przesyłana listami poleconymi za potwierdzeniem odbioru (w szczególności, jeżeli zawiera dane szczególnych kategorii).
14) Udostępnienie dokumentów w czasie świadczenia usług jest możliwe jedynie osobom uprawnionym. Kontrolerzy wykazują swoje uprawnienie do wglądu w dane osobowe znajdujące się w dokumentach. Wpisuje się udostępnienia danych do rejestru udostępnień z podaniem podstawy kontroli dokumentów zawierających dane osobowe, zwłaszcza szczególnych kategorii. Zabrania się udostępnienia danych osobom nieupoważnionym lub bez upoważnienia. Możliwe jest okazanie części, dokumentów z wyłączeniem tych, które nie mieszczą się w upoważnieniu kontrolującego. Osoba upoważniona do reprezentacji Administratora w czasie kontroli ma obowiązek odmówić wydania dokumentów, zawierających dane osobowe, co do których kontrolujący nie posiada upoważnienia do przeprowadzenia kontroli. Jeżeli zachodzą wątpliwości należy zwrócić się do Specjalisty ds. RODO o zajęcie stanowiska.

Procedura: **Nośniki danych nieelektroniczne - zabezpieczenia i tryb postępowania z ich udostępnianiem**	
numer procedury: 11	
dotyczy:	wszystkich osób przetwarzających dane osobowe

osoby odpowiedzialne: Upoważnieni do przetwarzania danych osobowych

1) Za dokumenty księgowe odpowiadają Administrator i pracownik, które je otrzymał.
2) Pracownik zabezpiecza dokumentację księgową przed nieuprawnionym dostępem osób trzecich i przypadkowym ich ujawnieniu.
3) Zapewnia się na nośniki danych osobowych szafkę zamykaną na klucz z dostępem wyłącznie pracownika uprawnionego, bez dostępu osób trzecich i możliwości uzyskania klucza do tej szafki przez osoby postronne, w pokoju zamykanym na klucz, do którego dostęp ma pracownik upoważniony. Dostęp innych osób do pokoju, jeżeli nie jest możliwy do wyeliminowania powoduje obowiązek wykonania Procedury numer 1 i codziennego sprawdzania na początek i na koniec pracy zawartości szafy z nośnikami danych, w tym w zakresie kompletności, zgodności z rejestrem, nienaruszalności. Sprawdza się zabezpieczenia fizyczne dostępu do akt- zamków w szafce, stanu szafy. Każde odchylenie od normy i zauważone braki uznaje się za ważny incydent mogący doprowadzić do ujawnienia danych osobowych na szeroką skalę.
4) Udziela się upoważnienia osobom trzecim mającym stały dostęp do biura, w którym są nośniki danych osobowych, a są to pracownicy niezależni innych podmiotów, do przebywania w pomieszczeniu i przeszkala się na te osoby za ich zgodą z polityki ochrony danych osobowych. Za ich zgoda odbiera się zobowiązanie przestrzegania zasad ochrony danych osobowych Administratora.
5) Dokumenty przechowuje się kompletne. Sprawdza się stan dokumentów – liczbę sztuk, zakres, jeżeli jest uzasadniona obawa naruszenia tych danych. Zauważone braki, uszkodzenia się protokołuje i zgłasza Administratorowi, jeżeli są istotne lub naruszają PODO.
6) Udostępnienie dokumentów w czasie świadczenia usług jest możliwe jedynie osobom uprawnionym. Kontrolerzy wykazują swoje uprawnienie do wglądu w dane osobowe znajdujące się w dokumentach zawierających dane osobowe. Wpisuje się udostępnienia danych do rejestru udostępnień z podaniem podstawy kontroli dokumentów zawierających dane osobowe, zwłaszcza szczególnych kategorii. Zabrania się udostępnienia danych osobom nieupoważnionym lub bez upoważnienia. Możliwe jest okazanie części, dokumentów z wyłączeniem tych, które nie mieszczą się w upoważnieniu kontrolującego.
7) Dokumenty księgowe nie są wynoszone poza biuro, chyba że tego wymaga organizacja pracy lub nakazują przepisy prawa unijnego lub krajowego.
8) Pracownicy są zobowiązani dochować należytej staranności w zabezpieczeniu danych i ich nośników, w szczególności:
   e) zabezpieczyć miejsce przechowywania dokumentów,
   f) nie udostępniać danych osobom trzecim, nawet innym pracownikom,
   g) nie wynosić dokumentów poza biuro, chyba że jest to konieczne ze względów organizacyjnych lub taki obowiązek nakładają przepisy prawa unijnego lub krajowego,
   h) zwracać dokumenty na miejsce na koniec dnia roboczego lub po skończeniu zadania,
   i) dbać o stan dokumentów, uchronić je przed uszkodzeniem lub zniszczeniem,
   j) nie dokonywać poprawek na dokumentacji, chyba że na taką poprawkę wyrazi zgodę Administrator,
   k) uzupełniać dokumenty wyłącznie we wskazanych miejscach,
   l) nie przekazywać informacji o danych znajdujących się w dokumentach także osobom, których dotyczą, bez zgody uprawnionego wyrażonej na piśmie lub elektronicznie.

9) Pracownik przekazuje posiadaną dokumentację Administratorowi na każde wezwanie, może przekazać kontrolującemu wyłącznie za zgodą Administratora, potwierdzając legalność działania.
10) Każda osoba, która weszła w posiadanie dokumentów zawierających dane osobowe, winna niezwłocznie zabezpieczyć dokumenty, bez wglądu w ich treść i przekazać Administratorowi.
11) Każda osoba, która zauważyła nieuprawnione udostępnienie, pozostawienie, przekazanie dokumentów księgowych lub uważa, że mogło do tego dojść, postępuje według instrukcji incydentu naruszenia ochrony danych osobowych.

Procedura: **Privacy by default w Podmiocie**	
numer procedury: 12	
dotyczy:	wszystkich osób przetwarzających dane osobowe
osoby odpowiedzialne:	Upoważnieni do przetwarzania danych osobowych

DOMYŚLNE ZACHOWANIE PRYWATNOŚCI

1) Już na etapie projektowania i opracowywania sposobów przetwarzania danych, a ponadto także na każdym kolejnym etapie przetwarzania, należy uwzględniać obowiązek wdrożenia domyślnych ustawień prywatności.
2) Jego istotą jest wdrożenie przez Administratora odpowiednich środków technicznych i organizacyjnych, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są **niezbędne** dla osiągnięcia każdego konkretnego celu przetwarzania.
3) Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.
4) Zasada ta oznacza, że ustawienia prywatności stosowane przez Administratora mają mieć na celu maksymalną ochronę użytkownika.
5) Wprowadzenie zasady domyślnej ochrony danych jest równoznaczne z koniecznością podjęcia przez użytkownika dodatkowych kroków w przypadku, gdyby chciał swoją prywatność w jakikolwiek sposób ograniczyć, np. poprzez udostępnianie swoich danych większej liczbie osób fizycznych.
6) Zatem zmiana domyślnie stosowanej maksymalnej ochrony prywatności będzie następować jedynie na wyraźne żądanie użytkownika danego systemu czy oprogramowania.

Procedura: **Privacy by design**	
numer procedury: 13	
dotyczy:	wszystkich osób przetwarzających dane osobowe

osoby odpowiedzialne:	Upoważnieni do przetwarzania danych osobowych

1) Już na etapie projektowania i opracowywania sposobów przetwarzania danych, a ponadto także na każdym kolejnym etapie przetwarzania, należy uwzględniać obowiązujące zasady ochrony danych osobowych.

W szczególności należy zadbać o zachowanie zasad:

- minimalizacji przetwarzania danych osobowych,
- jak najszybszej pseudonimizacji danych osobowych,
- przejrzystości co do funkcji i przetwarzania danych osobowych,
- umożliwienia osobie, której dane dotyczą, monitorowania przetwarzania danych,
- umożliwienia Administratorowi tworzenia i doskonalenia zabezpieczeń.

2) Do obowiązków Administratora należy zapewnienie, by stosowane rozwiązania były zgodne z przepisami rozporządzenia i chroniły prawa osób, których przetwarzane dane dotyczą. Niemniej osoby upoważnione, przy wykonywaniu czynności służbowych, powinny mieć tę zasadę na względzie.

Procedura: **Usuwania danych osobowych**	
numer procedury: 14	
dotyczy:	wszystkich osób przetwarzających dane osobowe
osoby odpowiedzialne:	Upoważnieni do przetwarzania danych osobowych i usuwania danych

1) Niszczenie dokumentów zawierających dane osobowe powinno być dokonywane w sposób uniemożliwiający identyfikację osoby, której dane dotyczą.
2) Dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, dla realizacji których dane te są przetwarzane.
3) Dane osobowe powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.
4) Podczas ustalania zasad i okresów usuwania danych osobowych powinno uwzględniać się przepisy obowiązującego prawa oraz cele administratora.
5) Dane osobowe powinny zatem być usuwane wtedy, gdy:

- przepisy szczególne regulują obowiązek przetwarzania danych osobowych przez ustalony okres, np. przepisy prawa pracy, prawa podatkowego, ustawa o rachunkowości,

- jeżeli ustawodawca krajowy lub unijny nie reguluje okresu przechowywania danych osobowych, wówczas należy kierować się zasadą ograniczenia celu.

6) Terminy retencji danych osobowych zostały ustanowione w *Rejestrze czynności przetwarzania danych osobowych*. Niniejsze terminy są wykorzystywane przy opracowaniu treści obowiązku informacyjnego, który należy spełnić wobec osób, których dane przetwarza Administrator. Jednym z jego elementów jest konieczność wskazania okresu, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe kryteria ustalania tego okresu.
7) Ustalając okres przechowywania danych osobowych należy wziąć pod uwagę obecną i przyszłą wartość informacji, koszty, ryzyko i zobowiązania związane z przetwarzaniem danych osobowych.
8) Administrator wyznacza osoby odpowiedzialne w Podmiocie za przestrzeganie niniejszej Procedury.
9) Osoby odpowiedzialne regularnie sprawdzają czy dane są niezbędne do realizacji określonych celów.
10) Osoby odpowiedzialne dokonują okresowych przeglądów ustalonych okresów przechowywania danych osobowych, lokalizacji danych osobowych, a także faktycznej weryfikacji realizacji obowiązku usuwania danych osobowych.

USUWANIE DANYCH OSOBOWYCH

Usuwanie danych osobowych w formie papierowej.

1) Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do niszczenia dokumentów i tymczasowych wydruków w niszczarkach, niezwłocznie po ustaniu celu ich przetwarzania, zgodnie z *Rejestrem czynności przetwarzania danych osobowych*.

2) Dokumenty powinny być niszczone tak, aby nie sposób było odczytać zawartych w nich informacji.

Usuwanie danych osobowych w formie elektronicznej

1) Usuwanie danych osobowych ma charakter zautomatyzowany – poprzez odpowiednią konfigurację systemów informatycznych.

2) Systemy informatyczne powinny pozwalać na ustalanie okresów przechowywania danych osobowych, a także umożliwić sprawne usuwanie całości lub części danych. Jeżeli system nie zapewnia takiej funkcjonalności – dane usuwa osoba upoważniona.

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

Zatwierdził: Administrator

***:** dokument wewnętrzny. Do wdrożenia w Spółce. Należy przedłożyć każdemu pracownikowi (lub w dziale) i pozostawić do zapoznania się z możliwością wielokrotnego odczytania w formie papierowej, elektronicznej przesyłając na skrzynki służbowe. Można potwierdzić wdrożenie podpisem osób zapoznanych.

Dokument podpisany przez Martin Mokwa
Data: 2025.04.28 11:58:06 CEST