SCADI
AGENCJA CELNA & BIURO RACHUNKOWE

POLITYKA BEZPIECZEŃSTWA

PRZETWARZANIA I OCHRONY DANYCH OSOBOWYCH

W SCADI SP. Z O.O.

Dokument przyjęty Uchwałą Nr 11/2018

Zarządu Spółki SCADI Sp. z o.o.

z dnia 25 maja 2018 r.

Spis treści

1. CEL POLITYKI

Niniejszy dokument określa zasady bezpieczeństwa przetwarzania i ochrony danych osobowych jakie powinny być stosowane w SCADI Sp. z o.o. przez pracowników i współpracowników, którzy przetwarzają dane osobowe. Stosowanie zasad określonych w niniejszym dokumencie ma na celu zapewnienie prawidłowej ochrony danych osobowych przetwarzanych przez SCADI Sp. z o.o. rozumianej jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą, przetwarzaniem z naruszeniem obowiązujących przepisów prawa oraz utratą, uszkodzeniem lub zniszczeniem.

2. DOKUMENT ODNIESIENIA

Polityka bezpieczeństwa przetwarzania i ochrony danych osobowych w SCADI Sp. z o.o., zwana dalej Polityką, została wydana w związku z Rozporządzeniem Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.

3. ZAKRES STOSOWANIA

Politykę stosuje się do zaumatyzowanego oraz ręcznego przetwarzania danych osobowych, danych osobowych zapisanych na zewnętrznych nośnikach informacji, a także informacji dotyczących bezpieczeństwa przetwarzania danych osobowych, w szczególności dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.
W zakresie podmiotowym, Polityka obowiązuje wszystkich pracowników SCADI Sp. z o.o. oraz inne osoby mające dostęp do danych osobowych, w tym osoby zatrudnione na podstawie umowy zlecenia lub umowy o dzieło lub innej umowy cywilno-prawnej.

4. BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH

Przez bezpieczeństwo przetwarzania danych osobowych rozumie się zapewnienie:

- poufności – właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;
- integralności — właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- rozliczalności — właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych określone zostały w załączniku do niniejszej Polityki.

5. DEFINICJE

Na użytek niniejszego dokumentu:

1) „Rozporządzenie” oznacza Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
2) „dane osobowe” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie

fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

3) „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
4) „zbiór danych" oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
5) „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
6) „podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
7) „naruszenie ochrony danych osobowych" oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
8) „przedsiębiorca" oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;
9) „organ nadzorczy" oznacza organ centralnej władzy publicznej ustanowiony na podstawie polskiego prawa zgodnie z art. 51 Rozporządzenia;
10) "inspektor ochrony danych" – osoba wyznaczona przez kierownictwo, odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.
11) „Spółka" oznacza SCADI spółka z ograniczoną odpowiedzialnością;
12) "kierownictwo" oznacza Zarząd, organ zarządzający i reprezentujący SCADI Sp. z o.o.
13) "osoba upoważniona" – osoba posiadająca formalne upoważnienie wydane przez kierownictwo do przetwarzania danych osobowych.

6. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. SCADI Sp. z o.o. jest administratorem danych osobowych będących w jej posiadaniu. W ramach prowadzonej działalności gospodarczej i świadczonych usług Spółka jest także podmiotem przetwarzającym dane osobowe udostępnione przez innych administratorów (przedsiębiorców).
2. Administrator zapewnia, że dane osobowe będą:
   1) Przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
   2) Zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;

3) Adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
4) Prawidłowe i w razie potrzeby uaktualniane; administrator podejmuje wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
5) Przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane („ograniczenie przechowywania”);
6) Przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

3. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 2 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).
4. Cel i zakres przetwarzania danych osobowych przez SCADI Sp. z o.o., ich przechowywanie oraz prawa osób, których dane są przetwarzane zostały przedstawione w załączniku do niniejszej Polityki.

7. ZGODNOŚĆ PRZETWARZANIA Z PRAWEM

Administrator uznaje, że przetwarzanie danych osobowych jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

1) Osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
2) Przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
3) Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
4) Przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym,

a także innych warunków określonych w art. 6 Rozporządzenia.

8. PRZETWARZANIE SZCZEGÓLNYCH KATEGORII DANYCH OSOBOWYCH

Administrator – SCADI Sp. z o.o. – nie zbiera i nie przetwarza danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

9. PRAWO DOSTĘPU DO DANYCH OSOBOWYCH

Osobie, której dane są przetwarzane administrator zapewnia:

1) Prawo dostępu do danych osobowych jej dotyczących oraz następujących informacji:
   a) cele przetwarzania;
   b) kategorie odnośnych danych osobowych;
   c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
   d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe,

kryteria ustalania tego okresu;

e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
f) informacje o prawie wniesienia skargi do organu nadzorczego;
g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle.

2) Prawo do sprostowania danych;
3) Prawo do usunięcia danych („prawo do bycia zapomnianym”);
4) Prawo do ograniczonego przetwarzania,

w sposób i na zasadach określonych w sekcji 2 i 3 Rozporządzenia.

10. OBOWIĄZKI ADMINISTRATORA I KIEROWNICTWA

1. Administrator, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z Rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
2. Do obowiązków kierownictwa należy:
   1) Podejmowanie odpowiednich i niezbędnych kroków majach na celu zapewnienie prawidłowej ochrony danych osobowych;
   2) Podział zadań i obowiązków związanych z organizacją ochrony danych osobowych;
   3) Wprowadzenie do stosowania procedur zapewniających prawidłowe przetwarzanie danych osobowych;
   4) Egzekwowanie rozwoju środków bezpieczeństwa przetwarzania danych osobowych;
   5) Poddawanie przeglądom skuteczność polityki bezpieczeństwa przetwarzania danych osobowych;
   6) Zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia;
   7) Zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu;
   8) Zapewnienie niezbędnych środków potrzebnych dla zapewnienia bezpieczeństwa przetwarzania danych osobowych.
3. Kierownictwo wykonuje także zadania inspektora danych osobowych, które zostały jemu przypisane w art. 39 Rozporządzenia, z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

11. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie dostępu do nich osobom nieuprawnionym.
2. Do obowiązków należy również:
   1) Przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami;
   2) Postępowania zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych;

3) Zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia;
4) Ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
5) Informowania kierownictwa o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe.

12. PODMIOT PRZETWARZAJĄCY

Administrator powierzając przetwarzanie danych podmiotowi przetwarzającemu kieruje się wymaganiami określonymi w art. 28 Rozporządzenia, a w szczególności:

1. Korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą;
2. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.
3. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy, która podlega prawu cywilnemu oraz:
   a) wiąże podmiot przetwarzający i administratora,
   b) określa przedmiot i czas trwania przetwarzania,
   c) określa charakter i cel przetwarzania,
   d) określa rodzaj danych osobowych oraz kategorie osób, których dane dotyczą,
   e) określa obowiązki i prawa administratora,
   f) uwzględnia postanowienia zawarte w art. 28 ust. 3 Rozporządzenia.

13. BEZPIECZEŃSTWO PRZETWARZANIA

1. Administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:
   1) Pseudonimizację i szyfrowanie danych osobowych;
   2) Zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
   3) Zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
   4) Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
2. Wdrażając odpowiednie środki techniczne i organizacyjne uwzględnia się stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
3. 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.

4. Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że przepisy prawa stanowią inaczej.

14. ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. W przypadku naruszenia ochrony danych osobowych, administrator z zachowaniem postanowień art. 33 Rozporządzenia bez zbędnej zwłoki zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
2. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

15. BEZPIECZEŃSTWO FIZYCZNE OBSZARÓW PRZETWARZANIA

1. Obszar przetwarzania
   1) Dane osobowe mogą być przetwarzane wyłącznie w obszarach przetwarzania danych osobowych, na które składają się pomieszczenia biurowe Spółki;
   2) Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych, w sposób ograniczający możliwość dostępu do nich osobom nieuprawnionych;
   3) Wydruki i nośniki elektroniczne zawierające dane osobowe należy przechowywać w zamykanych szafach, które znajdują się w obszarach przetwarzania danych osobowych;
   4) Niepotrzebne wydruki lub inne dokumenty należy niszczyć za pomocą niszczarek;
   5) Przebywanie wewnątrz obszarów przetwarzania danych osobowych osób nieuprawnionych jest dopuszczalne tylko w obecności osoby upoważnionej.
2. Bezpieczeństwo urządzeń
   1) Urządzenia służące do przetwarzania danych osobowych należy przechowywać w bezpieczny i nadzorowany sposób;
   2) Urządzenia mobilne takie jak np. komputery przenośne, tablety, smartfony i telefony komórkowe nie powinny być pozostawiane bez opieki jeżeli nie są zastosowane odpowiednie środki ochrony.
3. Fizyczna kontrola dostępu
   1) Stosowane procedury eksploatacyjne powinny zapewnić ochronę danych osobowych oraz dokumentacji systemowej przed nieautoryzowanym lub nieuprawnionym ujawnieniem, modyfikacją, usunięciem i zniszczeniem;
   2) Spółka stosuje politykę czystego biurka i czystego ekranu w celu redukcji ryzyka nieautoryzowanego i nieuprawnionego dostępu lub uszkodzenia danych osobowych;
   3) Kończąc pracę, każda osoba przetwarzająca dane osobowe zobowiązana jest zabezpieczyć swoje stanowisko pracy, w szczególności wszelką dokumentację, wydruki, elektroniczne nośniki informacji i umieścić je w zamykanych szafkach;
   4) Monitory komputerów należy ustawiać w taki sposób aby uniemożliwiać podgląd wyświetlanych danych osobowych przez osoby nieuprawnione;
   5) W przypadku korzystania z usług zewnętrznych podmiotów oferujących odbiór i niszczenie dokumentów

lub nośników zawierających dane osobowe, należy wybierać wykonawcę posiadającego odpowiednie doświadczenie i dysponującego środkami gwarantującymi wysoki poziom bezpieczeństwa.

16. OCENA RYZYKA I PRZEGLĄDY

1. Systemy informatyczne i aplikacje należy poddawać okresowej ocenie ryzyka pod kątem identyfikacji zagrożeń dla bezpieczeństwa przetwarzania danych osobowych.
2. Należy przeprowadzać okresowe przeglądy bezpieczeństwa przetwarzania danych osobowych w celu określenia wymaganego poziomu zabezpieczeń pozwalającego na ograniczenie ryzyka do poziomu akceptowalnego.
3. Narzędzia informatyczne służące do oceny ryzyka bezpieczeństwa przetwarzania danych należy chronić przed nieautoryzowanym lub nieuprawnionym dostępem a ich użycie powinno być odpowiednio kontrolowane.

17. ZARZĄDZANIE INCYDENTAMI

1. Zaistniałe incydenty związane z bezpieczeństwem przetwarzania danych osobowych powinny być rejestrowane i monitorowane w celu ich zidentyfikowania i zapobiegania wystąpieniu w przyszłości.
2. Zdarzenia systemowe powinny być przechowywane jako materiał dowodowy zaistniałych incydentów związanych z bezpieczeństwem przetwarzania danych osobowych.
3. Użytkownicy systemów zobowiązani są poznać i przestrzegać zasady zgłaszania incydentów związanych z bezpieczeństwem przetwarzania danych osobowych.
4. Zaistniałe zdarzenia związane z naruszeniem lub podejrzeniem naruszenia bezpieczeństwa przetwarzania danych osobowych takie jak np. utrata integralności, niedostępność, awarie, uszkodzenia, ostrzeżenia i alarmy bezpieczeństwa systemów informatycznych, urządzeń teleinformatycznych oraz danych powinny być niezwłocznie zgłaszane kierownictwu Spółki.

18. POSTANOWIENIA KOŃCOWE

1. Kierownictwo i pracownicy SCADI Sp. z o.o. przy przetwarzaniu danych osobowych zobowiązani są do stosowania postanowień zawartych w Rozporządzeniu i w niniejszej Polityce.
2. W wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących w Spółce, użytkownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.
3. Administrator świadomy jest odpowiedzialności karnej i administracyjnej, która na nim ciąży za nieprzestrzeganie przepisów o ochronie danych osobowych zawartych w Rozporządzeniu i innych przepisach prawa.

19. ZAŁĄCZNIKI

Załącznik 1: Cel i zakres przetwarzania danych osobowych, ich przechowywanie oraz prawa osób, których dane są przetwarzane

Administrator danych osobowych	Administratorem danych osobowych jest SCADI Sp. z o.o. z siedzibą 02-255 Warszawa, ul. Krakowiaków 103, wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie pod nr KRS 0000440355, NIP 5223001306, REGON 146394655
Dane kontaktowe administratora – SCADI Sp. z o.o.	Z administratorem można się kontaktować: • telefonicznie pod numerem: 22 868 11 08; • pocztą elektroniczną pod adresem e-mail: biuro@scadi.pl; • pisemnie przesyłając korespondencję na adres: SCADI Sp. z o.o., 02-255 Warszawa, ul. Krakowiaków 103
Cele przetwarzania danych, podstawa prawna oraz prawnie uzasadnione interesy SCADI Sp. z o.o.	Administrator przetwarza dane osobowe w celu: • zawarcia i wykonania umów łączących SCADI Sp. z o.o. z pracownikami oraz współpracownikami, klientami i kontrahentami – przetwarzanie jest niezbędne do realizacji umów (art. 6 ust. 1 lit. b Rozporządzenia); • ustalenia, dochodzenia lub obrony przed roszczeniami związanymi umowami lub przetwarzaniem danych osobowych, jeżeli przetwarzanie jest niezbędne do realizacji prawnie uzasadnionego interesu administratora (art. 6 ust. 1 lit. f Rozporządzenia); • spełnienia ciążących na administratorze obowiązków prawnych wynikających z prawa Unii Europejskiej lub prawa polskiego (m.in. wobec organów administracji celno-skarbowej lub organów ubezpieczeń społecznych), jeżeli przetwarzanie jest niezbędne do wypełnienia wymogów prawnych, którym podlega administrator (art. 6 ust. 1 lit. c Rozporządzenia)
Kategorie odbiorców danych	Odbiorcami danych osobowych mogą być podmioty z następujących kategorii: • upoważnione na podstawie obowiązujących przepisów prawa (zwłaszcza sądy i organy władzy publicznej); • świadczące usługi m.in.: – pocztowe i kurierskie; – archiwizacji danych; – informatyczne; – telekomunikacyjne; – prawne i windykacyjne; – audytorskie i kontrolne; – obsługi finansowej; – wynikające z obowiązków pracodawcy.
Okres przechowywania danych osobowych	Administrator przetwarza dane osobowe w celu: • wykonania umów – do momentu ich wygaśnięcia lub rozwiązania; • wypełnienia przez administratora obowiązków prawnych – do momentu wygaśnięcia obowiązków przechowywania danych wynikających z przepisów prawa; • innych celów związanych z działalnością gospodarczą SCADI Sp. z o.o. - do momentu osiągnięcia zamierzonego celu lub jego zaniechania.
Prawa przysługujące osobie, której dane są przetwarzane	Osoba, której dane są przetwarzane ma prawo: • dostępu do treści swoich danych osobowych, ich sprostowania (poprawiania, uzupełniania), ograniczenia ich przetwarzania lub usunięcia („prawo do bycia zapomnianym”);

	• do przenoszenia danych osobowych dostarczonych administratorowi bądź żądania, jeżeli jest to technicznie możliwe, przesłania tych danych innemu administratorowi; w celu skorzystania z powyższych praw należy kontaktować się z administratorem – SCADI Sp. z o.o. Dane kontaktowe wskazane są wyżej; • w celu wniesienia skargi do organu nadzorczego powołanego do ochrony danych osobowych w przypadku uznania, że przetwarzanie danych osobowych narusza przepisy Rozporządzenia.
Prawo do sprzeciwu	Osoba, której dane są przetwarzane ma prawo, bez względu na przyczynę, do wniesienia w dowolnym momencie sprzeciwu wobec przetwarzania danych osobowych na potrzeby marketingu bezpośredniego, w tym profilowania. W przypadku wniesienia sprzeciwu administrator odstąpi od przetwarzania danych w tym celu. Osoba, której dane są przetwarzane ma również prawo wniesienia w dowolnym momencie sprzeciwu wobec przetwarzania danych osobowych w celu ustalenia, dochodzenia lub obrony przed roszczeniami związanymi z zawartymi umowami lub z przetwarzaniem danych osobowych.
Źródło pochodzenia danych i kategorie danych	Dane osobowe niezbędne do wykonania zawartych umów administrator pozyskuje od swoich pracowników oraz współpracowników, klientów i kontrahentów. Dane osobowe są także przekazywane SCADI Sp. z o.o. w ramach powierzenia przetwarzania danych osobowych przez innych administratorów. Zbierane i przetwarzane dane osobowe obejmują głównie: • imiona i nazwiska, • daty urodzenia, • numery PESEL i/lub numery NIP, • adresy zamieszkania i/lub adresy prowadzenia działalności gospodarczej, • numery telefonów, • adresy poczty elektronicznej, • właściwe organy administracji celno-skarbowej, • dane identyfikacyjne dla potrzeb organów ubezpieczeń społecznych, • numery kont bankowych.
Informacja o wymogu lub dobrowolności podania danych osobowych oraz konsekwencjach ich niepodania	Podanie danych osobowych administratorowi jest dobrowolne, ale niezbędne do zawarcia i wykonania umów, w których stroną jest SCADI Sp. z o.o.
Przekazywane danych poza Europejski Obszar Gospodarczy	SCADI Sp. z o.o. nie zleca wykonania usług i zadań usługodawcom mającym siedzibę poza Europejskim Obszarem Gospodarczym (w „państwie trzecim”).

Załącznik 2: Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Dane osobowe są chronione przy zastosowaniu następujących zabezpieczeń niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych dany osobowych:

1. Ochrona pomieszczeń wykorzystanych do przetwarzania danych osobowych:
   - pomieszczenia, w których zlokalizowano przetwarzanie danych osobowych zabezpieczone są przed dostępem osób nieuprawnionych;
   - dokumentacja papierowa po godzinach pracy jest przechowywana w zamykanych biurkach lub szafach;
   - przebywanie osób nieupoważnionych w obszarze przetwarzania danych osobowych jest dopuszczalne wyłącznie za zgodą kierownictwa.

2. Przedsięwzięcia w zakresie zabezpieczenia sprzętu komputerowego:
   - dla zapewnienia ciągłości działania systemów informatycznych służących do przetwarzania danych osobowych stosuje się w nich sprzęt oraz aplikacje wyprodukowane przez renomowanych producentów oraz zabezpiecza się sprzęt przed awarią zasilania lub zakłóceniami w sieci zasilającej;
   - zbiory danych osobowych oraz aplikacje służące do przetwarzania danych osobowych są zabezpieczane przed przypadkową utratą albo celowym zniszczeniem poprzez wykonywanie kopii zapasowych;
   - kopie zapasowe są usuwane niezwłocznie po ustaniu ich użyteczności.

3. Przedsięwzięcia w zakresie ochrony teletransmisji danych:
   - w celu ochrony systemów informatycznych służących do przetwarzania danych osobowych przed zagrożeniami pochodzącymi z Internetu stosuje się zabezpieczenia chroniące przed nieuprawnionym dostępem;
   - transmisja danych osobowych przez publiczną sieć telekomunikacyjną jest zabezpieczona środkami kryptograficznej ochrony danych;

4. Przedsięwzięcia w zakresie środków ochrony w ramach oprogramowania systemów:
   - w celu zapewnienia rozliczalności operacji dokonywanych przez użytkowników systemu informatycznego, w systemie tym dla każdego użytkownika rejestrowany jest odrębny identyfikator i hasło;
   - do uwierzytelnienia użytkowników używa się identyfikatora i hasła, które składa się z co najmniej 8 znaków, i jest skonstruowane w sposób nie trywialny, w szczególności zawiera małe i duże litery, cyfry oraz znaki specjalne;
   - hasła służące do uwierzytelniania w systemach informatycznych służących do przetwarzania danych osobowych są zmieniane co najmniej raz na 30 dni;
   - w przypadku gdy system informatyczny służący do przetwarzania danych osobowych nie wymusza zmiany haseł, użytkownik jest zobowiązany do samodzielnej zmiany hasła po upływie 30 dni.

5. Przedsięwzięcia w zakresie środków ochrony w ramach narzędzi baz danych i innych narzędzi programowych:
   - w celu ochrony zbiorów danych osobowych prowadzonych w systemach informatycznych przed nieuprawnionym dostępem stosuje się mechanizmy kontroli dostępu do tych danych;
   - stosuje się oprogramowanie umożliwiające trwałe usunięcie danych osobowych z urządzeń, dysków lub innych elektronicznych nośników informacji, które przeznaczone są do naprawy, przekazania lub likwidacji przez osobę nieuprawnioną;

6. Przedsięwzięcia w zakresie środków ochrony w ramach systemu użytkowego:
   - w celu ochrony danych osobowych przetwarzanych na stacjach roboczych na czas krótkotrwałego opuszczenia stanowiska pracy przez użytkownika systemu, stosuje się mechanizm blokady stacji roboczej zabezpieczony hasłem;
   - na stacjach roboczych użytkownicy niedopuszczalne jest instalowanie nieautoryzowanego oprogramowania;
   - stosuje się oprogramowanie antywirusowe z automatyczną aktualizacją w celu ochrony systemu przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
   - kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie jak i do celów instalacyjnych.

7. Przedsięwzięcia w zakresie środków organizacyjnych.
   - dostęp do danych osobowych możliwy jest po uzyskaniu formalnego upoważnienia do przetwarzania danych osobowych wydanego przez kierownictwo Spółki;
   - monitoruje się wdrożone zabezpieczenia systemu informatycznego.