

Szanowni Państwo,

w związku ze świadczoną przez nas usługą, przesyłamy istotne informacje dotyczące przetwarzania danych osobowych w systemie SISMS. Zwracamy uwagę, iż zgodnie z wymaganiami RODO* zobowiązani są Państwo do zachowania przejrzystości wobec mieszkańców, którzy rejestrują się w Państwa serwisach informacyjnych w systemie SISMS.

Niniejsza wiadomość kierowana jest do osób, które zajmują się ochroną danych osobowych w Państwa instytucji oraz do osób odpowiedzialnych za zamieszczenie informacji na Państwa stronach www.

Prosimy o zapoznanie się z informacjami podanymi w załączniku do niniejszej wiadomości i uwzględnienie ich w prowadzonej przez Państwa dokumentacji dotyczącej ochrony danych osobowych - rejestrze czynności przetwarzania danych osobowych.

Ponadto, prosimy o zwrócenie szczególnej uwagi na udostępnienie na Państwa głównej stronie www informacji o systemie SISMS w prawidłowy sposób, tj.:

1. wyjaśnić w jakim celu i zakresie będziecie Państwo przysyłać informacje [przykład1](#) [przykład2](#)
2. prawidłowo podpiąć formularz rejestracyjny on-line, czyli tak, aby po jego otwarciu była dostępna treść spełniająca obowiązek informacyjny wymagany przez RODO [przykład](#).

W przypadku pytań prosimy o kontakt z panią Marią Kozłowską
email: maria.kozlowska@sisms.pl

W celu zweryfikowania i uzupełnienia prowadzanego przez SISMS Sp. z o.o. rejestru czynności przetwarzania, a w przypadku podpisanej umowy powierzenia również Rejestru kategorii, prosimy o przesłanie **aktualnego kontaktu do Państwa Inspektora Ochrony Danych. Informacje bardzo prosimy przysyłać pocztą elektroniczną na adres: kontaktiod@sisms.pl**

Przygotowując niniejszą wiadomość staraliśmy się zebrać i dostarczyć Państwu jak najwięcej informacji dotyczących przetwarzania danych w systemie SISMS. Mamy nadzieję, że udostępnione informacje uwzględniają Państwa potrzeby będą pomocne przy tworzeniu i utrzymaniu dokumentacji wymaganej Ogólnym rozporządzeniem o ochronie danych. Jako dostawca usługi dokładamy wszelkich starań, aby przetwarzanie danych osobowych było bezpiecznie i transparentne dla podmiotów, z którymi współpracujemy. Z tego powodu będziemy Państwa informować na bieżąco o wszelkich zmianach i zaleceniach związanych ze świadczoną przez nas usługą.

Dziękujemy za zaufanie i liczymy na dalszą owocną współpracę, również w zakresie ochrony danych osobowych.

*Rozporządzenia 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.

Z pozdrowieniami,

Zespół SISMS Sp. z o.o.

Samorządowy Informator SMS Sp. z o.o.
ul. Kasprowicza 46
51-137 Wrocław

SPEŁNIENIE WYMAGAŃ RODO W SYSTEMIE SISMS

Pragniemy poinformować, iż system SISMS, z którego Państwo korzystacie, spełnia następujące wymagania.

1. Zgody w SISMS

- Zgodę uzyskuje się na podstawie pełnych i poprawnych informacji.
- Nie pozyskuje się zgody pod przymusem.
- Wszystkie otrzymane zgody są rejestrowane i zarządzane.
- Po wycofaniu zgody osoby, przetwarzanie danych osobowych zostaje wstrzymane.
- W przypadku zmiany zgody lub braku odnowienia starych zgód przetwarzanie danych osobowych zostaje zatrzymane.

2. Przejrzystość przetwarzania w SISMS

- Polityka prywatności jest łatwo dostępna (udostępniona na stronie internetowej).
- Klauzula informacyjna jest dostępna w języku polskim.
- Za każdym razem, gdy pojawiają się zmiany w usłudze, celu lub podstawowej aplikacji, informacje opisujące usługę i oświadczenia o ochronie prywatności są odpowiednio aktualizowane.
- Informacje podstawowe opisujące usługę są udostępniane podmiotowi danych w Regulaminie.
- Kolejne wersje Regulaminów są zachowane i dostępne na stronie internetowej.
- Klauzule informacyjne są napisane zrozumiałym i prostym językiem.
- W klauzuli informacyjnej każdy cel jest powiązany z podstawą prawną.
- Klauzule online są dobrze zindeksowane i można je wyszukiwać.

3. Poprawność / Prawdliwość

- Dane są wprowadzane przez osobę, której dane dotyczą.
- Wprowadzenie błędnych danych uniemożliwia potwierdzenie rejestracji. Błędne dane są usuwane.
- Możliwe jest usunięcie nieaktywnych użytkowników na zlecenie Administratora danych.
- System definiuje minimalny zakres danych.
- Użytkownicy mają własne narzędzia do zarządzania danymi, które umożliwiają korektę lub usunięcie danych.

4. Minimalizacja danych

- Zbierane są tylko te dane, które są potrzebne do określonego celu.
- Dane przechowywane do analizy i statystyk są pseudonimowane.
- W grupach publicznych Nadawca może nadawać komunikaty bez bezpośredniego dostępu do danych osobowych.
- Określono cele i zakres danych przetwarzanych do realizacji danego celu.

5. Ograniczenie celu

- Pracownicy pracujący z danymi są informowani o celu gromadzenia danych.
- Koncepcja autoryzacji opiera się na profilach użytkowników.
- Wprowadzono zasady przyznawania i zatwierdzania dostępu do systemu.
- Okresowo wykonuje się przeglądy uprawnień u Dostawcy.
- Dostęp do danych następuje po uwierzytelnieniu za pomocą mechanizmów uwierzytelniania.
- Dostęp do danych i przetwarzanie danych jest rejestrowany na poziomie wystarczającym do wykrycia potencjalnego nadużycia lub przetwarzania w innym celu niż określony.
- Ustanowiono mechanizmy zapewniające pozyskiwanie oddzielnej zgody do przetwarzania danych do realizacji nowych lub dodatkowych celów.

6. Obsługa podmiotów danych

- System SISMS obsługuje funkcję wyszukiwania, która pozwala na wyszukanie pojedynczych rekordów.
- System SISMS obsługuje oznaczanie i ukrywanie niektórych zestawów danych dla niektórych typów przetwarzania.
- System SISMS obsługuje usuwanie poszczególnych danych.
- Żądania osób są przetwarzane indywidualnie.
- System SISMS jest w stanie umożliwić każdemu podmiotowi danych skuteczne zażądanie i przeprowadzenie korekty, usunięcia lub zablokowania jego danych.

7. Przetwarzanie za pomocą systemu

- Zasady przetwarzania danych w systemie jest opisana i udostępniona w Regulaminach.
- Osoby są informowane, że mogą swobodnie wyrejestrować się z usługi.
- Sprzeciwy osób są rozpatrywane indywidualnie.

8. Powiadamianie

- Wszyscy podwykonawcy biorący udział w procesie są zidentyfikowani i dostępni dla Dostawcy.
- Powiadomienia są wysyłane do osoby, której dane dotyczą, kiedy planowane jest ujawnienie jej danych osobowych stronom trzecim.
- Jednostka jest wyposażona w mechanizm samoobsługi, który pozwala zapisać i wypisać się z usług danego Nadawcy.
- Wysyłane jest powiadomienie, które opisuje zmiany, w przypadku zmiany danych, aktualizacji lub udostępnienia.

9. Transfery poza EOG

- Dane osobowe są przechowywane na terenie Polski.

10. Usuwanie danych

- Rozwiązania IT umożliwiają (ręczne) usunięcie zestawów danych.
- System usuwania umożliwia usuwanie:
 - o pełnego zapisu dotyczącego 1 osoby,
 - o pełnej dokumentacji grupy osób,
 - o część rekordu (określone pola danych).
- Dane, które nie są już potrzebne do określonego celu, są usuwane lub zanonimizowane.

ZABEZPIECZENIE PRZETWARZANIA DANYCH OSOBOWYCH

Zachowując należytą staranność w procesie przetwarzania danych osobowych oraz w celu zapewnienia właściwej komunikacji i przejrzystości, przesyłamy informacje o sposobie zabezpieczenia zastosowanie w SISMS sp. z o.o.

1. Inspektor Ochrony Danych.

Został wyznaczony Inspektor Ochrony Danych.

2. Osoby odpowiedzialne za proces przetwarzania danych osobowych

Wyznaczono osobę odpowiedzialną za bezpieczeństwo techniczne oraz osobę odpowiedzialną za organizację współpracy z poszczególnymi podmiotami w ramach świadczenia usługi.

3. Dokumenty dotyczące ochrony danych osobowych

Następujące działania zostały podjęte w celu osiągnięcia zgodności z Ogólnym rozporządzeniem o ochronie danych:

- Opracowano Rejestr czynności przetwarzania oraz Rejestr kategorii przetwarzania dokonywanych w imieniu innych administratorów.
- Wdrożono zabezpieczenia w postaci szyfrowanego połączenia https.
- Wdrożono proces postępowania z incydentami bezpieczeństwa informacji.
- Wdrożono procedury nadawania uprawnień do przetwarzania danych osobowych.
- Wdrożono procedury dotyczące korzystania z Internetu i poczty elektronicznej.
- Wdrożono zasady dotyczące uwierzytelniania w systemach informatycznych,
- Wdrożono procedury postępowania w przypadku awarii systemu informatycznego.
- Wdrożono narzędzie do monitorowania infrastruktury informatycznej.
- Wdrożono procedury zachowania ciągłości działania.
- Wdrożono regulamin użytkownika komputerów przenośnych.
- Wdrożono procedurę ochrony antywirusowej i zabezpieczeń sieciowych.
- Wdrożono procedurę wykonywania kopii bezpieczeństwa danych.
- Wdrożono procedurę niszczenia nośników danych.
- Pracownicy zostali przeszkoleni w zakresie ochrony danych osobowych.
- Pracownicy zostali przeszkoleni w zakresie wymaganych zabezpieczeń, w tym zabezpieczeń technicznych.
- Pracownicy zostali poinformowani o obowiązku zgłaszania incydentów i naruszeń bezpieczeństwa danych i znane są procedury zgłoszenia incydentów i naruszeń do Administratora danych.
- Pracownicy zostali zobowiązani do zachowania poufności.
- Wprowadzono zasady wprowadzania zmian w systemie informatycznym.

Posiadany wdrożone wewnętrzne dokumenty regulujące przetwarzanie danych osobowych, wśród których można wymienić:

- Politykę Bezpieczeństwa Ochrony Danych Osobowych.
- Instrukcję Zarządzania Systemem Informatycznym.
- Procedurę nadawania uprawnień do przetwarzania danych osobowych.
- Procedurę dotyczące korzystania z Internetu i poczty elektronicznej.

- Procedurę postępowania w przypadku awarii systemu informatycznego.
- Procedurę zachowania ciągłości działania.
- Procedurę ochrony antywirusowej i zabezpieczeń sieciowych.
- Procedurę wykonywania kopii bezpieczeństwa danych.
- Procedurę niszczenia nośników danych.

4. Zespół dedykowany ds. bezpieczeństwa informacji

Został powołany IDO oraz wyznaczona jest osoba odpowiedzialna za bezpieczeństwo techniczne przetwarzanych danych.

5. Zatwierdzenie dostępu do danych z ramienia SISMS sp. z o.o.

Dla osób działających w imieniu Spółki SISMS sp. z o.o. wydawane jest pisemne upoważnienie do danych. Upoważnienia udziela Prezesa Zarządu SISMS sp. z o.o..

6. Mechanizmy uwierzytelnienia użytkownika

Uwierzytelnienie w systemie następuje za pomocą loginu i hasła.

7. Nadzór na przetwarzaniem danych osobowych

Zastosowano narzędzia umożliwiające monitorowanie infrastruktury oraz zastosowano narzędzia umożliwiające odnotowanie informacji o działaniach użytkowników w systemie.

8. Wykonywanie kopii zapasowych

Pełne kopie zapasowe wykonywane są automatycznie. Dla Systemu SISMS kopia wykonywane jest z częstotliwością 4 razy na dobę w określonych godzinach.

Nośniki kopii: dyski serwerów.

9. Szkolenia personelu SISMS sp. z o.o.

Pracownicy SISMS sp. z o.o. zostali przeszkoleni oraz otrzymali odpowiednie przeszkolenie, instrukcje i wytyczne zapewniające bezpieczeństwo przetwarzanych danych.

10. Wyodrębnienie danych

Dane są przetwarzane w sposób umożliwiający odseparowanie/ rozdzielanie danych od danych innych podmiotów.

11. Naruszenie ochrony danych

SISMS sp. z o.o. posiada procedurę postępowania w przypadku naruszenia ochrony danych osobowych. Procedura zakłada, między innymi, następujące działania: zabezpieczenie przez dalszym dostępem osób nieupoważnionych do danych, ocenę sytuacji, identyfikację źródła, zbieranie dowodów i dokumentowanie działań, analizy, działania naprawcze, przywrócenie funkcjonowania systemu.

12. Usunięcie danych po zakończeniu okresu przetwarzania

Dane z systemu zostaną usunięte lub zostaną poddane anonimizacji.

13. Udostępnienie danych innym administratorom

Udostępnienie danych w grupach publicznych może być realizowane za zgodą osoby, której dane dotyczą.

Udostępnienie danych w grupach niepublicznych może być realizowane na podstawie polecenia wydanego przez administratora danych.

14. Dalsze powierzenie danych osobowych

Przy realizacji usługi, SISMS powierza dane osobowe następującym dostawcom:

- T-Mobile Polska S.A. ul. Marynarska 12, 02-674 Warszawa, NIP: 5261040567, KRS: 391193, REGON: 011417295; Powierzenie w celu zapewnienia kolokacji serwerów.
- ATM S.A. ul. Grochowska 21a, 04-186 Warszawa, NIP: 1130059989, KRS: 34947, REGON: 012677986. Powierzenie w celu zapewnienia kolokacji serwerów.

W celu zapewnienia korzystania z usług „zdalnej ręki” w kolokacji T-MOBILE, dane są podpowierane do ASTA Telekom Servis Sp. z o.o., Solec 78E, 05-532 Solec.

15. Zabezpieczenia fizyczne kolokacji

Zastosowano: zamykane drzwi, system alarmowy, wydzielone serwery odseparowane w zamykanej szafie, szafa w serwerowni zamykana na klucz.

16. Umowy powierzenia

Podpisano umowy powierzenia z dostawcami kolokacji serwerów.

17. Przekazywanie danych poza EOG

Nie dotyczy. Dane są przetwarzane wyłącznie na terenie Polski.

18. Zabezpieczenie transferu danych

Wdrożono zabezpieczenia w postaci szyfrowanego połączenia https dla systemu SISMS.

19. Prawa osób, których dane dotyczą

Zapewniono możliwość wycofania zgody na przetwarzanie danych.

Ustalono kanał komunikacji w sprawach związanych z realizacją praw osób.

Żądania inne niż żądanie wycofania zgody na przetwarzanie danych są rozpatrywane indywidualnie.

Pracownicy zostali przeszkoleni w zakresie praw przysługującym podmiotom danych.

ODPOWIEDZIALNOŚCI PRZY PRZETWARZANIU DANYCH W SYSTEMIE SISMS

W procesach przetwarzania danych osobowych Samorządowy Informator SMS sp. z o.o. pełni następujące role.

W procesie przetwarzania danych osobowych w odniesieniu do danych **w grupach niepublicznych** Samorządowy Informator SMS sp. z o.o. pełni rolę podmiotu przetwarzającego, któremu administrator powierzył dane zgodnie z art. 28 Ogólnego rozporządzenia o ochronie danych w oparciu o zawartą umowę powierzenia danych osobowych.

W procesie przetwarzania danych osobowych w odniesieniu do danych **w grupach publicznych** zarówno Samorządowy Informator SMS sp. z o.o. oraz Klient pełnią rolę współadministratorów, o których mowa w art. 26 Ogólnego rozporządzenia o ochronie danych. Warunki współadministrowania zostały określone zawartą umową, a w szczególności „Regulaminem świadczenia Usług drogą elektroniczną dla Klientów z wykorzystaniem Systemu SISMS”, który stanowi integralną część zawartej umowy.

Fakt współadministrowania został skonsultowany z kancelarią prawną, którą w przygotowanej opinii prawnej poparła to rozwiązanie. Więcej informacji na temat współadministrowania zostało podane poniżej.

WSPÓŁADMINISTROWANIE W GRUPACH PUBLICZNYCH

Współadministratorzy	Usługodawca	Klient / Nadawca
Dane Współadministratorów	Samorządowy Informator SMS Sp. z o.o. (SISMS Sp. z o.o.) Ul. Tadeusza Gajcego 19 51-143 Wrocław	Podmiot, który podpisał umowę z Usługodawcą na warunkach określonych w Regulaminie świadczenia usług drogą elektroniczną dla klientów z wykorzystaniem Systemu SISMS
Usługa	Przekazywanie za pośrednictwem Systemu SISMS, komunikatów oraz powiadomień nadawanych przez Administratora Danych Osobowych, w tym komunikatów, o których mowa w § 4 Rozporządzenia Ministra Finansów z dnia 30 grudnia 2015 r. w sprawie postępowania wierzycieli należności pieniężnych. Usługa jest świadczona w oparciu o Regulamin świadczenia Usług drogą elektroniczną dla Klientów będących Nadawcami komunikatów za pośrednictwem Systemu SISMS.	
Czynności przetwarzania 1	System SISMS Rejestracja i utrzymanie Użytkownika grup publicznych zapisanego do serwisów Klienta oraz świadczenie usługi zgodnie z "Regulaminem świadczenia usług drogą elektroniczną dla Użytkowników Systemu SISMS" w tym administrowanie, utrzymanie i rozwój systemu.	
Wspólne cele przetwarzania	Przekazywanie komunikatów oraz powiadomień do Użytkowników wpisanych do zdefiniowanych grup publicznych za pośrednictwem Systemu SISMS.	
Przesłanki świadczące o współadministrowaniu pomiędzy Administratorami danych, jako podmiotami decydującymi o celach i środkach przetwarzania	SISMS decyduje o celach i środkach ponieważ: zbiera i przetwarza dane osobowe Użytkowników w związku ze swoją działalnością zarobkową, ustala zakres tematyczny komunikatów, które mogą przysyłać Nadawcy, zawiera umowy z Nadawcami komunikatów oraz powiadomień, umożliwia Użytkownikowi zapisanie się do jednego z Kanałów, za pośrednictwem którego będą otrzymywać określone komunikaty, przesyła własne komunikaty do Użytkowników,	NADAWCA decyduje o celach i środkach ponieważ: Wybiera sposób komunikacji i dystrybucji komunikatów, akceptuje warunki świadczenia usługi za pośrednictwem Systemu SISMS, wybiera określone Kanały komunikacji w Systemie SISMS, określa treść komunikatów nadawanych do Użytkowników, decyduje o rodzajach komunikatów (informacyjne, komercyjne – handlowe).

	administruje, utrzymuje i rozwija System SISMS, odpowiada na pytania i żądania Użytkowników.	
Kategorie danych, które mogą być przetwarzane w ramach współadministrowania	imię, nazwisko -adres e-mail, telefon identyfikatory w systemie informacje o wybranych Kanałach i Nadawcach, daty i czas przesłania komunikatów, treści i rodzaje przesłanych komunikatów, informacje o wyrażonych zgodach i akceptacjach komunikatów, informacje o działaniach Użytkowników,	
Sposób ustalenia warunków dostępu do danych osobowych	W oparciu o zapisy § 13 ust. 3 Regulaminu świadczenia Usług drogą elektroniczną dla Klientów z wykorzystaniem Systemu SISMS, ustalono, że dane osobowe Użytkowników nie są udostępniane Klientowi (Nadawcy), chyba że Użytkownik udzieli wyraźnej, odrębnej zgody na takie udostępnienie.	
Zakresy dostępu do danych osobowych niezbędny do realizacji celu przetwarzania	Niezbędny jest pełny zakres do danych osobowych do wywiązania się z zobowiązań umownych, między innymi do: umożliwienia rejestracji Użytkownika w systemie, utrzymanie bazy danych, pobierania zgód i akceptacji Użytkownika, utrzymania i rozwoju Systemu SISMS, zapewnienia realizacji praw osób, których dane dotyczą, utrzymania retencji danych, wykonywania kopii zapasowych.	W grupach publicznych w Systemie SISMS zastosowano rozwiązania techniczne umożliwiające przesyłanie komunikatów i powiadomień bez dostępu do danych osobowych.

REJSTR CZYNNOŚCI PRZETWARZANIA

Informujemy, że SISMS sp. z o.o. prowadzi rejestr czynności przetwarzania, w którym wykazał czynności współadministrowane ze swoimi Klientami, dotyczące danych użytkowników systemu SISMS zapisanych do grup publicznych.

W celu zachowania spójności w ramerach prowadzonych przez współadministratorów, bardzo prosimy o ujęcie na stępujących informacji w swoim Rejestrze czynności przetwarzania.

1. Nazwa czynności przetwarzania

System SISMS - Przesyłanie komunikatów do Użytkowników grup publicznych za pośrednictwem Systemu SISMS.

2. Dane współadministratora (art. 30 ust. 1 lit. a)

Samorządowy Informator SMS sp. z o.o., 51-143 Wrocław, ul. Tadeusza Gajcego 19
NIP: 895-193-26-64, Regon: 020843579, KRS: 0000314727
Tel: (+48) 71 750 47 00, Fax: (+48) 71 750 47 01
E-mail: sekretariat@sisms.pl

3. Dane kontaktowe Inspektora Ochrony Danych (art. 30 ust. 1 lit. a)

Kontakt do Inspektora Ochrony Danych w SISMS sp. z o.o.: iod@sisms.pl

4. Cele przetwarzania (art. 30 ust. 1 lit b)

Rejestracja i utrzymanie Użytkownika grup publicznych zapisanego do serwisów Klienta oraz świadczenie usługi zgodnie z "Regulaminem świadczenia usług drogą elektroniczną dla Użytkowników Systemu SISMS" w tym administrowanie, utrzymanie i rozwój systemu SISMS.

5. Doprecyzowanie celu przetwarzania (art. 30 ust. 1 lit b)

Świadczenie usługi zgodnie z "Regulaminem świadczenia usług drogą elektroniczną dla Użytkowników Systemu SISMS", w tym także:

- zakładanie i zarządzanie Użytkownikiem,
- autoryzowanie Użytkownika,
- przekazywanie komunikatów,
- przesyłanie treści przez Użytkownika do określonego Nadawcy,
- upublicznianie wiadomości przez Użytkowników,
- udział w anonimowych ankietach,
- obsługa zgłoszeń Użytkowników,
- blokowanie użytkownika,

Umożliwienie pracy w systemie SISMS poprzez zapewnienie:

- utrzymanie SISMS,
- rozwoju SISMS,
- serwisowania SISMS,
- wsparcia i obsługi Użytkowników."

6. Kategorie osób (art. 30 ust. 1 lit. c)

Użytkownicy systemu SISMS którzy zarejestrowali się do grup publicznych Klienta w systemie SISMS.

7. Kategorie danych (art. 30 ust. 1 lit. c)

Dane zwykłe: imię i nazwisko, dane kontaktowe (np. adres e-mail, telefon), identyfikatory w systemach i nazwy użytkowników, identyfikatory IMEI, daty i treści komunikatów, informacje o pozyskanych zgodach i akceptacjach oraz pobranych oświadczeniach, informacje o działaniach użytkowników w systemach, informacje niezbędne do prawidłowego działania systemów,

8. Źródło danych

Osoba, której dane dotyczą.

9. Podstawa prawna

Art. 6 ust. 1 lit. 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.

Art. 6 ust. 1 lit 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.

10. Udostępnienie danych innemu administratorowi (art. 30 ust. 1 lit. d)

Dane mogą zostać udostępnione innemu administratorowi danych na podstawie przepisów prawa lub za zgodą osoby, której dane dotyczą.

11. Podmioty przetwarzające (art. 30 ust. 1 lit. d)

- T-Mobile Polska S.A. ul. Marynarska 12, 02-674 Warszawa, NIP: 5261040567, KRS: 391193, REGON: 011417295; Powierzenie w celu zapewnienia kolokacji serwerów.
- ATM S.A. ul. Grochowska 21a, 04-186 Warszawa, NIP: 1130059989, KRS: 34947, REGON: 012677986. Powierzenie w celu zapewnienia kolokacji serwerów.

W celu zapewnienia korzystania z usług „zdalnej ręki” w kolokacji T-MOBILE, dane są podpowierzane do ASTA Telekom Servis Sp. z o.o., Solec 78E, 05-532 Solec.

12. Transfer do kraju trzeciego lub organizacji międzynarodowej (art. 30 ust. 1 lit. e)

Nie dotyczy. Dane przetwarzane na terenie Polski.

13. Zabezpieczenia transferu danych do kraju trzeciego lub organizacji międzynarodowej (art. 30 ust. 1 lit. e)

Nie dotyczy.

14. Planowany termin usunięcia (art. 30 ust. 1 pkt f)

Dane będą usunięte lub zanonimizowane na życzenie użytkownika lub po całkowitym wyrejestrowaniu się Użytkownika z systemu SISMS.

15. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (art. 30 ust. 1 lit. g)

Zastosowane środki bezpieczeństwa podano w części „SPEŁNIENIE WYMAGAŃ RODO W SYSTEMIE SISMS” oraz w części „ZABEZPIECZENIE PRZETWARZANIA DANYCH OSOBOWYCH”.

INSPEKTOR OCHRONY DANYCH OSOBOWYCH W SISMS sp. z o.o.

Informujemy, iż obecnie funkcje Inspektora Ochrony Danych w SISMS sp. z o.o. pełni pani Dagmara Wrona.

Kontakt z naszym Inspektorem Ochrony Danych jest możliwy na adres e-mail: iod@sisms.pl

INSPEKTOR OCHRONY DANYCH OSOBOWYCH KLIENTA

W celu zweryfikowania i uzupełnienia prowadzanego przez SISMS sp. z o.o. Rejestru czynności przetwarzania, a w przypadku podpisanej umowy powierzenia również Rejestru kategorii, prosimy o przesłanie aktualnego kontaktu do Państwa Inspektora Ochrony Danych.

Informacje bardzo prosimy przesyłać pocztą elektroniczną na adres: kontaktiod@sisms.pl

DALSZE POWIERZENIE DANYCH

Informujemy, że dane osobowe przetwarzane w systemie SISMS, zarówno w Grupach Publicznych, jak i Grupach Niepublicznych, powierzamy następującym dostawcom:

- T-Mobile Polska S.A. ul. Marynarska 12, 02-674 Warszawa, NIP: 5261040567, KRS: 391193, REGON: 011417295; Powierzenie w celu zapewnienia kolokacji serwerów.
- ATM S.A. ul. Grochowska 21a, 04-186 Warszawa, NIP: 1130059989, KRS: 34947, REGON: 012677986. Powierzenie w celu zapewnienia kolokacji serwerów.
- W celu zapewnienia korzystania z usług „zdalnej ręki” w kolokacji T-MOBILE, dane są podpowierzane do ASTA Telekom Servis Sp. z o.o., Solec 78E, 05-532 Solec.

Powierzenie danych wyżej wymienionym podmiotom jest niezbędne do świadczenia usługi przez SISMS sp. z o.o.