

## Informacja o przetwarzaniu danych osobowych

przez **Securitas Services sp. z o.o.**, w związku z zawieraniem i wykonywaniem umów, przeznaczona dla Klientów lub Dostawców, ich przedstawicieli (wspólników, członków zarządu), prokurentów i innych pełnomocników oraz osób wskazanych do kontaktu z Securitas w związku z zawarciem i wykonywaniem umów

### 1. Kto jest administratorem Państwa danych osobowych

Administratorem Państwa danych osobowych (czyli podmiotem odpowiedzialnym za ich przetwarzanie) jest **Securitas Services sp. z o.o.** z siedzibą w Warszawie (dalej „**Securitas**”).

Administrator to osoba (firma), która odpowiada za to, żeby Państwa dane osobowe były bezpieczne i przetwarzane zgodnie z prawem, a w szczególności zgodnie z RODO<sup>1</sup>.

Pełne dane administratora to **Securitas Services sp. z o.o.** z siedzibą w Warszawie, ul. Postępu 6, 02-676 Warszawa, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego, nr KRS 0000045554, nr REGON 017190697, nr BDO 000459025, NIP 5213137719, kapitał zakładowy 2 000 000 zł.

### 2. Czy Securitas wyznaczyła inspektora ochrony danych

Tak, **Securitas wyznaczyła inspektora ochrony danych** osobowych. Można się z nim skontaktować pod adresem [iod@securitas.pl](mailto:iod@securitas.pl). Jeżeli chcą się Państwo skontaktować z Securitas, w kwestiach związanych z ochroną danych osobowych, to prosimy pod ten adres lub pocztą pod adres siedziby Securitas.

### 3. Skąd Securitas ma Państwa dane

Securitas uzyskała Państwa dane bezpośrednio od Państwa lub od firmy (Klienta lub Dostawcy Securitas), dla której Państwo pracują. Securitas może również weryfikować dane i pozyskiwać dodatkowe z publicznych rejestrów takich jak: KRS, REGON, CEIDG oraz od firm dostarczających bazy danych służące do weryfikacji kontrahentów, np. Dun & Bradstreet.

W większości przypadków zakres danych ogranicza się do danych identyfikacyjnych (takich jak imię, nazwisko, stanowisko, NIP i PESEL) oraz danych kontaktowych (takich jak adres e-mail, numer telefonu). W uzasadnionych sytuacjach (np. przy odroczonej płatności) Securitas przetwarza dane niezbędne do oceny wiarygodności finansowej Klienta lub Dostawcy. W niektórych przypadkach, gdy szczególnie istotna jest identyfikacja osoby (np. kiedy Securitas świadczy usługę wydawania kluczy), konieczne może być także przetwarzanie danych z dokumentu tożsamości (np. numer dowodu osobistego) oraz wizerunku.

Jeżeli Securitas zbiera dane od Państwa, to **ich podanie jest dobrowolne, jednak niezbędne do nawiązania lub kontynuowania współpracy** z Securitas i realizacji celów opisanych poniżej (→ pkt. 4). Odmowa przekazania danych może skutkować tym, że podjęcie lub kontynuowanie współpracy z Securitas okaże się niemożliwe.

---

<sup>1</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia a 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).

#### 4. W jakim celu i na jakiej podstawie prawnej Securitas przetwarza Państwa dane osobowe

Cel przetwarzania	Podstawa prawna
4.1. Wykonanie czynności zmierzających do zawarcia umowy (np. przygotowanie oferty, negocjacje) oraz realizacja obowiązków lub praw Securitas wynikających z umowy zawartej z Klientem lub Dostawcą	<u>art. 6 ust. 1 lit. f RODO</u> – prawnie uzasadniony interes lub <u>art. 6 ust. 1 lit. b RODO</u> – wykonanie umowy (dane osoby fizycznej będącej stroną umowy)
4.2. Realizacja obowiązków prawnych Securitas związanych z umową (np. wystawianie i przechowywanie faktur)	<u>art. 6 ust. 1 lit. c RODO</u> – obowiązek prawny
4.3. Ocena wiarygodności finansowej Klienta lub Dostawcy (np. jeżeli Securitas świadczy usługę z odroczoną płatnością)	<u>art. 6 ust. 1 lit. f RODO</u> – prawnie uzasadniony interes
4.4. Dochodzenie roszczeń wynikających lub związanych z umową lub obrona przed nimi (np. Securitas może mieć potrzebę wykazania pewnych faktów przed sądem lub urzędem)	<u>art. 6 ust. 1 lit. f RODO</u> – prawnie uzasadniony interes
4.5. Utrzymywanie kontaktu z Klientami i Dostawcami (ich przedstawicielami) w zakresie dotyczącym współpracy, w tym także w celu proponowania nowych produktów i usług Securitas	<u>art. 6 ust. 1 lit. f RODO</u> – prawnie uzasadniony interes

Państwa dane nie będą wykorzystywane do podejmowania decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych, w tym profilowania w rozumieniu art. 22 RODO.

#### 5. Jak długo Securitas będzie przetwarzać Państwa dane osobowe

Securitas będzie wykorzystywać dane osobowe przez okres niezbędny do realizacji opisanych powyżej celów. W zależności od podstawy prawnej będzie to odpowiednio:

- okres współpracy z Securitas (→ pkt. 4.1),
- okres wynikający z przepisów prawa (→ pkt. 4.2),
- okres przedawnienia roszczeń, co do zasady wynikający z Kodeksu cywilnego, a jeżeli Państwa dane stanowią dowód w postępowaniu prowadzonym na podstawie przepisów prawa lub Securitas poweźmie wiadomość, że mogą one stanowić dowód w takim postępowaniu – okres ten ulega przedłużeniu do czasu prawomocnego zakończenia postępowania (→ pkt. 4.4),
- do czasu złożenia skutecznego sprzeciwu (→ pkt. 4.1, 4.3, 4.4 i 4.5).

#### 6. Komu Securitas może przekazywać Państwa dane osobowe

Państwa dane są przetwarzane przez upoważnionych pracowników i współpracowników Securitas. Dane są udostępniane:

- wewnątrz grupy kapitałowej Securitas,
- podmiotom zewnętrznym, które przetwarzają je w imieniu Securitas (np. podwykonawcom z zakresu usług IT),

- podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa (np. Policji) oraz innym administratorom (np. firmie audytorskiej, kancelariom prawnym).

## 7. Czy dane będą przekazywane poza Europejski Obszar Gospodarczy

Jeżeli będzie to niezbędne do realizacji wskazanych powyżej celów, Securitas może przekazywać Państwa dane osobowe do renomowanych podwykonawców lub innych kontrahentów w krajach spoza EOG<sup>2</sup>.

Mając na względzie, że poziom ochrony danych osobowych w tych krajach może różnić się od zapewnianego w Unii Europejskiej, przekazywanie danych odbywa się z zapewnieniem odpowiedniego stopnia ochrony, przede wszystkim poprzez:

- współpracę z firmami przetwarzającymi dane osobowe w krajach spoza EOG, wobec których Komisja Europejska stwierdziła, że zapewniają odpowiedni poziom ochrony (dotyczy to m.in. firm z USA, certyfikowanych na podstawie porozumienia UE-USA<sup>3</sup>, takich jak *Microsoft*),
- w razie braku decyzji Komisji Europejskiej, stosowanie w umowach z takimi firmami standardowych klauzul umownych (SCC) lub wiążących reguł korporacyjnych (BCR), zatwierdzonych przez właściwy organ nadzorczy,
- stosowanie warunków określonych w [art. 49 RODO](#).

Securitas zapewnia, że każdy transfer danych osobowych realizowany będzie na podstawie odpowiednich umów, w sposób bezpieczny i kontrolowany.

W każdym z przypadków opisanych powyżej, mogą Państwo zażądać dalszych informacji o stosowanych zabezpieczeniach w tym zakresie, uzyskać kopię tych zabezpieczeń oraz informację o miejscu ich udostępnienia.

## 8. Jakie mają Państwo prawa związane z przetworzeniem danych przez Securitas

Securitas – na państwa wniosek, **na zasadach określonych w [RODO](#)**:

- umożliwi Państwu dostęp do danych,
- sprostuje Państwa dane, jeżeli są nieprawidłowe,
- przeniesie Państwa dane do innego administratora,
- usunie Państwa dane osobowe lub ograniczy ich przetwarzanie.

Niezależnie od powyższego mogą Państwo także wnieść sprzeciw odnośnie do przetwarzania Państwa danych osobowych przez Securitas na podstawie jej prawnie uzasadnionego interesu ([art. 6 ust. 1 lit. f RODO](#), → [pkt. 4.1, 4.3, 4.4 i 4.5](#)).

Jeżeli uznają Państwo, że Securitas przetwarza Państwa dane osobowe niezgodnie z prawem, mogą Państwo wnieść skargę do [Prezesa Urzędu Ochrony Danych Osobowych](#).

<sup>2</sup> EOG – Europejski Obszar Gospodarczy, obejmujący kraje Unii Europejskiej oraz Islandię, Liechtenstein i Norwegię.

<sup>3</sup> Obecnie *The Data Privacy Framework (DPF) Program*.