

Zasady ochrony danych osobowych w Kristensen Group Investments Sp. z o.o.

Niniejsze zasady ochrony danych osobowych w Kristensen Group Investments Sp. z o.o., zwane dalej także Zasadami, polityka bezpieczeństwa lub Polityką, ma na celu zapewnienie przetwarzanie danych osobowych zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej zwanego RODO) oraz ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (dalej zwaną Ustawą Wdrażającą).

§ 1.

Ogólne zasady ochrony danych osobowych w Kristensen Group Investments Sp. z o.o. (dalej zwane też Polityką lub zasadami) są sprecyzowane przez niniejszą politykę. O ile którekolwiek z tych zasad sprzeczne są z RODO lub Ustawą Wdrażającą, stosuje się RODO i Ustawę Wdrażającą.

§ 2.

Na potrzeby niniejszych Zasad ustala się iż wszelkie definicje użyte w tekście mają znaczenie opisane w RODO za wyjątkiem:

Sieć lokalna – połączenie Systemów informatycznych Administratora Danych wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych;

Zbiór danych – każdy zestaw danych o zawierający dane osobowe;

Przetwarzanie danych – jakiegokolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w formie operacji na elektronicznym Zbiorze Danych

Zabezpieczenie danych– środki techniczne i praktyki służące ochronie danych przed ich nieuprawnionym Przetwarzaniem;

Identyfikator użytkownika – niepowtarzalny ciąg znaków identyfikujący osobę upoważnioną do przetwarzania danych osobowych

Hasło – niepowtarzalny ciąg znaków znany jedynie osobie uprawnionej do pracy z danymi osobowymi

§ 3.

1. Administratorem Danych jest Kristensen Group Investments Sp. z o.o. z siedzibą w Warszawie, przy Al. Rzeczypospolitej 18/70, 02-972 Warszawa, wpisana do Rejestru Przedsiębiorców KRS prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000361316, NIP: 5213573863, REGON: 142498062 (dalej zwana Kristensen lub Administratorem).

2. Polityka dotyczy wszystkich Danych osobowych przetwarzanych w Kristensen, niezależnie od formy ich przetwarzania (zbiory w formie papierowej, elektronicznej, systemy informatyczne).
3. Polityka jest udostępniana do wglądu na żądanie każdej osoby lub podmiotu, zaś przechowywana jest w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora przy Al. Rzeczypospolitej 18/70 w Warszawie.
4. Każda osoba przetwarzające dane osobowe zapoznaje się obowiązkowo z niniejszą Polityką. Polityka jest stale dostępna do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych. Za osoby które winny się z Polityką zapoznać uważa się w szczególności pracowników i współpracowników Kristensen. Każdy z przetwarzających Dane osobowe winien być pisemnie upoważniony do przetwarzania zgodnie z „Upoważnieniem do przetwarzania danych osobowych” – wzór Upoważnienia stanowi Załącznik nr 2. Upoważnienie może ograniczać dostęp do danych osobowych.
5. Dla skutecznej realizacji RODO Administrator Danych zapewnia m.in. środki techniczne i rozwiązania organizacyjne ochrony danych w postaci m.in. szyfrowania, haseł dostępu, kluczy oraz innych fizycznych środków ograniczenia dostępu. Upoważniony nie może korzystać ze środków dostępu do danych osobowych przynależnych innym osobom.
6. Administrator okresowo monitoruje i stale kontroluje przetwarzanie danych osobowych w sposób ciągły, czuwając nad przestrzeganiem m.in. RODO oraz Polityki. Upoważnieni do przetwarzania danych osobowych stale czuwają nad integralnością i zabezpieczeniem zbiorów danych oraz urządzeń wykorzystywanych przy ich przetwarzaniu przez ingerencją osób trzecich.
7. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania Użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.

§ 4.

1. Dane osobowe przetwarzane przez Kristensen obejmują : imię i nazwisko, nr PESEL, datę urodzenia, NIP, KRS, REGON, RHB, adres zamieszkania i adres dla korespondencji, miejsca wykonywania usług i sprzedaży produktów oraz inne lokalizacje którymi Osoby te są zainteresowane, zdjęcia osób lub urządzeń, nr dokumentów tożsamości lub innych podobnych dokumentów, adresy poczty elektronicznej lub inne identyfikatory używane w systemach elektronicznych (w szczególności loginy i nazwy użytkowników tychże systemów).
2. Administrator danych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób, zaś w przypadku stwierdzenia, iż przetwarzanie takie ma miejsce niezwłocznie należy podjąć działania przewidziane w art. 35 i następnych RODO. Administrator przetwarza dane wyłącznie w celach handlowych oraz reklamowych.
3. Administrator danych prowadzi rejestr czynności przetwarzania. Wzór rejestru czynności przetwarzania stanowi Załącznik nr 1 do niniejszej polityki.

§ 5.

1. Dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest konieczny dla osiągnięcia celu przetwarzania danych, w szczególności komunikacji z kontrahentem oraz sporządzeniem, dostarczeniem lub wysyłką powiązanych z tym dokumentów i usług.
2. Nie jest dopuszczalne przetwarzanie danych osób które nie są pracownikami, partnerami handlowymi Administratora, potencjalnymi partnerami handlowymi, pracownikami lub osobami powiązаныmi z partnerami handlowymi, względnie nie wyraziły na to zgody, jak też nie występuje inna podstawa przetwarzania tych danych.
3. Czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane, względnie zaś przechowywanie ich odbywa się bez ich przetwarzania.
4. Wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO, z zastrzeżeniem art. 6 ust. 1 lit b RODO.

§ 6.

1. Administrator danych nie przekazuje osobom, których dane dotyczą, informacji w sytuacji, w której dane te muszą zostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej (art. 14 ust 5 pkt d RODO).
2. Dane winny być zabezpieczone przed naruszeniami zasad ich ochrony.
3. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych osobowych uważa się w szczególności:
 - a) naruszenie bezpieczeństwa systemów elektronicznych lub informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach lub przy ich udziale;
 - b) udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym;
 - c) niedopełnienie (umyślne lub nieumyślne) obowiązku zapewnienia danym osobowym ochrony, zachowania w tajemnicy danych osobowych oraz nieprzestrzeganie zasad i sposobów ich zabezpieczenia, niezależnie od tego czy spowodowało to uszkodzenia, utratę, zmiany lub nieuprawnione kopiowanie Danych osobowych;
 - d) przetwarzanie Danych osobowych niezgodnie z celem i zakresem dla którego je pozyskano;
 - e) naruszenie praw osób, których dane są przetwarzane.
4. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych Użytkownik (w szczególności Pracownik) zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora Danych.
5. W przypadku wejścia w posiadanie danych niepotrzebnych dane te należy niezwłocznie usunąć w sposób trwały.

§ 7.

1. Administrator gwarantuje, że w przypadku zatrudnienia lub zmiany warunków zatrudnienia pracowników lub współpracowników (osób podejmujących czynności na rzecz Administratora Danych na podstawie innych umów cywilnoprawnych) osoby te:
 - były odpowiednio przygotowani do wykonywania swoich obowiązków,
 - każdy pracownik zobowiązał się do zachowania danych osobowych przetwarzanych w Kristensen Group w tajemnicy. „Oświadczenie i zobowiązanie osoby przetwarzającej dane osobowe do zachowania tajemnicy” stanowi element „Upoważnienia do przetwarzania danych osobowych”.
 - zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
 - zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu.

§ 8.

1. Obszar, w którym przetwarzane są Dane osobowe, obejmuje w szczególności siedzibę rejestrową Administratora, komputery, telefony, tablety, płyty CD, pendrive, serwery poczty elektronicznej oraz dyski wirtualne, jak również inne nośniki danych znajdujące się poza obszarem wskazanym powyżej.
2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być odpowiednie do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych i nie powinny odbiegać od praktyk typowych dla tego rodzaju zabezpieczeń.

§ 9.

Środki obejmują:

- a) Ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do osób odpowiednio upoważnionych, stosowanie sejfów i szafek zamykanych kluczami lub w inny sposób blokowanych przed dostępem do nich. W okresie nieobecności pomieszczenia te są zamykane i monitorowane z użyciem systemu automatycznego ostrzegania (alarmu).
- b) Ograniczenie przebywania/dostępu do danych - inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych lub korzystać z ich zbiorów jedynie w towarzystwie osoby upoważnionej.
- c) Niszczanie niepotrzebnych danych osobowych i nośników z użyciem niszczarki do dokumentów oraz oprogramowania niszczącego.
- d) Ochronę sieci lokalnej oraz komputerów i podobnych urządzeń przy użyciu oprogramowania typu firewall/antispayware.
- e) Wykonywanie kopii awaryjnych danych stosownie do potrzeb i możliwości technicznych.
- f) Zabezpieczenie dostępu do urządzeń elektronicznych przy pomocy haseł dostępu.
- g) Wykorzystanie szyfrowania danych przy ich transmisji.

§ 10. Naruszenia zasad ochrony danych osobowych

1. Administrator nie przekazuje danych osobowych innym podmiotom, za wyjątkiem dokonywania wpisów w ewidencjach prowadzonych przez organy administracji, w szczególności zaś gdy dotyczy to ubezpieczeń społecznych lub uprawnień do wykonywania zawodu.
2. W każdym przypadku, w którym zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Wzór zgłoszenia określa załącznik nr 4 do niniejszej polityki.
1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
3. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.
4. Administrator Danych Osobowych nie będzie przekazywał danych osobowych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek osoby, której dane dotyczą.

§ 11. Postanowienia końcowe

Za niedopełnienie obowiązków wynikających z niniejszego dokumentu osoba przetwarzające dane niezgodnie z zasadami które są wdrożone niniejszą Polityką, ponosi odpowiedzialność m.in. na podstawie Kodeksu pracy. Załączniki stanowią integralną część niniejszej polityki.