Polityka Bezpieczeństwa Danych Osobowych

Podstawa prawna

1. Dane osobowe w KPT sp. z o.o. przetwarzane są z poszanowaniem obowiązujących w tym zakresie przepisów prawa, a w szczególności:
    1) 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 – dalej również jako „RODO")
    2) Przepisów Ustawy z dnia 16 lipca 2004 roku – Prawo Telekomunikacyjne (Dz. U. Nr 171 poz. 1800 z późn.),
    3) Przepisów Ustawy z dnia 13 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji (Dz. U. Nr 47 poz. 211 z późn. zm.);
    4) Przepisów art. 22 § 1 -5 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tj. Dz.U. z 1998 r. nr 21, poz. 94 z póź. zm.) i przepisów wykonawczych wydanych z upoważnienia tej ustawy.
    5) Innych przepisów ustawy i rozporządzeń normujących przetwarzanie danych osobowych określonych kategorii.
2. Dane osobowe w KPT sp. z o.o. przetwarzane są w celu realizacji zadań. W szczególności dane osobowe przetwarza się
    1) Dla zabezpieczenia prawidłowego toku podstawowej działalności, realizacji innych usprawiedliwionych celów i zadań KPT sp. z o.o.
    2) Dla zapewnienia prawidłowej, zgodnej z prawem i celami KPT sp. z o.o. polityki personalnej oraz bieżącej obsługi stosunków pracy a także innych stosunków zatrudnienia nawiązywanych przez KPT sp. z o.o.

Podstawowe Definicje

3. Przez użyte w dokumencie określenia rozumie się:

1) **KPT sp. z o.o.** – Krakowski Park Technologiczny spółka z ograniczoną odpowiedzialnością z siedzibą w Krakowie.
2) **Administrator Danych Osobowych (ADO)** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
3) **dane osobowe** – 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;

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) **przetwarzanie danych osobowych** – 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;
6) **system informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
7) **zabezpieczenie danych osobowych** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
1) **Administrator Systemu Informatycznego (ASI)** – zespół IT odpowiedzialny za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach;
8) **Budynki KPT sp. z o.o.** – budynek KPT Podole przy ul. Podole 60 w Krakowie oraz budynek przy ul. prof. M. Życzkowskiego 14 w Krakowie.

Cel wprowadzenia dokumentu Polityki Bezpieczeństwa Danych Osobowych

4. Zarząd KPT sp. z o.o. deklaruje zaangażowanie w prawidłowym zarządzaniu bezpieczeństwem danych osobowych w KPT sp. z o.o.
5. Zarząd KPT sp. z o.o. oświadcza, że dołoży wszelkich starań celem zapewnienia bezpieczeństwa ochrony danych osobowych.
6. Poprzez bezpieczeństwo należy rozumieć stan faktyczny uniemożliwiający przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
7. Niniejszy dokument został przygotowany z myślą o zapewnieniu bezpieczeństwa danym osobowym w KPT sp. z o.o. ze szczególnym uwzględnieniem zgodności z prawem.
8. Celem Polityki Bezpieczeństwa Danych Osobowych jest osiągnięcie i utrzymanie akceptowalnego poziomu bezpieczeństwa aktywów informacyjnych KPT sp. z o.o. poprzez wdrożenie odpowiedniego systemu ochrony tych aktywów przed zagrożeniami wewnętrznymi i zewnętrznymi.

9. Celem jest również podniesienie poziomu świadomości pracowników KPT sp. z o.o. co do istoty problemu bezpieczeństwa danych osobowych.

Zakres stosowania dokumentu Polityki Bezpieczeństwa Danych Osobowych.

10. Polityka Bezpieczeństwa Danych Osobowych ma zastosowanie w stosunku do wszystkich postaci informacji zawierających dane osobowe: dokumentów papierowych, zapisów elektronicznych i innych, będących własnością KPT sp. z o.o. lub administrowanych przez KPT sp. z o.o. i przetwarzanych w systemach informatycznych, tradycyjnych (papierowych) i komunikacyjnych KPT sp. z o.o.
11. Polityka Bezpieczeństwa Danych Osobowych ma zastosowanie w stosunku do wszystkich pracowników KPT sp. z o.o., jak również osób trzecich mających dostęp do danych osobowych w KPT sp. z o.o.
12. Ochrona danych osobowych wynikająca z Polityki Bezpieczeństwa Danych Osobowych jest realizowana na każdym etapie przetwarzania informacji.

Zasady dotyczące przetwarzania danych osobowych

13. Dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);

b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami („ograniczenie celu”);

c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);

d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);

e) 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; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);

f) 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”).

Inspektor ochrony danych osobowych

14. Zarząd KPT sp. z o.o. powołał Inspektora Ochrony Danych. Podlega on bezpośrednio Zarządowi. Zarząd KPT sp. z o.o., zapewnia, że Inspektor Ochrony Danych nie będzie otrzymywał instrukcji dotyczących wykonywania zadań związanych z pełnieniem swojej funkcji. Nie będzie on odwoływany ani karany za wypełnianie swoich zadań.

15. Jego zadania obejmują w szczególności:
    a) informowanie administratora oraz pracowników administratora o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz innych przepisów,
    b) monitorowanie przestrzegania Rozporządzenia oraz innych przepisów Unii i państw członkowskich oraz wewnętrznych regulacji administratora,
    c) szkolenie personelu uczestniczącego w operacjach przetwarzania danych osobowych,
    d) przeprowadzanie systematycznych audytów w organizacji,
    e) udzielanie wskazówek administratorowi w przedmiocie wdrożenia odpowiednich i skutecznych środków technicznych jak również organizacyjnych mających zabezpieczyć dane osobowe oraz sposobu wykazania przestrzegania prawa przez administratora w szczególności jeżeli chodzi o identyfikowanie ryzyka związanego z przetwarzaniem, o jego ocenę pod katem źródła, charakteru, prawdopodobieństwa i wagi zagrożenia oraz o najlepsze praktyki pozwalające zminimalizować to ryzyko,
    f) udzielanie na żądanie zaleceń co do oceny skutków przetwarzania danych osobowych oraz monitorowanie ich wykonania,
    g) współpraca z organem nadzorczym,
    h) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem.
16. Osoby, których dane dotyczą, mogą kontaktować się z Inspektorem Ochrony Danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO pod adresem iod@kpt.krakow.pl

Środki techniczne i organizacyjne niezbędne dla realizacji zasad przetwarzania danych osobowych

17. Administratorem Danych Osobowych jest KPT sp. z o.o.
18. Zarządzanie bezpieczeństwem danych osobowych jest procesem ciągłym, realizowanym przy współdziałaniu użytkowników z Inspektorem Ochrony Danych oraz Administratorem Systemów Informatycznych.
19. KPT sp. z o.o. stosuje przy przetwarzaniu danych środki techniczne i organizacyjne zapewniające ochronę danych, określone w art. 32-36 RODO w szczególności, zapewnia zabezpieczenie integralności i poufności danych osobowych.

20. KPT sp. z o.o. realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych wyznacza budynki, pomieszczenia i części pomieszczeń, tworzące obszary KPT sp. z o.o. w którym przetwarzane są dane osobowe.
21. Dostęp do miejsc w których przetwarzane są dane osobowe zabezpieczony jest poprzez system kart dostępu wydawanych przez KPT sp. z o.o.
22. Budynki KPT sp. z o.o. są ochraniane przez podmiot profesjonalny. Ponadto w budynkach KPT sp. z o.o. funkcjonuje monitoring wizyjny. Informacja o wykorzystaniu monitoringu wizyjnego znajduje się:
    - budynek KPT Życzkowskiego - na głównych drzwiach wejściowych od strony frontowej oraz od strony parkingu wewnętrznego;
    - budynek KPT Podole – na elewacji dwóch budowli platform garażowych zlokalizowanych od strony frontowej budynku po lewej i prawej stronie schodów prowadzących do wejścia głównego do budynku;
    tj. w miejscu ogólnodostępnym oraz widocznym dla wszystkich wchodzących do budynku.

Prawa osób , których dane są przetwarzane przez KPT sp. z o.o.

23. KPT sp. z o.o. gwarantuje osobom fizycznym, których dane osobowe są przetwarzane w związku z bieżącą działalnością, realizację uprawnień gwarantowanych im przez obowiązujące przepisy prawa.
24. W szczególności każdej osobie fizycznej, której dane osobowe są przetwarzane w związku z działalnością KPT sp. z o.o. przysługuje prawo do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub prawo do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych.

Konsekwencje naruszenia Polityki Bezpieczeństwa Informacji

25. Osoby naruszające zasady Polityki Bezpieczeństwa Ochrony Danych zostaną pociągnięte do odpowiedzialności służbowej (porządkowej lub dyscyplinarnej) lub karnej.

Postanowienia końcowe

26. Szczegółowe zasady dotyczące przetwarzania danych osobowych uregulowane zostały w regulaminie o charakterze wewnętrznym.