

SPIS TREŚCI

1. [Wprowadzenie](#)
2. [Zbiór podstawowych definicji](#)
3. [Zasady ochrony danych osobowych](#)
4. [Cele Polityki Bezpieczeństwa](#)
5. [Przetwarzanie danych osobowych](#)
6. [Prawa osób, których dane dotyczą](#)
7. [Reguły bezpieczeństwa przetwarzania danych osobowych](#)
8. [Udostępnienie danych osobowych](#)
9. [Procedura postępowania na wypadek naruszeń](#)
10. [Postanowienia końcowe](#)
11. [Załączniki](#)

1. Wprowadzenie

Administrator - New Tech Center OU z siedzibą w Riigiloiv, asut.nr 1824801 – działając w oparciu o art. 24 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 (Dz.U.UE.L.2016.119.1), w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych, wprowadza niniejszym wewnętrzny system regulacji z zakresu danych osobowych. Opracowany on został na podstawie:

- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (dalej RODO)

Polityka Bezpieczeństwa Ochrony Danych Osobowych określa reguły przetwarzania danych osobowych oraz sposobów ich zabezpieczenia, jako zestaw praw, zasad i zaleceń regulujących sposób ich zarządzania, ochrony i dystrybucji w New Tech Center OU z siedzibą w Riigiloiv, asut.nr 1824801.

Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń techniczno-organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych.

2. Zbiór podstawowych definicji

1. **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.
2. **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.

3. **Ograniczenie przetwarzania danych osobowych** - oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.
4. **Profilowanie** - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
5. **Pseudoanimizacja** - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
6. **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.
7. **Administrator danych osobowych** - 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.
8. **Podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.
9. **Odbiorca** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.
10. **Strona trzecia** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.

11. **Zgoda na przetwarzanie danych osobowych** – oznacza zgodę osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.
12. **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.
13. **Dane genetyczne** - oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.
14. **Dane biometryczne** - oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.
15. **Dane dotyczące zdrowia** - oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.
16. **Przedstawiciel** - oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 RODO do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia.
17. **Przedsiębiorca** - oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą.
18. **Organ nadzorczy** - oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO.

3. Zasady ochrony danych osobowych

Zgodnie z RODO podmiot przetwarzający dane osobowe powinien kierować się następującymi zasadami:

1. Zasada zgodności, rzetelności i przejrzystości z prawem

Art. 5 ust. 1 lit a) RODO wysuwa ogólny postulat, który wymaga od Administratora danych przetwarzania danych zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

Zasad przejrzystości wymaga od Administratora danych podania osobie, której dane dotyczą dla jakich celów przedmiotowe dane są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane. Ponadto zasada ta wymaga, by wszelkie informacje i wszelkie komunikaty

związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem.

Wszelkie informacje te mogą być przekazywane w formie elektronicznej a w stosownych wypadkach dodatkowo wizualizowane, na przykład za pomocą strony internetowej, gdy są kierowane do ogółu społeczeństwa. Dotyczy to w szczególności sytuacji, gdy duża liczba podmiotów i złożoność technologiczna działań sprawiają, że osobie, której dane dotyczą, trudno jest dowiedzieć się i zrozumieć, czy dotyczące jej dane osobowe są zbierane, przez kogo oraz w jakim celu, na przykład w przypadku reklamy w internecie.

Gdy przetwarzanie dotyczy dziecka – powinny być sformułowane tak jasnym i prostym językiem, by dziecko mogło je bez trudu zrozumieć.

2. Zasada ograniczenia celu przetwarzania danych osobowych

Powyższa zasada nakłada na Administratora danych obowiązek zbierania danych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

Przetwarzanie danych osobowych do celów innych niż cele, w których dane te zostały pierwotnie zebrane, powinno być dozwolone wyłącznie w przypadkach, gdy jest zgodne z celami, w których dane osobowe zostały pierwotnie zebrane. Za przypadki, o których jest mowa powyżej badania naukowe, historyczne lub cele statystyczne.

Natomiast jeżeli Administrator danych planuje przetwarzać dane osobowe w celu innym niż cel, w których dane osobowe zostały zebrane, powinien on przed takim dalszym przetwarzaniem poinformować osobę, której dane dotyczą, o innym celu oraz dostarczyć jej w tym zakresie innych niezbędnych informacji.

3. Zasada minimalizacji danych

Zgodnie z przepisami RODO od Administratora danych wymaga się by adekwatnie, stosownie oraz w sposób ograniczony do swoich celów gromadził i przechowywał dane osobowe.

Chodzi tu w szczególności o zapewnienie ograniczenia okresu przechowywania danych do ścisłego minimum. Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu.

4. Zasada prawidłowości danych

Na Administratorze danych ciąży obowiązek by dane osobowe przez niego posiadane były prawidłowe natomiast w przypadku ich niezgodności zobowiązany jest on do ich aktualizacji.

W celu realizacji nałożonych na Administratora danych obowiązków zobowiązany jest on podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

5. Zasada ograniczenia przechowania danych

Administrator danych zobligowany jest do przechowywania danych 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.

Powyższa zasada oraz obowiązki z niej wynikające nałożone na Administratora Danych wymagają w szczególności zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum. Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu.

6. Zasada integralności i poufności danych

Administrator danych przetwarzając dane osobowe powinien zapewnić im odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. Oznacza to ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.

7. Zasada rozliczalności

Administrator musi wykazać, że określone decyzje odnoszące się do procesów przetwarzania danych osobowych zostały przeanalizowane z punktu widzenia zgodności z ogólnymi zasadami przetwarzania danych, a przede wszystkim, że są z nimi zgodne.

4. Cele Polityki Bezpieczeństwa

Celem Polityki Bezpieczeństwa Danych Osobowych jest określenie oraz wdrożenie zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w New Tech Center OU z siedzibą w Männimäe, Pudisoo küla, Kuusalu vald, Harju maakond, a w szczególności:

1. zapewnienie spełnienia wymagań prawnych;
2. zapewnienie poufności, integralności oraz rozliczalności danych osobowych przetwarzanych w firmie;
3. podnoszenie świadomości osób przetwarzających dane osobowe;
4. zaangażowanie osób przetwarzających dane osobowe firmy w ich ochronę.

5. Przetwarzanie danych osobowych

Nadawanie upoważnień do przetwarzania danych osobowych

Administrator danych zezwala na przetwarzanie danych osobowych przez pracowników bądź inne osoby jedynie wówczas, gdy zostało uprzednio udzielone imienne upoważnienie do przetwarzania, w zakresie przewidzianym w upoważnieniu. Niedopuszczalnym jest przetwarzanie danych osobowych przez osoby nieupoważnione lub przetwarzanie w większym zakresie niż określony w upoważnieniu.

Administrator danych udziela upoważnienia w formie pisemnej oraz prowadzi rejestr upoważnień. Rejestr podlega bieżącej kontroli przeprowadzanej co 12 miesięcy. Kontrola obejmuje aktualność i prawidłowość danych ujętych w rejestrze, w tym w zakresie faktycznego zakresu przetwarzania danych zgodnie z upoważnieniami.

Upoważnienie wydawane jest po uprzednim zapoznaniu pracownika bądź osoby przetwarzającej dane osobowe w przedsiębiorstwie, której upoważnienie ma zostać nadane po odebraniu od niej oświadczenia o poufności. Upoważnienie wydawane jest na okres nie dłuższy niż 24 miesiące i może zostać przez Administratora danych w każdym czasie odwołane. Odwołanie upoważnienia następuje każdorazowo w przypadku, gdy:

1. Upoważniony dopuścił się naruszenia zasad przetwarzania danych osobowych, a naruszenie miało charakter umyślny i zawiniony.
2. Upoważniony zaprzestał czasowo albo na stałe wykonywać obowiązki związane z przetwarzaniem danych osobowych (np. zmiana stanowiska, rozwiązanie umowy o pracę).

Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy:

- zapoznanie się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami Polityki Bezpieczeństwa Ochrony Danych Osobowych
- przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych Osobowych w pisemnym upoważnieniu i tylko w celu wykonywania nałożonych obowiązków służbowych;
- niezwłoczne informowanie Administratora Danych o wszelkich nieprawidłowościach dotyczących bezpieczeństwa danych osobowych przetwarzanych w przedsiębiorstwie
- w przypadku stwierdzenia naruszenia, jeśli to możliwe zobowiązana jest do podjęcia niezbędnych, koniecznych działań minimalizujących skutki naruszenia
- ochronę danych osobowych oraz środków wykorzystywanych do przetwarzania danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
- korzystanie z systemów informatycznych firmy w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń
- bezterminowe zachowanie w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
- zachowanie szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych w celu ochrony interesów osób, których dane dotyczą.
- przestrzegania tzw. zasady czystego biurka poprzez:
 - Niepozostawianie w obszarze stanowiska pracy dokumentów i nośników podczas nieobecności przy stanowisku;
 - Nieprzechowywanie niezabezpieczonych dokumentów i nośników, które nie są konieczne do realizacji bieżącej czynności na stanowisku pracy;
 - Zabezpieczanie dokumentów i nośników przed nieuprawnionym dostępem
- Niszczona dokumentów i nośników danych w taki sposób, ażeby zaznajomienie było niemożliwe – za wykorzystaniem niszczarek lub innych metod bezpiecznej utylizacji

Podstawa przetwarzania danych osobowych

Administrator danych przetwarza dane wyłącznie w przypadku, gdy 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 celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią.

Pracownik bądź inna osoba w przedsiębiorstwie posiadający upoważnienie do przetwarzania danych osobowych winna w toku podejmowanych czynności, na bieżąco monitorować czy przetwarzane przez niego dane spełniają ww. kryteria legalności.

Zgoda na przetwarzanie danych osobowych

W przypadkach, gdy koniecznym jest uzyskanie zgody na przetwarzanie danych osobowych, Administrator danych zapewnia, ażeby osoba udzielająca zgody miała pełną świadomość skutków udzielenia zgody.

Za skutecznie udzielenie zgody na przetwarzanie danych uważa się złożenie oświadczenia o wyrażeniu zgody, które spełnia poniższe kryteria:

1. zgoda udzielona została dobrowolnie i świadomie przez osobę, której dane dotyczą;
2. zgoda wskazuje, w jakim zakresie dozwolone jest przetwarzanie danych przez Administratora danych, tj. jakie kategorie danych obejmuje.
3. zgoda wskazuje, w jakim celu dozwolone jest przetwarzanie danych przez Administratora danych.

Przed uzyskaniem zgody od osoby, której dane dotyczą, Administrator danych informuje, że zgoda może być odwołana w każdym czasie.

Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

Administrator jest w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na operację przetwarzania. Administrator danych prowadzi ewidencje udzielonych zgód na przetwarzanie danych osobowych podmiotu. Jeżeli zgoda udzielona została ustnie, celem spełnienia zasady rozliczalności, członek personelu Administratora danych sporządza notatkę służbową wskazującą przez kogo i w jakim zakresie udzielona została zgoda.

Wzór zgody na przetwarzanie danych osobowych stanowi załącznik do niniejszej Polityki.

Przetwarzanie danych osobowych na podstawie przepisu prawa, umowy, uzasadnionego interesu

Administrator danych uprawniony jest do przetwarzania danych osobowych również wówczas, gdy wynika to z:

1. Przepisu prawa, który nakłada na niego obowiązek określonego działania
2. Zawartej umowy, celem jej realizacji
3. W związku z realizacją uzasadnionego interesu Administratora danych

Administrator danych szczegółowo określa podstawę przetwarzania przez niego danych osobowych, w tym wskazuje swój uzasadniony interes.

Powierzenie przetwarzania danych osobowych

Administrator danych może zlecić innemu podmiotowi przetwarzanie danych osobowych w celu realizacji określonego zadania. W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przede wszystkim cel i zakres przetwarzania danych osobowych

6. Prawa osób, których dane dotyczą

Administrator danych zobowiązany jest do zapewnienia realizacji praw osób, których dane dotyczą, podejmuje w tym celu następujące działania:

1. Wdraża procedury ułatwiające osobie, której dane dotyczą, wykonywanie praw, poprzez udzielenie informacji o powołanych u Administratora danych stanowiskach z zakresu bezpieczeństwa danych, w tym podania danych kontaktowych do osób pełniących stosowne funkcje
2. Wdraża kanały komunikacji z osobami, których dane dotyczą
3. Uświadamia wszystkich pracowników i inne osoby przetwarzające dane w przedsiębiorstwie o prawach osób, których dane dotyczą i sposobach ich realizacji;
4. Informuje osoby, których dane dotyczą o przysługujących im prawach i sposobach ich realizacji, w szczególności poprzez stosowanie klauzuli informacyjnych
5. Udostępnia do powszechnej wiadomości, wyciąg z niniejszej Polityki obejmujący [rozdział 6 – Prawa osób, których dane dotyczą](#), w ogólnodostępnym miejscu

Obowiązki informacyjne

Niezależnie od podstawy przetwarzania danych osobowych, osoba, której dane dotyczą uzyskuje stosowne informacje. Treść klauzuli informacyjnej uzależniona jest od sposobu pozyskania danych.

Jeżeli dane pozyskiwane są bezpośrednio od osoby, której dane dotyczą Administrator danych udziela informacji zgodnie z *załącznikiem – Klauzula informacyjna* – art. 13 RODO

Jeżeli dane osoby, której dane dotyczą pozyskiwane są od osoby trzeciej, Administrator udziela informacji zgodnie z *załącznikiem – Klauzula informacyjna* – art. 14 RODO

Administrator może odstąpić od udzielenia informacji objętych klauzulami jeżeli osoba, której dane dotyczą je posiada, a Administrator danych jest w stanie tą okoliczność wykazać.

Odstąpienie od udzielenia informacji wymaga indywidualnej decyzji Administratora danych i zostaje stosownie udokumentowane.

Informacje o przetwarzaniu danych osobowych dotyczących osoby, której dane dotyczą, należy przekazać tej osobie w momencie zbierania danych, a jeżeli danych nie uzyskuje się od osoby, której dane dotyczą, lecz z innego źródła – w rozsądnym terminie, nie dłuższym niż 30 dni.

W przypadku kiedy dane osobowe stosowane są wyłącznie do komunikacji z osobą, której dane dotyczą w związku z realizacją umowy zawartej z podmiotem trzecim będącym Administratorem danych osoby, New Tech Center OU najpóźniej przy pierwszej takiej komunikacji z osobą, informuje o przetwarzaniu danych oraz udziela stosownych, dalszych informacji.

Uprawnienia osoby, której dane dotyczą

Administrator danych zapewnia realizację praw osoby, której dane dotyczą poprzez poinformowanie jej o przysługujących prawach i sposobach ich realizacji, na następujących zasadach.

Każda osoba, której dane są przez Administratora danych przetwarzane ma możliwość zgłoszenia żądania:

1. dostępu do swoich danych,
2. sprostowania swoich danych,
3. przeniesienia swoich danych,
4. usunięcia lub ograniczenia przetwarzania swoich danych (tzw. prawo do bycia zapomnianym)
5. wniesienia skargi do organu nadzorczego
6. wniesienia sprzeciwu

Żądania określone w pkt 1 – 4 oraz 6, zostają zgłoszone przez osobę uprawnioną w formie pisemnej lub elektronicznej.

Wszelkie zgłoszenia rozpoznane są niezwłocznie, w terminie nie dłuższym niż 30 dni. Jeżeli z przyczyn niezawinionych przez Administratora zachowanie ww. terminu nie jest możliwe, Administrator danych zawiadamia zgłaszającego o planowanym rozpatrzeniu zgłoszenia. Powyższy termin może zostać przedłużony maksymalnie do 3 miesięcy łącznie, z uwagi na skomplikowany charakter żądania lub znaczną liczbę żądań.

Administrator danych informuje również o nieuwzględnieniu żądania i wskazuje podstawy takiej decyzji.

Jeśli zgłaszający przekazał żądanie za pomocą komunikacji drogą elektroniczną, kanał ten zostaje zachowany, chyba że osoba, której dane dotyczą, zażąda innej formy komunikacji. Każdy pracownik Administratora danych lub inna osoba przetwarzająca dane osobowe w przedsiębiorstwie, posiadająca uprawnienia do przetwarzania danych obowiązana jest na żądanie osoby, której dane dotyczą, do udzielenia informacji o jej prawach i sposobach ich realizacji.

Administrator danych prowadzi dokumentację dotyczącą wniesionych żądań w formie elektronicznej. Dokumentacja obejmuje wszystkie czynności podjęte w ramach postępowania z wniosków osób, których dane dotyczą, a po jego zakończeniu przechowywana jest przez okres 1 roku

Prawo dostępu i informacji

Każda osoba, której dane dotyczą ma prawo pozyskania informacji czy Administrator danych przetwarza jej dane osobowe, a jeżeli tak to w jakim zakresie i na jakich zasadach.

W celu zapewnienia realizacji przedmiotowego uprawnienia, Administrator danych zapewnia, żeby każda osoba, której dane dotyczą mogła uzyskać informację o przetwarzaniu jej danych poprzez zgłoszenie żądania w tym zakresie.

Zapytanie o przetwarzanie danych może zostać zgłoszone w formie pisemnej lub elektronicznej jednakże jeżeli obejmuje wniosek o udzielenie informacji o celach przetwarzania, kategorii przetwarzanych danych, informacji o odbiorcach danych i innych szczegółowych informacji, lub żądanie udostępnienia kopii danych, Administrator danych poprzedzi odpowiedź, dokonując czynności weryfikacyjnych mających na celu zidentyfikowanie czy otrzymane zgłoszenie zostało przedłożone rzeczywiście przez osobę, której dane dotyczą.

Osoba, której dane dotyczą ma prawo do następujących informacji dotyczących przetwarzania jego danych przez Administratora danych w poniższym zakresie:

1. Wskazanie celów przetwarzania danych
2. Wskazanie kategorii przetwarzanych danych osobowych

3. Podanie informacji o odbiorcach lub kategoriach odbiorców danych
4. Wskazanie okresu przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
5. Udzielenie informacji o przysługujących uprawnieniach podmiotowi danych, w tym informacji o prawie wniesienia skargi do organu nadzorczego,
6. Wskazanie informacji o źródle danych, jeżeli Administrator pozyskał dane od innej osoby niż zgłaszający Podmiot danych.
7. Poinformowania o zautomatyzowanym podejmowaniu decyzji (jeżeli takie administrator realizuje wobec tej osoby), w tym o profilowaniu oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Niezależnie od żądania informacyjnego, osoba, której dane są przetwarzane przez Administratora danych ma prawo żądania uzyskania do tych danych bezpośredniego dostępu. Realizacja tego prawa następuje poprzez udostępnienie przez Administratora kopii danych.

Sprostowanie danych

Podmiot danych, którego dane osobowe są przetwarzane przez Administratora danych ma prawo weryfikacji aktualności i poprawności przetwarzanych swoich danych osobowych. Za nieprawidłowe uznawane są takie dane, które odbiegają od danych rzeczywistych, w szczególności wówczas gdy dane:

1. Zapisane są błędnie (omyłki pisarskie);
2. Są nieaktualne (nastąpiła zmiana okoliczności np. zmiana nazwiska);
3. Są niepełne (nie uwzględniają określonej kategorii danych).

Podmiot danych wskazuje w żądaniu dane, które są nieprawidłowe podając jednocześnie właściwą wersję danych. Celem weryfikacji, Administrator może zobowiązać Podmiot danych do złożenia stosownego oświadczenia.

Podmiot danych uprawniony jest do żądania sprostowania lub uzupełnienia danych.

Na czas prowadzenia czynności wyjaśniających przez Administratora, Podmiot danych może żądać ograniczenia przetwarzania danych w zakresie objętym wnioskiem.

Przeniesienie danych

Podmiot danych, którego dane osobowe są przetwarzane przez Administratora danych:

1. w sposób zautomatyzowany (za pomocą systemów informatycznych)
- oraz
2. na podstawie udzielonej zgody na przetwarzanie danych lub na podstawie zawartej umowy

ma prawo wniesienia żądania przeniesienia jego danych osobowych.

Spełnienie ww. warunków musi nastąpić łącznie.

Prawo osoby, której dane dotyczą wyraża się:

1. w obowiązku Administratora danych do przekazania żądającemu kopii danych, które uprzednio zostały Administratorowi przekazane w związku z zawarciem i realizacją umowy lub na podstawie zgody.

Dane zostają przekazane w ujednoliconym, powszechnie używanym formacie nadającym się do odczytu maszynowego tj. formie pliku .docx lub wydruku komputerowego, w zależności od formy wystąpienia z żądaniem

2. w obowiązku przesłania przez Administratora bezpośrednio innemu podmiotowi, danych dotyczących zgłaszającego - o ile jest to technicznie możliwe.

Tym samym Administrator danych zapewnia Podmiotowi danych, gwarancje ponownego i pełnego wykorzystania danych osobowych zapisanych w formacie udostępnianego pliku.

Usunięcie lub ograniczenie przetwarzania

Osoba, której dane dotyczą ma prawo zgłosić żądanie ograniczenia przetwarzania danych jego dotyczących, w przypadku:

1. kwestionowania prawidłowości danych
2. osoba, której dane dotyczą sprzeciwia się usunięciu danych jego dotyczących
3. podmiot danych wniósł sprzeciw wobec przetwarzania jego danych osobowych

Ograniczenie przetwarzania następuje od chwili wniesienia żądania, przez czas konieczny do przeprowadzenia postępowania wyjaśniającego przez Administratora danych.

W czasie ograniczenia przetwarzania danych, Administrator uprawniony jest wyłącznie do ich przechowywania. Pozostałe operacje na danych wymagają zgody osoby, której dane dotyczą. Dopuszczalnym jest jednak przetwarzanie danych w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej.

Administrator ogranicza przetwarzanie danych osobowych poprzez:

1. czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania,
2. blokadę dostępu do wybranych danych.

Osoba, której dane dotyczą ma prawo zgłosić żądanie usunięcia danych jego dotyczących, przetwarzanych przez Administratora danych, w następujących sytuacjach:

1. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
2. osoba, której dane dotyczą cofnęła zgodę, na której opiera się przetwarzanie zgodnie i brak jest innej podstawy prawnej przetwarzania;
3. osoba, której dane dotyczą wniósł skuteczny sprzeciw wobec przetwarzania jego danych;
4. dane osobowe były przetwarzane niezgodnie z prawem;
5. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w przepisach prawa powszechnie obowiązującego;
6. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1. RODO

Dane nie podlegają usunięciu jeżeli ich przetwarzanie jest niezbędne:

1. do korzystania z prawa do wolności wypowiedzi i informacji;
2. do wywiązania się przez Administratora danych z prawnego obowiązku wymagającego przetwarzania lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
3. z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego;
4. do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych;
5. do ustalenia, dochodzenia lub obrony roszczeń.

Administrator danych jako podmiot działający w sektorze prywatnym ze szczególną uwagą weryfikuje wystąpienie okoliczności ujętych w pkt 2 i 5.

Jeżeli żądanie usunięcia danych dotyczy danych udostępnionych przez Administratora danych podmiotom trzecim, Administrator zawiadamia powyższe podmioty, które przetwarzają takie dane osobowe o usunięciu wszelkich łączy do tych danych, kopii lub powieleń tych kopii.

Sprzeciw Podmiotu danych

Osoba, której dane dotyczą ma prawo do wniesienia sprzeciwu dotyczącego przetwarzania danych jego dotyczących, wyłącznie wówczas gdy:

1. Administrator danych przetwarza dane w celu wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
2. Administrator danych przetwarza dane w celu realizacji jego prawnie uzasadnionych interesów.

Prawo do wniesienia sprzeciwu nie jest ograniczone czasowo, Podmiot danym może wnieść sprzeciw w każdym czasie.

Pomimo wniesienia sprzeciwu Administrator danych jest uprawniony ich przetwarzania wyłącznie wówczas, gdy:

1. występują istotne i prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą,
2. przetwarzanie związane jest z koniecznością ustalenia, dochodzenia lub obrony roszczeń.

Ciężar wykazania, istnienia ważnych prawnie uzasadnionych interesów Administratora danych spoczywa na nim samym.

7. Reguły bezpieczeństwa przetwarzania danych osobowych

Administrator danych wdraża odpowiednie środki techniczne, fizyczne i organizacyjne, celem zapewnienia właściwego poziomu bezpieczeństwa przetwarzanych danych osobowych.

W oparciu o przeprowadzoną analizę ryzyka naruszenia praw lub wolności osób związaną z przetwarzaniem danych, uwzględniającą różny stopień prawdopodobieństwa wystąpienia i wagę zagrożenia, Administrator wprowadził stosowne zabezpieczenia.

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres i cele przetwarzania oraz ww. ryzyko, Administrator danych wprowadził poziomy zabezpieczeń:

1. Poziom standardowy, obejmujący:
 1. organizacyjne środki zabezpieczania danych,
 2. techniczne środki zabezpieczania danych,
 3. fizyczne środki zabezpieczania danych

Zabezpieczenia tego poziomu obowiązują na wszystkich stanowiskach, na których dochodzi do przetwarzania danych, niezależnie od zakresu przetwarzania i częstotliwości. Poziom standardowy zabezpieczeń obejmuje przetwarzanie danych standardowych oraz danych których ryzyko przetwarzania nie przekracza ustalonego poziomu granicznego. Każdy pracownik bądź inna osoba przetwarzająca dane osobowe w przedsiębiorstwie upoważniona do ich przetwarzania obowiązana jest stosować następujące zasady:

1. Organizacyjne środki zabezpieczania danych

Przetwarzanie danych odbywa się przy zachowaniu poniższych zasad:

- Przetwarzanie danych następuje wyłącznie przez osoby posiadające upoważnienie i zaznajomione z zasadami przetwarzania danych przyjętymi przez Administratora danych
- Administrator danych zapewnia, ażeby osoby, za pomocą których dokonywane jest przetwarzanie danych zostały przeszkolone z zakresu bezpieczeństwa danych osobowych
- Obszarami przechowywania danych osobowych są serwery New Tech Center OU
- Zabranie się przenoszenia danych poza wyznaczone obszary, w szczególności poza serwisy wskazane w pkt 3 powyżej. Odstępstwo od tej zasady każdorazowo poprzedzone jest decyzją Administratora oraz zastosowanie odpowiednich środków zabezpieczeń.
- Udostępnianie lub powierzanie danych osobowych odbywa się wyłącznie w oparciu o zawarte umowy powierzenia lub porozumienia.

2. Techniczne środki zabezpieczania danych

Dane osobowe znajdujące się w obszarach, o których mowa w art. 7 ust. 1 pkt 3 zabezpieczone są przy użyciu następujących środków technicznych:

- Certyfikaty SSL
- Cloudflare
- Certyfikaty ISO 27001 i 20000
- 2FA (dwustopniowa weryfikacja)
- Hasło

8. Udostępnienie danych osobowych

Udostępnienie danych osobowych w firmie dopuszcza się na podstawie jednej z podstaw prawnych określonych w RODO lub na podstawie przepisów innych ustaw. Administrator danych prowadzi ewidencję udostępniania danych osobowych instytucjom i osobom spoza przedsiębiorstwa.

9. Procedura postępowania na wypadek naruszeń

Postępowanie w przedmiocie naruszenia ochrony danych osobowych

Przez naruszenie ochrony danych (incydent) należy rozumieć każde zdarzenie skutkujące lub mogące skutkować (naruszenie potencjalne):

1. Utratą całkowitą lub częściową danych osobowych, w tym uszkodzeniem danych;
2. Nieuprawnionym dostępem do danych, zarówno nieuprawnionym udostępnieniem jak i nieuprawnionym pozyskaniem;
3. Nieuprawnioną modyfikacją danych

Naruszenie może wystąpić na każdym etapie przetwarzania danych, w toku zbierania, utrwalania, przechowywania, opracowywania, zmieniania, udostępniania i usuwania.

Naruszenie może wystąpić w obszarze przetwarzania danych w wersji papierowej jak i w systemie informatycznym.

Każdy pracownik lub inna osoba przetwarzająca dane osobowe w przedsiębiorstwie Administratora danych niezwłocznie po powzięciu informacji lub uzasadnionego podejrzenia o incydencie obowiązana jest:

1. Powiadomić Administratora danych o incydencie określając:
 - o Czas i miejsce zdarzenia
 - o Istotne informacje o zdarzeniu
2. Podjąć działania zaradcze mające na celu minimalizację skutków incydentu

Administrator danych niezwłocznie po zawiadomieniu podejmuje działania:

1. Wyjaśniające przyczynę i przebieg zdarzenia
2. Ustalające udział osób trzecich w zdarzeniu
3. Zabezpieczające ślady i dowody zdarzenia
4. Ustalające szacunkowy zasięg skutków zdarzenia, w tym:
 - o Ilość danych narażonych incydemem;
 - o Kategorie danych narażonych incydemem.
5. Ochronne przed wystąpieniem zdarzenia w przyszłości.

Z przebiegu zdarzenia oraz przyjętych środków minimalizujących wystąpienie zdarzenia w przyszłości sporządzana zostaje stosowna dokumentacja. Wnioski w niej ujęte uwzględniane zostają w toku prac aktualizacyjnych nad systemem bezpieczeństwa danych Administratora danych

Administrator danych prowadzi rejestr wszystkich ujawnionych naruszeń ochrony danych, w tym naruszeń nie podlegających notyfikacji lub zawiadomieniu osoby, której dane dotyczą

Obowiązek notyfikacji organu nadzorczego

Każdorazowo w przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator danych zawiadamia organ nadzorczy. Zawiadomienie następuje niezwłocznie, nie później jednak niż w terminie 72 godzin od stwierdzenia naruszenia. Niezachowanie ww. terminu dopuszczalne jest wyłącznie w drodze wyjątku, w szczególnie uzasadnionych przypadkach. Wówczas zawiadomienie zawiera wyjaśnienie przyczyn opóźnienia.

Obowiązek notyfikacji nie dotyczy naruszenia ochrony danych jeżeli prawdopodobieństwo, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych jest znikome. Decyzję w tym zakresie podejmuje Administrator danych

Wzór formularza zawiadomienie zawarty stanowi załącznik do niniejszej Polityki – *Zawiadomienie o naruszeniu*.

Zawiadomienie osoby, której dane dotyczą

Wzór formularza zawiadomienie stanowi załącznik do niniejszej Polityki - *Zawiadomienie o naruszeniu*

10. Postanowienia końcowe

Przedmiotowa Polityka Bezpieczeństwa Ochrony Danych Osobowych stanowi dokument wewnętrzny Administratora danych, z którego treścią zapoznani zostają wszyscy pracownicy Administratora danych

Nie może ona zostać udostępniona osobom nieupoważnionym, chyba, że jest to konieczne dla realizacji obowiązków Administratora danych wynikających z przepisów prawa lub w

celu realizacji umowy. Każdorazowa decyzja o udostępnieniu Polityki lub wyciągu z niej poprzedzona zgodą Administratora udzieloną na piśmie.

Każdy z pracowników Administratora danych zobowiązany jest złożyć oświadczenie o tym, iż został zapoznany z obowiązującymi przepisami oraz przyjętymi regulacjami znajdującymi się w niniejszej Polityce, a także o zobowiązaniu się do ich przestrzegania.

W sprawach nieuregulowanych w przyjętej Polityce i dokumentacji wewnętrznej Administratora danych z zakresu bezpieczeństwa danych zastosowanie mają przepisy RODO oraz krajowych aktów prawa powszechnie obowiązującego.