Polityka Ochrony Danych Osobowych

1. Polityka Ochrony Danych Osobowych, zwana dalej „Polityką", określa środki techniczne i organizacyjne zastosowane przez Administratora Danych dla zapewnienia ochrony danych osobowych oraz tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych osobowych w systemie informatycznym lub w kartotekach, albo w sytuacji podejrzenia o takim naruszeniu.
2. Celem niniejszej Polityki ochrony danych osobowych (RODO) jest wypełnienie założeń 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 (ogólne rozporządzenie o ochronie danych, dalej też zwane RODO).
3. Nadzór nad przestrzeganiem zasad opisanych w niniejszej Polityce oraz przepisów ochrony danych osobowych pełni Administrator danych.
4. Definicje i załączniki:
   1) **Administrator danych** - oznacza osobę fizyczną lub prawną, podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

      Administratorem jest: STOWARZYSZENIE KRAKOWSKI KOMITET ZWALCZANIA RAKA z siedzibą w Krakowie, Pawia 8/, 31-154 Kraków, wpisanym do rejestru przedsiębiorców prowadzonym przez Sąd Rejonowy dla Krakowa-Śródmieścia w Krakowie Wydział XI Gospodarczy - Krajowy Rejestr Sądowy pod nr KRS 0000376025, NIP 6762434912 (dalej jako ADO).
   2) **bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
   3) **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;
   4) **dane szczególne** - oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne,

biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;

6) **hasło** – rozumie się przez to ciąg znaków alfanumerycznych, znany jedynie użytkownikowi;
7) **identyfikator** – rozumie się przez to, ciąg znaków literowych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
8) **incydent ochrony danych osobowych** – zdarzenie albo seria niepożądanych lub niespodziewanych zdarzeń ochrony danych osobowych stwarzających znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrożenia ochrony danych osobowych.
9) **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.
10) **obszar przetwarzania danych** – rozumie się przez to budynki i pomieszczenia określone przez administratora danych, tworzące obszar, w którym przetwarzane są dane osobowe i inne informacje prawem chronione.
11) **odbiorca danych** – 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;
12) **osoba, podmiot danych** - oznacza osobę, której dane dotyczą;
13) **podmiot przetwarzający** - oznacza organizację lub osobę, której ADO powierzył przetwarzanie danych osobowych.
14) **polityka** - oznacza niniejszą politykę ochrony danych osobowych;
15) **postępowanie z ryzykiem** – proces planowania i wdrażania działań wpływających na ryzyko; Ryzyko – niepewność osiągnięcia zamierzonych celów;
16) **poufność danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom; szacowanie ryzyka – proces identyfikowania, analizowania i oceniania ryzyka;
17) **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;

18) **RODO** - oznacza rozporządzenie parlamentu europejskiego i rady (UE) 2016/679 z 27.04.2016 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.Urz. UE l 119, s. 1).
19) **serwisant** – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego;
20) **system informatyczny administratora danych** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych;
21) **teletransmisja** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
22) **uwierzytelnienie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
23) **użytkownik** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło;
24) **zgoda 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.

5. W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.
6. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów i zapewnić:
   1) **rozliczalność** – rozumie się przez to właściwość zapewniającą, że działania użytkownika mogą być przypisane w sposób jednoznaczny tylko temu użytkownikowi;
   2) **integralność danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) **poufność danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
   4) **integralność systemu** – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej jak i przypadkowej.

7. Za przestrzeganie zasad ochrony i bezpieczeństwa danych odpowiedzialni są użytkownicy.
8. Realizację powyższych zamierzeń powinny zagwarantować następujące założenia:
    1) Wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania danych osobowych oraz ich odpowiedzialność za ochronę tych danych.
    2) Przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych.
    3) Przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory).
    4) Podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń,
    5) Okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych.
9. **Za naruszenie ochrony danych osobowych uważa się w szczególności**:
    1) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują
    2) naruszenie lub próby naruszenia integralności danych rozumiane jako wszelkie modyfikacje, zniszczenia lub próby ich dokonania przez osoby nieuprawnione lub uprawnione działające w złej wierze lub jako błąd w działaniu osoby uprawnionej (np. zmianę zawartości danych, utratę całości lub części danych),
    3) naruszenie lub próby naruszenia integralności systemu
    4) zmianę lub utratę danych zapisanych na kopiach zapasowych,
    5) naruszenie lub próby naruszenia poufności danych,
    6) nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
    7) udostępnienie osobom nieupoważnionym danych osobowych
    8) zniszczenie, uszkodzenie lub wszelkie próby nieuprawnionej ingerencji w system informatyczny zmierzające do zakłócenia jego działania bądź pozyskania w sposób niedozwolony lub w celach niezgodnych z przeznaczeniem danych zawartych w systemie,
    9) inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy.
10. **Za naruszenie ochrony danych osobowych uważa się również włamanie do budynku lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań**.
11. Dla zapewnienia bezpieczeństwa danych i informacji zastosowano następujące środki organizacyjne:
    1) Każda osoba działająca z upoważnienia Administratora i mająca dostęp do danych osobowych przetwarzała je wyłącznie na polecenie Administratora.

2) Każdy z pracowników i współpracowników powinien zachować szczególną ostrożność przy przenoszeniu danych.
3) Należy chronić dane przed dostępem do nich osób nieupoważnionych.
4) Pomieszczenia w których są przetwarzane dane osobowe powinny być zamykane na klucz.
5) Dostęp do kluczy posiadają tylko upoważnieni pracownicy i współpracownicy.
6) Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W wypadku, gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia Administratora.
7) Dostęp do pomieszczeń, w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy.
8) W przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
9) Szafy, w których przechowywane są dane powinny być zamykane na klucz.
10) Klucze do tych szaf posiadają tylko upoważnieni pracownicy.
11) Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych, a następnie powinny być zamykane.
12) Dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych, a następnie muszą być chowane do szaf.
13) Dostęp do komputerów, na których są przetwarzane dane - mają tylko upoważnieni pracownicy i współpracownicy.
14) Monitory komputerów, na których przetwarzane są dane, są tak ustawione, aby osoby nieupoważnione nie miały wglądu w dane.
15) W wypadku potrzeby wyniesienia komputera przenośnego (np. typu laptop, notebook) zawierającego dane osobowe, lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane.
16) Nie należy udostępniać osobom nieupoważnionym tych komputerów.
17) W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami - należy dokonać tego z zachowaniem szczególnej ostrożności.
18) Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe.
19) W wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM, pendrive) - należy taki nośnik zniszczyć fizycznie.
20) W przypadku wykorzystania do przenoszenia dysków - dane należy kasować z tych dysków.
21) Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.

22) Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz.
23) Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione - niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.

12. W przypadku stwierdzenia naruszenia:
    1) zabezpieczenia systemu informatycznego,
    2) technicznego stanu urządzeń,
    3) zawartości zbioru danych osobowych,
    4) ujawnienia metody pracy lub sposobu działania programu,
    5) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
    6) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

    każda osoba zatrudniona przy przetwarzaniu danych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora danych.
13. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe.

    Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.
14. Dostęp do danych osobowych:
    1) Przetwarzanie, w tym udostępnianie danych osobowych jest prawnie dopuszczalne, jeżeli jest niezbędne dla zrealizowania obowiązku wynikającego z przepisu prawa.
    2) W przypadku udostępnienia danych osobowych w celach innych niż włączenie do rejestru, administrator danych udostępnia posiadane informacje osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
    3) Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
    4) Podmiot występujący o udostępnienie informacji powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żądania ich udostępnienia. Tylko w takiej sytuacji można dokonać oceny, czy w określonym przypadku udostępnienie danych jest prawnie dopuszczalne i czy nie będzie ono stanowić naruszenia zasad ochrony informacji.
    5) Przetwarzanie, w tym udostępnianie danych osobowych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby,

której dane dotyczą, oraz następuje w celu badań naukowych, dydaktycznych, historycznych oraz statystycznych.

6) Udostępnienie danych może nastąpić jedynie za zgodą Administratora danych i powinno być odpowiednio udokumentowane.

15. Prawa podmiotów danych.

    Każdej osobie, której dane osobowe są przetwarzane, przysługuje prawo do kontroli przetwarzania jej danych osobowych, a w szczególności prawo do:

    1) uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby Administratora Danych;
    2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych osobowych;
    3) uzyskania informacji, od kiedy są przetwarzane jej dane osobowe oraz podania w powszechnie zrozumiałej formie treści tych danych;
    4) uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące;
    5) uzyskania informacji o sposobie udostępniania danych osobowych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane;
    6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów prawa albo są już zbędne do realizacji celu, dla którego zostały zebrane.

16. Polityka jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.
17. Użytkownicy są zobowiązani zapoznać się z treścią Polityki.
18. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie aktualnie obowiązujące przepisy prawa w zakresie ochrony danych osobowych.
19. Użytkownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych postanowień zawartych w niniejszej Polityce. W wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących u Administratora Danych, użytkownicy mają obowiązek stosowania unormowań dalej idących, których stosowanie zapewni wyższy poziom ochrony informacji.

Zatwierdzam

.....

(data, podpis, pieczątka Administratora)