Fundacja Pomocy na rzecz Poszkodowanych w Wypadkach
Komunikacyjnych i z Dysfunkcją Neurologiczną "WSTAŃ"
ul. Zbożowa 30A, 20-827 Lublin
NIP 712-322-88-85, Regon 060687496, KRS 0000367755
BGŻ 39 2030 0045 1110 0000 0275 1390

# Polityka Ochrony Danych Osobowych w Fundacji Pomocy Na Rzecz Poszkodowanych w Wypadkach Komunikacyjnych i z Dysfunkcją Neurologiczną "Wstań"z siedzibą w Lublinie

Polityka Ochrony Danych Osobowych sporządzona została w celu określenia zasad ochrony danych osobowych stosowane przez Fundację pomocy na rzecz poszkodowanych w wypadkach komunikacyjnych i z dysfunkcją neurologiczną "Wstań" z siedzibą w Lublinie [dalej: Fundacja Wstań]- Administrator / Podmiot przetwarzający (dalej użyte pojęcie Administratora oznacza i/lub Podmiot przetwarzający) w celu spełnienia wymagań Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 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 jako „RODO") oraz Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018 poz. 1000 z dnia 2018.05.24 ).

**Najważniejsze definicje:**

**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

**Administrator** - 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

**Podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora

**Przetwarzanie**- 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;

**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;

**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;

**Inwentaryzacja danych**

Dane osobowe wymagające ochrony zostały wykazane w Rejestrze kategorii czynności przetwarzania. Rejestr obejmuje zbiory ze stwierdzonym potencjalnym ryzykiem naruszenia praw lub wolności osób fizycznych.

**Administrator zapewnia, że:**

1. dane są legalnie przetwarzane
2. dane osobowe są adekwatne w stosunku do celów przetwarzania
3. dane osobowe są przetwarzane przez określony konkretny czas
4. wobec osób, które przetwarza administrator wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14) wraz ze wskazaniem im praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu)

Fundacja Pomocy na rzecz Poszkodowanych w Wypadkach
Komunikacyjnych i z Dysfunkcją Neurologiczną "WSTAŃ"
ul. Zbożowa 30A, 20-827 Lublin
NIP 712-322-88-85, Regon 060687496, KRS 0000367755
BGŻ 39 2030 0045 1110 0000 0275 1390

5. zapewniono ochronę danych w przypadku powierzenia przetwarzania danych w postaci umów powierzenia z podmiotami przetwarzającymi (art. 28)

**Upoważnienia**

1. Administrator odpowiada za nadawanie i anulowanie upoważnień do przetwarzania danych we wszystkich zbiorach.
2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.
3. Upoważnienia nadawane są w formie udokumentowanego zakresu obowiązków.
4. Upoważnienia mogą być nadawane w formie poleceń.

**Instrukcja postępowania z incydentami**

Procedura definiuje katalog prawdopodobieństwa wystąpienia i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest zminimalizowanie skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu prawdopodobieństwa wystąpienia lub wystąpieniu incydentu bezpośredniego przełożonego.
2. Do typowych zagrożeń dla bezpieczeństwa danych osobowych należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)
4. W przypadku stwierdzenia wystąpienia incydentu, Administrator prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki
    b. inicjuje ewentualne działania dyscyplinarne
    c. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu
    d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia
5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.
7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

**Regulamin Ochrony Danych Osobowych**

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania. Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

**Szkolenia**

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznana z przepisami RODO.
2. Za przeprowadzenie szkolenia odpowiada Administrator .
3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia .

**Procedura przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego**

Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

**Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych**

Administrator zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości Przetwarzanych danych. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych. Środki obejmują Ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do osób odpowiednio upoważnionych. Inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie osoby upoważnionej.

**Polityka bezpieczeństwa informacji**

a) Zamykanie pomieszczeń tworzących obszar Przetwarzania danych osobowych na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich.
b) Wykorzystanie zamykanych szafek i sejfów do zabezpieczenia dokumentów.
c) Wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe.
d) Ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz,
e) Wykonywanie kopii awaryjnych ,
f) Ochronę sprzętu komputerowego wykorzystywanego u administratora przed złośliwym oprogramowaniem,
g) Zabezpieczenie dostępu do urządzeń przy pomocy haseł dostępu
h) Wykorzystanie szyfrowania danych przy ich transmisji.

Fundacja Pomocy na rzecz Poszkodowanych w Wypadkach Komunikacyjnych i z Dysfunkcją Neurologiczną "WSTAŃ"
ul. Zbożowa 30A, 20-827 Lublin
NIP 712-322-88-85, Regon 060687496, KRS 0000367755
BGŻ 39 2030 0045 1110 0000 0275 1390

Prezes Zarządu Fundacji
"WSTAŃ"
Grażyna Rokosz

Fundacja Pomocy na rzecz Poszkodowanych w Wypadkach
Komunikacyjnych i z Dysfunkcją Neurologiczną "WSTAŃ"
ul. Zbożowa 30A, 20-827 Lublin
NIP 712-322-88-85, Regon 060687496, KRS 0000367755
BGŻ 39 2030 0045 1110 0000 0275 1390

# KLAUZULA INFORMACYJNA DLA DARCZYŃCY

Wykonując zobowiązania wynikające z art. 13 ust. 1 i 2 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. Urz. UE L 119/1 z 04.05.2016 r.), dalej jako „RODO" Fundacja Pomocy Na Rzecz Poszkodowanych w Wypadkach Komunikacyjnych i z Dysfunkcją Neurologiczną "Wstań" z siedzibą w Lublinie, ul. Zbożowa 30A, 20-837 Lublin, wpisana do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej prowadzonego przez Sąd Rejonowy Lublin-Wschód W Lublinie z Siedziba w Świdniku, VI Wydział Gospodarczy Krajowego Rejestru Sadowego pod numerem 0000367755 (dalej zwana również: „Fundacją Wstań") informuję, że:

1. Administratorem Pani/Pana danych osobowych jest Fundacja Pomocy Na Rzecz Poszkodowanych w Wypadkach Komunikacyjnych i z Dysfunkcją Neurologiczną "Wstań" z siedzibą w Lublinie, ul. Zbożowa 30A, 20-837 Lublin, kontakt: info@fundacjawstan.pl, nr tel.: 603 995 501;
2. Pani/Pana dane osobowe przetwarzane będą w celu prowadzenia ksiąg rachunkowych i dokumentacji podatkowej, na podstawie art. 6 ust. 1 lit. c RODO w związku z art. 74 ust. 2 ustawy z dnia 29 września 1994 r. o rachunkowości oraz w związku z art. 26 ust. 7 ustawy z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych; Pani/Pana dane osobowe mogą być również przetwarzane w celach kontaktowych z Administratorem, na postawie art. 6 ust. 1 lit. a RODO, tj. odrębnej zgody;
3. Administrator przetwarza następujące kategorie Pani/Pana danych osobowych: imię i nazwisko, dane adresowe, numer rachunku bankowego, inne dane zawarte w tytule wpłaty; Pani/Pana dane osobowe zostały przekazane Administratorowi przez banki, z którymi Administrator zawarł umowy na świadczenie usług bankowych; pozostałe dane osobowe (m.in. adres email, telefon) przetwarzane będą na podstawie wyrażonej przez Panią/Pana odrębnie dobrowolnej zgody;
4. odbiorcą Pani/Pana danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie odrębnych przepisów prawa, upoważnieni pracownicy/współpracownicy Administratora, dostawcy usług technicznych i organizacyjnych;
5. Pani/Pana dane osobowe nie będą przekazywane odbiorcy w państwie trzecim lub organizacji międzynarodowej;
6. Pani/Pana dane osobowe będą przechowywane przez okres przechowywania dokumentacji księgowej i podatkowej wynikający z przepisów prawa, a w przypadku danych przetwarzanych na podstawie zgody - do momentu jej odwołania;
7. posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
8. ma Pani/Pan prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie przez Administratora danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
9. podanie danych osobowych objętych treścią odrębnej zgody jest dobrowolne, jednakże niezbędne do realizacji wyżej wskazanego celu;
10. wobec Pani/Pana nie będą podejmowane zautomatyzowane decyzje, w tym Pani/Pana dane nie będą podlegały profilowaniu.

**Prezes Zarządu Fundacji**
**"WSTAŃ"**

*Grażyna Rokosz*

Fundacja Pomocy na rzecz Poszkodowanych w Wypadkach
Komunikacyjnych i z Dysfunkcją Neurologiczną "WSTAŃ"
ul. Zbożowa 30A, 20-827 Lublin
NIP 712-322-88-85, Regon 060687496, KRS 0000367755
BGŻ 39 2030 0045 1110 0000 0275 1390

# REGULAMIN OCHRONY DANYCH OSOBOWYCH - W FUNDACJI POMOCY NA RZECZ POSZKODOWANYCH W WYPADKACH KOMUNIKACYJNYCH I Z DYSFUNKCJĄ NEUROLOGICZNĄ "WSTAŃ" Z SIEDZIBĄ W LUBLINIE

## I.

## Zasady bezpiecznego użytkowania sprzętu

Pracownik przetwarzający dane osobowe korzystający ze sprzętu IT w miejscu pracy, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony.

1. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT.
2. Samowolne otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
3. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wgląd do danych wyświetlanych na monitorach komputerowych.
4. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOS + L) lub wylogować się z systemu bądź z programu.
5. Po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy po czym zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne na których znajdują się dane osobowe.
6. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkownania komputerów)
7. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien trwale zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce, zniszczenie twardego dysku, pendrive młotkiem)
8. Użytkownicy komputerów przenośnych na których znajdują się dane osobowe lub z dostępem do danych osobowych przez internet zobowiązani są do stosowania zasad bezpieczeństwa zawartych w Regulaminie laptopów.

## II.

## Zarządzanie uprawnieniami

1. Każdy użytkownik z dostępem do danych osobowych (np. na swoim komputerze, na dysku sieciowym, w programie lub aplikacji, w poczcie elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się
2. Użytkownik otrzymuje dostęp i odpowiednie uprawnienia do zasobów i aplikacji na polecenie przełożonych i przy realizacji informatyków-administratorów
3. Użytkownicy nie mają prawa do samodzielnej zmiany uprawnień, np. przydzielenia sobie uprawnień administratora w Windows.
4. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest zatem umożliwianie innym osobom praca na koncie innego użytkownika

## III.

## Polityka haseł

1. Hasła powinny składać się z np. 14 znaków , powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne), nie mogą być łatwe do odgadnięcia, nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty
2. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na widocznych kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie, a w przypadku ujawnienia hasła – należy natychmiast go zmienić

3. Hasła muszą być zmieniane co 60 / 90 dni, jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła

## IV.

## Zabezpieczenie dokumentacji papierowej z danymi osobowymi

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „Polityki czystego biurka"., która polega ona na zamykaniu dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich lub w lesie.

## V.

## Zasady wynoszenia nośników z danymi poza siedzibę

1. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Pracodawcy / Zleceniodawcy.
2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski, zahasłowane pliki)
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach
4. Należy korzystać ze sprawdzonych firm kurierskich
5. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą

## VI.

## Zasady korzystania z internetu

1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem)
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

## VII.

**Zasady korzystania z poczty elektronicznej**

1. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione
2. W przypadku przesyłania danych osobowych poza organizację należy wykorzystywać mechanizmy ochronne (hasłowanie wysyłanych dokumentów lub plików spakowanych, podpis elektroniczny)
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 12 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata
6. **WAŻNE:** Nie należy otwierać załączników (plików) w mailach nawet od rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy. Tego typu maile większości przypadków zawierają załączniki ze szkodliwymi programami, które po „kliknięciu" infekują komputer użytkownika oraz często pozostałe komputery w sieci. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy
7. **WAŻNE:** Bez weryfikacji wiarygodności nadawcy, nie należy „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych. Użytkownik „klikając" na taki hiperlink bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy
8. Należy zgłaszać informatykowi przypadki podejrzanych emaili
9. Użytkownicy nie powinni rozsyłać „niezawodowych" emaili w formie „łańcuszków szczęścia", np. Życzenia Świąteczne adresowane do 230 osób.
10. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości"!
11. Użytkownicy nie powinni rozsyłać, maili zawierających załączniki o dużym rozmiarze
12. Użytkownicy powinni okresowo kasować niepotrzebne maile
13. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych
14. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób
15. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
16. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych
17. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego
18. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania
19. Użytkownik bez zgody Pracodawcy / Zleceniodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy / Zleceniodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej

**VIII.**

**Ochrona antywirusowa**

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe

3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, zainstaluj program antywirusowy", użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Informatyka lub osobę upoważnioną.

## IX.
## Skrócona instrukcja
## postępowania w przypadku naruszenia ochrony danych osobowych

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Pracodawcy / Zleceniodawcy w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych
2. Do sytuacji wymagających powiadomienia, należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
3. Do incydentów wymagających powiadomienia, należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)
4. Typowe przykłady incydentów wymagające reakcji:
    a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania
    b. dokumentacja jest niszczona bez użycia niszczarki
    c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie
    d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe
    e. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe
    f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia Pracodawcy / Zleceniodawcy
    g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej
    h. telefoniczne próby wyłudzenia danych osobowych
    i. kradzież, zagubienie komputerów lub CD, twardych dysków, Pen-drive z danymi osobowymi
    j. maile zachęcające do ujawnienia identyfikatora i/lub hasła,
    k. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów
    l. hasła do systemów przyklejone są w pobliżu komputera

## X.
## Obowiązek zachowania poufności i ochrony danych osobowych

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
    a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Pracodawcę / Zleceniodawcę zadaniach
    b. zachowania w tajemnicy danych osobowych do których mam lub będzie miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Pracodawcę / Zleceniodawcę
    c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Pracodawcę / Zleceniodawcę
    d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych

e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem

2. Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych
3. Osoby zapoznane z treścią niniejszego Regulaminu ODO lub przeszkolone zobowiązane są podpisać Oświadczenie o poufności
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego
5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych

## XI.
## Postępowanie dyscyplinarne

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Pracodawcę / Zleceniodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.

Prezes Zarządu Fundacji
"WSTAŃ"
*Grażyna Rokosz*