PROCEDURA POSTĘPOWANIA
NA WYPADEK NARUSZEŃ BEZPIECZEŃSTWA DANYCH
DLA FUNDACJI WIDZEWA

1. Każda osoba upoważniona do przetwarzania danych osobowych, zobowiązana jest do powiadomienia Administratora, w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.

2. Jeśli naruszenie dotyczy danych osobowych przetwarzanych w ramach infrastruktury IT, o każdym stwierdzonym lub domniemanym naruszeniu bezpieczeństwa danych, należy niezwłocznie poinformować również Dział IT (Administratora Systemów Informatycznych/ Informatyka).

3. Do sytuacji wymagających powiadomienia, należą:

   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,

   b) niewłaściwe zabezpieczenie sprzętu IT oraz 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).

4. 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).

5. 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 pozwalających na wgląd osób postronnych w dane osobowe,

   f) wynoszenie danych osobowych w wersji papierowej i elektronicznej poza siedzibę Przedsiębiorstwa, bez zgody Pracodawcy/Zleceniodawcy/Administratora,

g) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej,

h) telefoniczne próby wyłudzenia danych osobowych,

i) kradzież, zagubienie komputerów lub CD, twardych dysków, pendrive, innych nośników danych z danymi osobowymi,

j) maile zachęcające do ujawnienia identyfikatora i/lub hasła,

k) podejrzenie wirusa komputerowego lub niestandardowe działanie komputerów,

l) pozostawianie niezabezpieczonych haseł do systemów w pobliżu komputera, biurka.

6. Osoba, która wykryła naruszenie, zobowiązana jest podjąć czynności niezbędne do powstrzymania skutków naruszenia oraz ujawnić wszystkie znane jej okoliczności, które uzasadniają podejrzenie o naruszeniu, a także zabezpieczyć wszelkie ślady i dowody umożliwiające ustalenie przyczyn oraz ewentualnych skutków naruszenia do czasu przybycia na miejsce osób odpowiedzialnych (np. poprzez: zabezpieczenie dostępu do miejsca zdarzenia, wstrzymanie pracy na sprzęcie, wykonanie wydruku lub zrzutu ekranu monitora, zabezpieczenie kopii lub wydruków).

7. W przypadku stwierdzenia naruszenia bezpieczeństwa danych, należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia osób odpowiedzialnych.

8. Powiadomienie o naruszeniu powinno zawierać w szczególności:

a) czas i miejsce naruszenia,

b) kategorie danych oraz przybliżoną liczbę osób, których dotyczy naruszenie,

c) opis naruszenia,

d) możliwe konsekwencje naruszenia,

e) informacje o ewentualnym podjęciu środków zaradczych.

9. Wystąpienie każdego naruszenia powinno zostać w odpowiedni sposób udokumentowane. Z prowadzonego postępowania sprawdzającego Administrator Danych (lub inna osoba odpowiedzialna lub upoważniona przez Administratora) powinien sporządzić Raport. Wzór Raportu z naruszenia stanowi **załącznik nr 1.**

10. Niezależnie od tego, czy dane naruszenie zostanie zgłoszone do organu nadzorczego (Prezesa Urzędu Ochrony Danych Osobowych), fakt jego zaistnienia powinien zostać również odnotowany w Rejestrze incydentów/naruszeń, stanowiącym **załącznik nr 2.**

11. Organem właściwym do zgłaszania naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO). Zgłoszenia można dokonać na 4 sposoby:

1) Elektronicznie poprzez wypełnienie **dedykowanego formularza elektronicznego** dostępnego pod adresem: https://www.biznes.gov.pl/pl/opisy-procedur/-/proc/889.

2) Elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP:**/UODO/SkrytkaESP.**

3) Elektronicznie poprzez wysłanie wypełnionego formularza, za pomocą **pisma ogólnego dostępnego na platformie biznes.gov.pl** (Jak znaleźć Urząd w formularzu pisma ogólnego?)lub **platformie epuap.gov.pl**.

4) **Tradycyjną pocztą** wysyłając wypełniony formularz na adres Urzędu.

Załącznik nr 1

RAPORT Z NARUSZENIA
W FUNDACJI WIDZEWA Z SIEDZIBĄ W ŁODZI
AL. MARSZAŁKA JÓZEFA PIŁSUDSKIEGO 138, 92-230 ŁÓDŹ

1. Data:……. Godzina:…….....

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

……...
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika - jeśli występuje)

3. Lokalizacja zdarzenia: …….
(nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa danych osobowych oraz okoliczności towarzyszące:

……..……
……..……
……..……

5. Potencjalne przyczyny wystąpienia zdarzenia:

……..……
……..……
……..……

6. Podjęte działania:

……..……
……..……
……..……

7. Postępowanie wyjaśniające:

……..……
……..……
……..……

……
(data, podpis Administratora Danych)

Załącznik nr 2 FUNDACJA WIDZEWA Z SIEDZIBĄ W ŁODZI AL. MARSZAŁKA JÓZEFA PIŁSUDSKIEGO 138 92-230 ŁÓDŹ	**Formularz rejestracji incydentu**		

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH ORAZ INCYDENTÓW BEZPIECZEŃSTWA

Opis/okoliczności naruszenia/incydentu	Ilość osób dotknięta naruszeniem/ incydentem	Skutki naruszenia/ incydentu	Działania zaradcze	Data rozpoczęcia wdrożenia działań	Data zakończenia wdrażania działań	Stopień ryzyka naruszenia (niski, średni, wysoki)	Osoba odpowiedzialna za wdrożenie działań

FUNDACJA
WIDZEWA