INSTRUKCJA POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA INCYDENTU ZWIĄZANEGO Z NARUSZENIEM ZASAD OCHRONY DANYCH OSOBOWYCH

W przypadku stwierdzenia wystąpienia incydentu związanego z naruszeniem zasad ochrony danych osobowych Użytkownik niezwłocznie informuje Administratora Danych Osobowych lub osoby przez niego upoważnione albo Inspektora Ochrony Danych Osobowych (jeśli został powołany) o naruszeniu lub o podejrzeniu naruszenia, a w rezultacie o konieczności przeprowadzenia sprawdzenia doraźnego.

Typowe sytuacje, o których użytkownik powinien powiadomić Inspektora Ochrony Danych (jeśli został powołany) lub Administratora albo osoby przez niego upoważnione, to w szczególności:

a) Ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
b) Zniszczenie dokumentacji zawierającej dane osobowe bez użycia niszczarki,
c) Fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
d) Otwarte drzwi do pomieszczeń, szaf, w których przechowywane są dane osobowe,
e) Ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
f) Przerwa w dostawie prądu lub atak typu blokada usług, w wyniku których administrator tymczasowo lub trwale traci dostęp do danych osobowych.
g) Wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz firmy bez upoważnienia inspektora ochrony danych lub administratora danych osobowych,
h) Udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
i) Telefoniczne próby wyłudzenia danych osobowych,
j) Kradzież komputerów lub cd, twardych dysków, pendrive'a z danymi osobowymi,
k) E-maile zachęcające do ujawnienia identyfikatora i/lub hasła,
l) Pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
m) Przechowywanie haseł do systemów w pobliżu komputera.

W ramach czynności sprawdzających Administrator Danych Osobowych lub osoba przez niego upoważniona wykonuje następujące działania:

1. Określa sposób udokumentowania sprawdzenia, a w jego ramach:

a) sporządza **notatki z czynności sprawdzających,** w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;

b) odbiera **pisemne wyjaśnienia** od osób, których czynności objęto sprawdzeniem;

c) sporządza **kopie** okazanych dokumentów;

d) sporządza **kopie obrazów** wyświetlonych na ekranach urządzeń stanowiących część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;

e) sporządza **kopie zapisów** rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

2. Podejmuje **działania** mające za zadanie **zabezpieczenie** dowodów związanych z incydentem;
3. Ustala **przyczyny** oraz osoby odpowiedzialne za powstanie incydentu;
4. Podejmuje działania mające na celu **przywrócenie** stanu zgodnego z prawem;
5. Przygotowuje zgłoszenie zawierające **elementy określone w art. 33 ust. 3 RODO;**
6. **Zgłasza naruszenie do Prezesa Urzędu Ochrony Danych Osobowych**, bez zbędnej zwłoki, a w miarę możliwości nie później niż w terminie **72 godzin** po stwierdzeniu naruszenia, chyba że jest mało prawdopodobne, aby naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Wypełnij w tym celu: Wzór zgłoszenia incydentu naruszenia danych osobowych do organu nadzorczego

7. W przypadku zgłoszenia dokonanego po upływie **72 godzin** od chwili naruszenia, dołącza wyjaśnienie przyczyn opóźnienia. Zgodnie z art. 33 ust. 4 RODO, Administrator może udzielać informacji sukcesywnie.
8. Zawiadamia osoby, których dane dotyczą, o naruszeniu ochrony danych osobowych – jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, i jest to wymagane zgodnie z art. 34 RODO, na przykład:
   a) sytuacje, w których naruszenie prowadzi do dyskryminacji,
   b) kradzieży tożsamości,
   c) oszustwa,
   d) straty finansowej
   e) uszczerbku na reputacji.
   f) jeżeli naruszenie dotyczy danych wrażliwych.

……..

[data wprowadzenia procedury i podpis Administratora]