Załącznik do zarządzenia Rektora nr 6/2020 z dn. 13.01.2020

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Procedura Zarządzania Naruszeniami w Państwowej Wyższej Szkole Zawodowej w Głogowie jest zgodna z:

1. Rozporządzeniem 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 (w skrócie RODO);
2. Wytycznymi Grupy Roboczej (GDPR) ds. Ochrony danych 29 18/EN WP 250 rev.01 „dotyczące zgłaszania naruszenia ochrony danych" w rozumieniu rozporządzenia 2016/679.
3. Zarządzeniem Rektora nr 15/2018 z dnia 25 maja 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji Państwowej Wyższej Szkoły Zawodowej w Głogowie (z późn. zm.)

POSTANOWIENIA OGÓLNE

§1.

Instrukcja niniejsza określa tryb i zasady postępowania osób zatrudnionych przy przetwarzaniu danych osobowych, w przypadku, gdy:

- stwierdzono naruszenie zabezpieczenia systemu informatycznego,
- stan urządzenia, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej, mogą wskazywać na naruszenie zabezpieczeń danych.

NARUSZENIA OCHRONY DANYCH OSOBOWYCH - DEFINICJE

§2.

1. Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.
2. Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:
   1) naruszenie lub próbę naruszenia integralności systemu oraz zbioru danych,
   2) nieuprawniony dostęp lub próbę dostępu do systemu lub pomieszczeń (widoczne uszkodzenia bądź naruszenia zabezpieczeń),
   3) nieautoryzowane zniszczenie lub próbę zniszczenia danych zgromadzonych w systemie,
   4) zmianę lub utratę danych zapisanych na kopiach zapasowych lub archiwalnych dokonaną w sposób nieautoryzowany,

5) nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
6) inny stan systemu lub pomieszczeń (ślady na drzwiach, oknach i szafach wskazujące np. na włamanie) niż pozostawiony przez użytkownika po zakończeniu lub po przerwie w pracy z systemem,
7) podejrzenie o wycieku danych osobowych (np., udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej, wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz Uczelni bez upoważnienia, itp.),
8) zagubienie, w szczególności zgubienie lub kradzież nośnika z danymi: np. pendrive, płyta CD, dysk, dokumenty) lub nieautoryzowane/nieplanowane usunięcie danych osobowych,
9) otrzymanie zgłoszenia, od osoby której dane dotyczą o niewłaściwym wykorzystaniu jej danych,
10) podejrzenie, że do systemów lub pomieszczeń, gdzie są przetwarzane dane osobowe miały dostęp osoby nieuprawnione.

3. Naruszenia dotyczą danych osobowych przetwarzanych w formie elektronicznej oraz papierowej.

DZIAŁANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

§3.

1. Każdy pracownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie zgłosić to:
   - swojemu bezpośredniemu przełożonemu, który przekazuje informację Inspektorowi Ochrony Danych,
   - bezpośrednio Inspektorowi Ochrony Danych.
2. Administrator Systemu Informatycznego jest zobowiązany do informowania Inspektora Ochrony Danych o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

§4.

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 Inspektora Ochrony Danych lub innej osoby upoważnionej przez Administratora Danych.

§5.

Do czasu przybycia Inspektora Ochrony Danych lub osoby upoważnionej przez administratora danych, pracownik:

1) zabezpiecza dostęp do miejsca lub urządzenia,
2) wstrzymuje pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, które w związku z naruszeniem ochrony zostały wstrzymane,

3) podejmuje, stosownie do zaistniałej sytuacji inne, niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych

§6.

1. Inspektor Ochrony Danych po otrzymaniu zgłoszenia o naruszeniu:
   1) ocenia zaistniałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe, stan urządzeń i zbioru danych,
   2) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia systemu (odłączenie urządzeń, odłączenie wadliwych urządzeń, zmiana haseł, blokowanie dostępu do sieci telekomunikacyjnej, programów oraz zbiorów danych),
   3) zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia, jak również sprawdza zawartość zbioru danych osobowych,
   4) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
   5) sprawdza sposób działania programu (w tym również obecność wirusów komputerowych);
   6) ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu,
   7) niezwłocznie zapewnia przywrócenie prawidłowego stanu działania systemu, a w przypadku uszkodzenia danych, odtwarza je z ostatnich kopii awaryjnych z zachowaniem należytych środków ostrożności,
   8) sprawdza jakość komunikacji w systemie informatycznym,
   9) dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych wskutek naruszenia oraz poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych,
   10) spisuje relację osoby zatrudnionej przy przetwarzaniu danych, która dokonała powiadomienia,
   11) podejmuje decyzję o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych i w przypadkach uzasadnionych niezwłocznie powiadamia właściwą osobę podejmującą decyzję w imieniu administratora danych,
   12) dokumentuje wszystkie czynności związane z naruszeniem w ***Rejestrze naruszeń***,
   13) sporządza raport zawierający w szczególności: dane personalne osoby, która stwierdziła naruszenie, datę i godzinę powiadomienia, opis podjętych czynności i ich uzasadnienie ***Załącznik nr 1***.,
   14) podejmuje czynności mające na celu minimalizację szkody.

§7.

1. Inspektor Ochrony Danych po identyfikacji problemu dokonuje klasyfikacji naruszenia. Naruszenie klasyfikowane jest jako:
   1) nieskutkujące ryzykiem naruszenia praw lub wolności osób fizycznych,
   2) skutkujące ryzykiem naruszenia praw lub wolności osób fizycznych.

2. Naruszenie kwalifikuje się jako naruszenie ochrony danych podlegające zgłoszeniu w ciągu 72h do Prezesa Urzędu Ochrony Danych Osobowych jeżeli konsekwencją naruszenia jest np. utrata kontroli nad danymi osobowymi lub ograniczenie praw osób, których dane dotyczą, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.
3. Jeżeli naruszenie zostanie zakwalifikowane jako skutkujące ryzykiem naruszenia praw lub wolności osób fizycznych, Inspektor Ochrony Danych:
   - uzupełnia Rejestr naruszeń,
   - przygotowuje zgłoszenie naruszenia do Prezesa Urzędu Ochrony Danych Osobowych.

ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORGANOWI NADZORCZEMU

§8.

1. Przygotowane przez Inspektora Ochrony Danych zgłoszenie naruszenia, Administrator Danych przekazuje do Prezesa Urzędu Ochrony Danych Osobowych niezwłocznie, lecz nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia.
2. Do zgłoszenia przekazanego po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

§ 9.

1. Administrator danych informuje Prezesa Urzędu Ochrony Danych Osobowych o zaistniałym naruszeniu, poprzez podanie następujących informacji:
   1) opisu charakteru naruszenia ochrony danych osobowych, w tym jeżeli to możliwe wskazania kategorii i przybliżonej liczby osób, których dane dotyczą, oraz kategorii i przybliżonej liczby wpisów danych osobowych, których dotyczy naruszenie,
   2) wskazanie punktu kontaktowego, od którego można uzyskać więcej informacji na temat naruszenia,
   3) opisu możliwych konsekwencji naruszenia ochrony danych osobowych,
   4) opisu środków zastosowanych lub proponowanych przez administratora danych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.
2. Zgłoszenia stanowi ***Załącznik nr 2*** do niniejszej Instrukcji.
3. Administrator danych w celu wyjaśnienia sprawy, w zależności od potrzeby prowadzi korespondencję z Prezesem Urzędu Ochrony Danych Osobowych udzielając wszelkich niezbędnych informacji.
4. Jeżeli naruszenie danych osobowych ma znamiona przestępstwa wówczas Administrator Danych informuje odpowiednie organy ścigania.

ZAWIADAMIANIE OSOBY, KTÓREJ DANE DOTYCZĄ, O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

§ 10.

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator Danych bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Administrator danych informuje osobę, której dane zostały naruszone o rodzaju zagrożenia, a w szczególności przedstawia opis charakteru naruszenia, podjęte działania w celu ograniczenia zagrożenia oraz wydaje zalecenia co do minimalizacji potencjalnych niekorzystnych skutków.
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
   1) Administrator Danych wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
   2) Administrator Danych zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
   3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

ŚRODKI ZARADCZE

§ 11.

W celu minimalizacji strat oraz w ramach zastosowania środków zaradczych przed następnymi naruszeniami Administrator Danych:

1) jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego - niezwłocznie zleca lub przeprowadza, w stosownym zakresie, przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe,
2) jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych – zleca lub przeprowadza dodatkowe kursy i szkolenia osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań rozważa możliwość ich ukarania w trybie przewidzianym odrębnymi przepisami.

NARUSZENIE DANYCH OSOBOWYCH - ODPOWIEDZIALNOŚĆ

§12.

1. Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe.

2. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.
3. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

Załącznik nr 1

RAPORT Z NARUSZENIA OCHRONY DANYCH

1. Data ..... Godzina .....

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem

.....

(imię, nazwisko, stanowisko służbowe,):

3. Lokalizacja zdarzenia:

.....……

(nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

.....

5. Podjęte działania:

.....

6. Wstępna ocena przyczyn wystąpienia naruszenia:

.....

7. Postępowanie wyjaśniające i naprawcze:

.....

…… ……..

(podpis pracownika) (data i podpis Inspektora Ochrony Danych)

Zgłoszenie naruszenia ochrony danych osobowych

1. Typ zgłoszenia

Wskaż czy zgłaszasz naruszenie ochrony danych osobowych mające charakter jednorazowego zdarzenia (np. zgubienie, kradzież nośnika danych, przypadkowe wysłanie danych osobie nieuprawnionej), czy przygotowujesz wstępne zgłoszenie, które uzupełnisz później, lub czy uzupełniasz lub zmieniasz wcześniejsze zgłoszenie.

Podaj swoją sygnaturę sprawy (opcjonalnie)
(np. sygnatura w Twoim wewnętrznym rejestrze naruszeń) Kliknij tutaj, aby wprowadzić tekst.

☉ Zgłoszenie kompletne/jednorazowe	○ Zgłoszenie wstępne	○ Zgłoszenie uzupełniające/zmieniające
	Podaj przybliżoną datę uzupełnienia zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę.	Podaj datę poprzedniego zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę. Podaj sygnaturę sprawy UODO Kliknij tutaj, aby wprowadzić tekst.

☐ Naruszenie zostało lub zostanie zgłoszone organowi ochrony danych osobowych w innym państwie Jeśli tak, podaj w jakim.

☐ Naruszenie zostało lub zostanie zgłoszone innym organom np. Policja, CSIRT NASK, CSIRT GOV, CSIRT MON (najedź myszką na nazwę organu by dowiedzieć się więcej)

Podaj nazwy tych organów
Kliknij tutaj, aby wprowadzić tekst.

Podaj numer/sygnaturę zgłoszenia do innego organu
Kliknij tutaj, aby wprowadzić tekst.

2. Podmiot zgłaszający

2A. Dane administratora danych

Pełna nazwa administratora Kliknij tutaj, aby wprowadzić tekst.

REGON (opcjonalnie)	Podaj numer.	NIP (opcjonalnie)	Podaj numer.	KRS (opcjonalnie)	Podaj numer.

Sektor (opcjonalnie) Dla sektora publicznego: Wybierz element. Dla sektora prywatnego: Wybierz element.

2B. Adres siedziby administratora danych

Ulica	Kliknij tutaj, aby wprowadzić tekst.	Numer domu	Podaj numer Numer lokalu Podaj numer
Miejscowość	Kliknij tutaj, aby wprowadzić tekst.	Kod pocztowy	Kliknij tutaj, aby wprowadzić tekst.
Gmina	Kliknij tutaj, aby wprowadzić tekst.	Powiat	Kliknij tutaj, aby wprowadzić tekst.
Województwo	Kliknij tutaj, aby wprowadzić tekst.	Państwo	Kliknij tutaj, aby wprowadzić tekst.

2C. Osoby uprawnione do reprezentowania administratora

1.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
2.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
3.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
4.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
5.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.

2D. Pełnomocnik

☐ Wniosek wypełniany przez pełnomocnika (opcjonalnie)

Jeśli zgłoszenie przesyłane jest w formie elektronicznej, należy załączyć pełnomocnictwo **udzielone w formie elektronicznej** oraz dowód uiszczenia opłaty skarbowej

2E. Inspektor ochrony danych

Imię i nazwisko	imię i nazwisko.	Numer telefonu	Numer telefonu.	Adres e-mail	E-mail.

☐ Inspektor nie został wyznaczony

Jeśli inspektor nie został wyznaczony podaj dane innego punktu kontaktowego, od którego można uzyskać więcej informacji o naruszeniu.

Kliknij tutaj, aby wprowadzić tekst.

2F. Inne podmioty uczestniczące w przetwarzaniu danych, których dotyczy naruszenie (opcjonalnie)

Podaj nazwy podmiotów, dane kontaktowe i wyjaśnij ich rolę w procesie przetwarzania, którego dotyczy naruszenie (np. podmiot przetwarzający, współadministratora, operator pocztowy itp.)

1.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
2.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
3.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
4.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
5.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.

3. Czas naruszenia

3A. Wykrycie naruszenia i powiadomienie organu nadzorczego

Data stwierdzenia naruszenia
Wskaż kiedy dowiedziałeś/aś się o naruszeniu.
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić datę.

Sposób stwierdzenia naruszenia
Np. zgłoszenie osoby której dane dotyczą czy cykliczny przegląd logów systemowych zgodnie z wdrożoną polityką bezpieczeństwa

Kliknij tutaj, aby wprowadzić tekst.

Data powiadomienia przez podmiot przetwarzający
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

Powody opóźnienia powiadomienia organu nadzorczego o naruszeniu
Pole obowiązkowe jeśli czas od momentu stwierdzenia naruszenia do czasu wypełniania formularza jest dłuższy niż 72h

Kliknij tutaj, aby wprowadzić tekst.

3B. Czas naruszenia

Data i czas zaistnienia/rozpoczęcia naruszenia
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

Data i czas zakończenia naruszenia
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

4. Charakter naruszenia

4A. Opisz szczegółowo na czym polegało naruszenie

Kliknij tutaj, aby wprowadzić tekst.

4B. Na czym polegało naruszenie?

☐ a) Zgubienie lub kradzież nośnika/urządzenia

☐ b) Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji

☐ c) Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy

☐ d) Nieuprawnione uzyskanie dostępu do informacji

☐ e) Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń

☐ f) Złośliwe oprogramowanie ingerujące w poufność, integralność lub dostępność danych

☐ g) Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)

☐ h) Nieprawidłowa anonimizacja danych osobowych w dokumencie

☐ i) Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora

☐ j) Niezamierzona publikacja

☐ k) Dane osobowe wysłane do niewłaściwego odbiorcy

☐ l) Ujawnienie danych niewłaściwej osoby

☐ m) Ustne ujawnienie danych osobowych

4C. Działanie złośliwego oprogramowania (odpowiedz na poniższe pytania, jeśli w sekcji 4B zaznaczono pole f)

a) Jeśli w ocenie administratora doszło wyłącznie do naruszenia dostępności danych, w jaki sposób stwierdzono, że nie doszło do naruszenia ich poufności? (w sytuacji gdy np. dane nie zostały pobrane przez osobę nieupoważnioną, a jedynie zaszyfrowane w sposób uniemożliwiający uzyskanie do nich dostępu)

Kliknij tutaj, aby wprowadzić tekst.

b) Czy, a jeżeli tak, to w jakiej formie, złośliwe oprogramowanie poinformowało o konieczności uiszczenia opłaty w celu odzyskania dostępu do danych (podaj nazwę złośliwego oprogramowania, sposób poinformowania, żądaną kwotę, kanał komunikacji, sposób zapłaty oraz termin)

Kliknij tutaj, aby wprowadzić tekst.

c) Jeżeli doszło do utraty dostępności danych, to czy administrator był w posiadaniu kopii zapasowej, jeśli tak to w jakim czasie ją przywrócił?

Kliknij tutaj, aby wprowadzić tekst.

UWAGA: *Jeżeli zgłoszenie naruszenia dotyczy podejrzanych załączników, phishingu, szantażu czy działania złośliwego oprogramowania, rozważ zgłoszenie zdarzenia do CERT Polska pod adresem https://incydent.cert.pl/. Dokonanie takiego zgłoszenia jest szczególnie zalecane w przypadku, kiedy odpowiedzi na powyższe pytania są utrudnione bądź niemożliwe.*
O fakcie zgłoszenia incydentu do CERT Polska poinformuj w zgłoszeniu uzupełniającym Prezesa UODO (pkt 1 formularza) podając datę zgłoszenia, jego numer oraz ewentualnie informacje na temat incydentu otrzymane od CERT Polska).

4D. Przyczyna naruszenia

☐ Wewnętrzne działanie niezamierzone

☐ Wewnętrzne działanie zamierzone

☐ Zewnętrzne działanie niezamierzone

☐ Zewnętrzne działanie zamierzone

4E. Charakter

☐ Naruszenie poufności danych
Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych

☐ Naruszenie integralności danych
Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania

☐ Naruszenie dostępności danych
Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną

4F. Dzieci

☐ Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.
(opcjonalnie)

5. Liczba osób i wpisów

Przybliżona liczba osób, których dotyczy naruszenie

Kliknij tutaj, aby wprowadzić tekst.

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie
Nie dotyczy to liczby osób. Jednej osobie można przypisać kilka wpisów (np. jednej osobie można przypisać kilka wykonanych transakcji)

Kliknij tutaj, aby wprowadzić tekst.

6. Kategorie danych osobowych

UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

6A. Dane podstawowe

- ☐ Nazwiska i imiona
- ☐ Imiona rodziców
- ☐ Data urodzenia
- ☐ Numer rachunku bankowego
- ☐ Adres zamieszkania lub pobytu
- ☐ Numer ewidencyjny PESEL
- ☐ Adres e-mail
- ☐ Nazwa użytkownika i/lub hasło
- ☐ Dane dotyczące zarobków i/lub posiadanego majątku
- ☐ Nazwisko rodowe matki
- ☐ Seria i numer dowodu osobistego
- ☐ Numer telefonu
- ☐ Wizerunek
- ☐ Inne, wskaż jakie:

Kliknij tutaj, aby wprowadzić tekst.

6B. Dane szczególnej kategorii

- ☐ Dane o pochodzeniu rasowym lub etnicznym
- ☐ Dane o poglądach politycznych
- ☐ Dane o przekonaniach religijnych lub światopoglądowych
- ☐ Dane o przynależności do związków zawodowych
- ☐ Dane dotyczące seksualności lub orientacji seksualnej
- ☐ Dane dotyczące zdrowia
- ☐ Dane genetyczne
- ☐ Dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej

6C. Dane, o których mowa w art. 10 RODO

- ☐ Dane dotyczące wyroków skazujących
- ☐ Dane dotyczące czynów zabronionych
- ☐ Inne

Kliknij tutaj, aby wprowadzić tekst.

7. Kategorie osób

- ☐ Pracownicy
- ☐ Użytkownicy
- ☐ Subskrybenci
- ☐ Studenci
- ☐ Uczniowie
- ☐ Służby mundurowe (np. wojsko, policja)
- ☐ Klienci (obecni i potencjalni)
- ☐ Klienci podmiotów publicznych
- ☐ Pacjenci
- ☐ Dzieci
- ☐ Osoby o szczególnych potrzebach (np. osoby starsze, niepełnosprawne itp.)

Szczegółowy opis kategorii osób, których dotyczy naruszenie:
Opisz np. kogo i w jakim przedziale czasowym dotyczy naruszenie
W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

Kliknij tutaj, aby wprowadzić tekst.

8. Możliwe konsekwencje

8A. Uszczerbek fizyczny, majątkowy, niemajątkowy lub inne znaczące konsekwencje dla osoby, której dane dotyczą

- ☐ Utrata kontroli nad własnymi danymi osobowymi
- ☐ Ograniczenie możliwości realizowania praw z art. 15-22 RODO
- ☐ Ograniczenie możliwości realizowania praw
- ☐ Dyskryminacja
- ☐ Kradzież lub sfałszowanie tożsamości
- ☐ Strata finansowa
- ☐ Naruszenie dobrego imienia
- ☐ Utrata poufności danych osobowych chronionych tajemnicą zawodową
- ☐ Nieuprawnione odwrócenie pseudonimizacji
- ☐ Inne

Opisz poniżej inne skutki naruszenia prawa do ochrony danych osoby, której dane dotyczą:

Kliknij tutaj, aby wprowadzić tekst.

8B. Czy wystąpiło wysokie ryzyko naruszenia praw lub wolności osób fizycznych?

- ◉ Tak
- ○ Nie

Uzasadnienie

Kliknij tutaj, aby wprowadzić tekst.

9. Środki bezpieczeństwa i środki zaradcze

9A. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa dotychczas stosowanych

Kliknij tutaj, aby wprowadzić tekst.

9B. Środki bezpieczeństwa zastosowane lub proponowane w celu zminimalizowana ryzyka ponownego wystąpienia naruszenia

Kliknij tutaj, aby wprowadzić tekst.

9C. Środki zastosowane lub proponowane w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

10. Czy osoby, których dane dotyczą, zostały zawiadomione o naruszeniu?

◉ Tak	○ Nie, ale zostaną zawiadomione Pamiętaj, że po powiadomieniu osób, należy przesłać treść zawiadomienia do UODO.	○ Nie, nie zostaną zawiadomione, ponieważ:	○ Nie oceniłem jeszcze

Czy indywidualnie?

◉ Tak

○ Nie, gdyż indywidualne zawiadomienie każdej osoby, której dane dotyczą wymagałoby niewspółmiernie dużego wysiłku. W związku z tym został bądź zostanie wydany publiczny komunikat lub zastosowany podobny środek, za pomocą którego osoby, których dane dotyczą, zostały bądź zostaną poinformowane w równie skuteczny sposób.

Wskaż datę zawiadomienia
Kliknij tutaj, aby wprowadzić datę.

Wskaż datę planowanego zawiadomienia
Kliknij tutaj, aby wprowadzić datę.

☐ Nie znam jeszcze daty kiedy zamierzam zawiadomić osoby, których dane dotyczą

Liczba zawiadomionych osób
Kliknij tutaj, aby wprowadzić tekst.

Środki komunikacji wykorzystane do zawiadomienia osoby, której dane dotyczą
Kliknij tutaj, aby wprowadzić tekst.

Umieść zanonimizowaną treść zawiadomienia, którą przesłałeś bądź zamierzasz przesłać do osób, których dane dotyczą.

Pamiętaj, że zawiadomienie powinno:

- opisywać jasnym i prostym językiem charakter naruszenia ochrony danych osobowych,
- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Kliknij tutaj, aby wprowadzić tekst.

○ przed naruszeniem wdrożono odpowiednie techniczne i organizacyjne środki ochrony (wskazane w pkt. 9A formularza) i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, anonimizacja czy pseudonimizacja uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.

○ po naruszeniu zastosowano środki (wskazane w pkt. 9C formularza) eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.

○ stwierdzono brak wysokiego ryzyka naruszenia praw lub wolności osób fizycznych (uzasadnienie w pkt. 8B formularza).

Jeśli jeszcze nie oceniłeś, czy zamierzasz zawiadomić osoby, których dane dotyczą, pamiętaj, że po podjęciu takiej decyzji będziesz musiał złożyć zgłoszenie uzupełniające.

11. Przetwarzanie transgraniczne

☐ Naruszenie ma charakter transgraniczny

Zaznacz kraje Europejskiego Obszaru Gospodarczego, których dotyczy naruszenie:

☐ Austria	☐ Belgia	☐ Bułgaria	☐ Chorwacja
☐ Cypr	☐ Czechy	☐ Dania	☐ Estonia
☐ Finlandia	☐ Francja	☐ Grecja	☐ Hiszpania
☐ Holandia	☐ Irlandia	☐ Islandia	☐ Liechtenstein
☐ Litwa	☐ Luksemburg	☐ Łotwa	☐ Malta
☐ Niemcy	☐ Norwegia	☐ Portugalia	☐ Rumunia
☐ Słowacja	☐ Słowenia	☐ Szwecja	☐ Węgry

☐ Wielka Brytania ☐ Włochy

_____
Data, miejscowość
(dla zgłoszenia w formie papierowej)

_____
Podpis osoby lub osób upoważnionych
do reprezentowania administratora
(dla zgłoszenia w formie papierowej

Informacja:

Administrator danych osobowych.
Administratorem Państwa danych osobowych będzie Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) z siedzibą w Warszawie, przy ul. Stawki 2.
Można się z nami kontaktować w następujący sposób:
a) listownie: ul. Stawki 2, 00-193 Warszawa
b) przez elektroniczną skrzynkę podawczą dostępną na stronie https://www.uodo.gov.pl/pl/p/kontakt
c) telefonicznie: (22) 531 03 00

Inspektor ochrony danych.
Możecie się Państwo kontaktować również z wyznaczonym przez Prezesa UODO inspektorem ochrony danych pod adresem email IOD@uodo.gov.pl

Cele i podstawy przetwarzania.
Będziemy przetwarzać Państwa dane osobowe zawarte w formularzu w celu przyjmowania zgłoszeń o naruszeniu ochrony danych osobowych zgodnie z art. 33 ust 1 , 3 i 4 RODO[1] bądź art. 44 ust. 1 – 5 DODO[2], podejmowania działań określonych w art. 34 ust. 4 oraz art. 58 ust. 2 RODO bądź art. 45 ust. 5 DODO, a także prowadzenia przez organ wewnętrznego rejestru naruszeń na podstawie art. 57 ust. 1 lit. u RODO. Następnie Państwa dane będziemy przetwarzać w celu wypełnienia obowiązku archiwizacji dokumentów wynikającego z ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

Odbiorcy danych osobowych.
Odbiorcami Państwa danych osobowych będą Minister Cyfryzacji w związku z zamieszczeniem formularza na platformie E-PUAP bądź Minister Przedsiębiorczości i Technologii w związku z zamieszczeniem formularza na platformie biznes.gov.pl

Okres przechowywania danych.
Będziemy przechowywać Państwa dane przez czas realizacji uprawnień Prezesa UODO wskazanych w art. 34 ust. 4 RODO i art. 58 ust. 2 RODO bądź art. 45 ust. 5 DODO, a następnie - zgodnie z obowiązującą w Urzędzie Prezesa UODO Instrukcją kancelaryjną oraz przepisami o archiwizacji dokumentów - przez okres 10 lat od końca roku, w którym zgłoszono naruszenie ochrony danych, lub - w przypadku skierowania wystąpienia lub wydania decyzji administracyjnej – wieczyście.

Prawa osób, których dane dotyczą.
Zgodnie z RODO przysługuje Państwu:
a) prawo dostępu do swoich danych oraz otrzymania ich kopii;
b) prawo do sprostowania (poprawiania) swoich danych;
c) prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej;
d) prawo do ograniczenia przetwarzania danych;
e) prawo do wniesienia skargi do Prezesa UODO (na adres Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa)

Informacja o wymogu podania danych.
Podanie przez Państwa danych osobowych w niniejszym formularzu jest obowiązkiem wynikającym z art. 33 ust. 3 RODO oraz z art. 63 § 2-3a ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego.

[1] 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 (RODO) oraz podjętych działań.
[2] Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości