Zarządzenie Nr 104/2019
Starosty Powiatu Ropczycko – Sędziszowskiego
w Ropczycach z dnia 1 października 2019r.

w sprawie:

wprowadzenia „Instrukcji postępowania w przypadku naruszenia ochrony danych osobowych" w Starostwie Powiatowym w Ropczycach"

Na podstawie art. 34 ust. 1 i art. 35 ust. 2 ustawy z dnia 5 czerwca 1998r. o samorządzie powiatowym (tj. Dz. U. z 2019 r., poz. 511), w związku z art. 24 ust. 2 Rozporządzenia 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 (Dz. Urz. UE L 119, s. 1)

zarządzam co następuje;

§ 1. Wprowadzam „Instrukcję postępowania w przypadku naruszenia ochrony danych osobowych" w Starostwie Powiatowym w Ropczycach", która stanowi ***załącznik nr 1*** do niniejszego zarządzenia.

§ 2. Zobowiązuje się dyrektorów wydziałów, kierowników referatów i osoby na samodzielnych stanowiskach pracy do zapoznania się oraz zapoznania podległych im pracowników z unormowaniami Instrukcji, jej wdrożenia oraz bieżącego nadzoru nad jej przestrzeganiem.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
Witold Bartak

ADWOKAT
mgr Józef Gudyka

INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

§ 1.
CEL INSTRUKCJI

1.Instrukcja postępowania w przypadku naruszenia ochrony danych jest dokumentem opracowanym i wdrożonym w Starostwie Powiatowym w celu zapewnienia przestrzegania zasad ochrony danych osób fizycznych, w szczególności ochrony ich praw i wolności. Instrukcja przeznaczona jest dla wszystkich pracowników i współpracowników Administratora Danych Osobowych (dalej: ADO) i określa tryb postępowania w przypadku, gdy:

1) stwierdzono naruszenie lub istnieje podejrzenie naruszenia ochrony danych osobowych, zgromadzonych w systemach informatycznych lub na innych nośnikach informacji, w tym dokumentach papierowych,

2) stan urządzenia, zawartość zbioru danych osobowych; ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenia zasad ochrony danych.

2.Celem niniejszej instrukcji jest określenie zadań pracowników w zakresie:

1) ochrony danych osobowych przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą oraz wykorzystywaniem danych osobowych w celach niezgodnych z tym, dla którego zostały zgromadzone;

2) prawidłowego reagowania pracowników zatrudnionych przy przetwarzaniu danych osobowych w przypadku stwierdzenia naruszenia ochrony danych osobowych lub zabezpieczeń systemu informatycznego;

3) ograniczenia ryzyka powstania zagrożeń oraz minimalizacja skutków wystąpienia zagrożeń.

§ 2.
DEFINICJE

1. **NARUSZENIE OCHRONY DANYCH** - 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;

2. **BEZPIECZEŃSTWO PRZETWARZANIA** – zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania oraz zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

3. **ZDARZENIU ZWIĄZANYM Z BEZPIECZEŃSTWEM INFORMACJI** – zdarzenie związane z bezpieczeństwem informacji, jako określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem;

4. **INCYDENCIE ZWIĄZANYM Z BEZPIECZEŃSTWEM INFORMACJI** – jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne zakłócenia w realizacji zadań i zagrażają bezpieczeństwu informacji;

5. ZAGROŻENIACH SYSTEMU – to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę;

6. NARUSZENIE DOSTĘPNOŚCI - polega na trwałej utracie lub zniszczeniu danych osobowych;

7. NARUSZENIE POUFNOŚCI - to niedozwolone lub przypadkowe ujawnienie lub dostęp do danych osobowych;

8. NARUSZENIE INTEGRALNOŚCI - to niedozwolona lub przypadkowa zmiana danych osobowych;

9. ROZLICZALNOŚĆ - to cecha zapewniająca działanie podmiotu przetwarzającego dane osobowe, która może być przypisana w sposób jednoznaczny tylko temu, jednemu podmiotowi;

10. DZIAŁANIA KORYGUJĄCE -- jest to działanie przeprowadzone w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji;

11.DZIAŁANIA ZAPOBIEGAWCZE– jest to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej;

12. ZNISZCZENIE - danych osobowych oznacza sytuację, w której dane przestają istnieć lub przestają istnieć w formie umożliwiającej ich wykorzystanie przez ADO;

13. USZKODZENIE - oznacza sytuację, w której dane osobowe zostały zmodyfikowane, zepsute lub nie są już kompletne;

14. UTRATĘ - danych osobowych należy rozumieć jako sytuację, w której dane mogą nadal istnieć, ale ADO utracił kontrolę nad nimi lub dostęp do nich, lub nie jest już w ich posiadaniu;

15. NIEUPRAWNIONE UJAWNIENIE - lub nieuprawniony dostęp do danych osobowych może obejmować ujawnienie danych osobowych (lub udostępnienia ich) odbiorcom, którzy nie są uprawnieni do otrzymania ich (lub uzyskania do nich dostępu), lub jakąkolwiek inną formę przetwarzania, która narusza przepisy z zakresu ochrony danych osobowych, a zwłaszcza RODO.

16. RODO – Rozporządzenie 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).

§ 3.
ISTOTA NARUSZENIA DANYCH OSOBOWYCH

1. Naruszenie systemu ochrony danych osobowych może zostać stwierdzone w przypadku gdy:

1) stwierdzono naruszenie zabezpieczeń danych osobowych;

2) w przypadku danych przetwarzanych w formie tradycyjnej stan pomieszczeń, szaf, okien, drzwi, dokumentów lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych;

3) w przypadku danych przetwarzanych w formie elektronicznej stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu, jakość komunikacji lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.

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:

- nieautoryzowany dostęp do danych;
- nieautoryzowane modyfikacje lub zniszczenie danych;
- udostępnienie lub umożliwienie dostępu do danych osobowych osobom lub podmiotom do tego nieupoważnionym;
- nielegalne ujawnienie danych;
- pozyskiwanie danych z nielegalnych źródeł.

3.Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.

4.Do typowych incydentów bezpieczeństwa danych osobowych należą:

1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);

2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych);

3) 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. Żeby zaistniało naruszenie, muszą być spełnione łącznie trzy przesłanki:

1) naruszenie **musi dotyczyć danych** osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez podmiot, którego dotyczy naruszenie;

2)skutkiem naruszenia **może być** zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych;

3) naruszenie **jest skutkiem złamania zasad bezpieczeństwa** danych.

§ 4.
SPOSÓB REAGOWANIA NA NARUSZENIA DANYCH OSOBOWYCH

1. Każdy (w tym podmiot przetwarzający), kto stwierdzi lub podejrzewa, że określone zdarzenie należy zakwalifikować jako zdarzenie, które może prowadzić do naruszenia ochrony danych osobowych, a w konsekwencji do naruszenia praw i wolności osób, których dane dotyczą, zawiadamia o tym niezwłocznie Administratora Danych Osobowych i Inspektora Ochrony Danych (dalej: IOD) lub bezpośrednio IOD w celu umożliwienia mu podjęcia czynności w ramach postępowania wyjaśniającego.

2. Każdy pracownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony danych osobowych oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia, a przede wszystkim:

1) powstrzymać się od rozpoczęcia lub kontynuowania jakiejkolwiek czynności lub pracy mogącej spowodować zatarcie śladów bądź dowodów naruszenia;

2) podjąć, stosownie do zaistniałej sytuacji, niezbędne działania celem zapobiegnięcia dalszym zagrożeniom, które mogą skutkować naruszeniem danych osobowych;

3) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia IOD lub innej osoby upoważnionej przez Administratora Danych Osobowych.

3. W przypadku, gdy incydent dotyczy przetwarzania danych w systemie informatycznym konieczne jest dodatkowo poinformowanie o powyższym Administratora Systemu Informatycznego (dalej jako: ASI) lub osobę odpowiedzialną za system IT.

4.Zgłoszenie incydentu odbywa się poprzez przekazanie informacji w postaci formularza zgłoszeniowego, którego wzór stanowi ***załącznik nr 1*** do niniejszej instrukcji. Po potwierdzeniu wystąpienia incydentu naruszenia bezpieczeństwa informacji ADO/IOD, określa priorytet ważności incydentu i czas na jego usunięcie.

5.IOD prowadzi rejestr naruszeń ochrony danych osobowych, zgodnie z art. 34 RODO według wzoru, który stanowi ***załącznik nr 2*** do niniejszej instrukcji. W ewidencji powinny zatem znaleźć się zarówno naruszenia ochrony danych osobowych podlegające obowiązkowi notyfikacyjnemu Prezesowi UODO, jak i te, które nie podlegają zgłoszeniu organowi nadzorczemu ze względu na to, że mało prawdopodobne jest, by skutkowały one ryzykiem naruszenia praw lub wolności osób fizycznych.

6.Jakiekolwiek próby powstrzymania pracownika przed zgłoszeniem podejrzenia zagrożenia lub naruszenia bezpieczeństwa przetwarzania danych osobowych są zabronione.

7.Administrator Systemu Informatycznego jest zobowiązany do informowania ADO/IOD o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

2.W celu przygotowania systemu informatycznego do wykrywania incydentów bezpieczeństwa informacji stosuje się:

a) okresowe przeglądy logów z systemów operacyjnych, urządzeń sieciowych i aplikacji;

b) incydenty mogą być sygnalizowane przez alerty z systemów zabezpieczeń (firewall, IPS, antywirus itp.);

c) komunikaty z systemu zarządzania zdarzeniami;

d) raporty o nieprawidłowościach, weryfikacji integralności plików;

e) logi z systemów operacyjnych, urządzeń sieciowych i aplikacji;

f) obserwacje i oceny dokonywane przez personel jednostki.

§ 5.
DOKUMENTOWANIE OKOLICZNOŚCI NARUSZENIA

1.IOD, a także ASI, do którego wpłynęło zgłoszenie w postaci formularza, o którym mowa w § 4 ust. 4 podejmuje:

1) działania interwencyjne i zabezpieczające;

2) uruchamia zespół szybkiego reagowania (dalej jako Zespół), w skład którego wchodzi IOD oraz osoby wyznaczone przez ADO w tym, w szczególności dyrektor wydziału w którym doszło do zdarzenia oraz jeśli to konieczne ASI lub osoba odpowiedzialna za system IT, w celu analizy zdarzenia i ustalenie:

a) czy doszło do naruszenia ochrony danych osobowych;

b) czy zachodzi konieczność zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu, zgodnie z art. 33 RODO;

c) czy zachodzi konieczność zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, zgodnie z art. 34 RODO;

2.W toku prowadzonych czynności IOD, ASI lub inna osoba prowadząca postępowanie pod nadzorem IOD uprawniona jest do podejmowania wszelkich działań mogących służyć wyjaśnieniu sytuacji, w tym wstępu do wszelkich pomieszczeń i dostępu do wszelkich danych, systemów, raportów i innych dokumentów mogących mieć wpływ na wyjaśnienie okoliczności zdarzenia.

3. IOD w toku prowadzonego postępowanie wyjaśniającego:

1) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki;

2) działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu;

3) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia;

4) dokumentuje okoliczności naruszenia.

4.Osoby uczestniczące w postępowaniu zobowiązane są do pełnej współpracy z Zespołem prowadzącym postępowanie wyjaśniające. Brak udokumentowania naruszenia we właściwy sposób może prowadzić do wykonania przez organ nadzorczy uprawnień na mocy art. 58 RODO lub nałożenia administracyjnej kary pieniężnej zgodnie z art. 83 RODO.

5. Jeśli doszło do naruszenia danych osobowych, IOD:

1) oznacza w rejestrze dane zdarzenie jako naruszenie;

2) powiadamia o wynikach analizy, o której mowa w ust. 3 niniejszego paragrafu Administratora Danych Osobowych oraz osobę odpowiedzialną za system IT, jeśli naruszenie dotyczy zagadnień z obszaru informatycznego;

3) jeśli zachodzi przesłanka wskazana w niniejszym paragrafie w ust. 1 pkt. 2 lit. b przygotowuje wraz z Zespołem stosowne zgłoszenie do Prezesa Urzędu Ochrony Danych Osobowych;

4) jeśli zachodzi przesłanka wskazana w niniejszym paragrafie w ust. 1 pkt. 2 lit. c przygotowuje wraz Zespołem zawiadomienie osoby, której dane dotyczą.

6.Wytworzoną dokumentację IOD przedkłada Staroście Powiatu niezwłocznie, w terminie umożliwiającym dochowanie przez ADO terminów, o których mowa w § 6 ust. 1 wraz z rekomendacją dalszego trybu postępowania.

7. Procedura postępowania w przypadku naruszenia przedstawiona w wersji graficznej stanowi ***załącznik nr 3*** do niniejszej instrukcji.

§ 6.
ZGŁASZANIE NARUSZENIA OCHRONY DANYCH ORGANOWI NADZORCZEMU

1. W przypadku stwierdzenia w toku prowadzonych czynności wyjaśniających wystąpienia naruszenia ochrony danych osobowych podlegającego notyfikacji do organu nadzorczego tj. Prezesa Urzędu Ochrony Danych, zgodnie z art. 33 RODO, po otrzymaniu stosowanej informacji od IOD, ADO - bez zbędnej zwłoki - w miarę możliwości nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że mało

prawdopodobne jest, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

2. Zgłoszenia ADO dokonuje z wykorzystaniem formularza zgłoszenia naruszenia ochrony danych osobowych do organu nadzorczego dostępnego na platformie biznes.gov.pl, którego wzór stanowi ***załącznik nr 4*** do niniejszej instrukcji.

3. Do zgłoszenia przekazanego Prezesowi Urzędu Ochrony Danych Osobowych po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

4. Jeżeli naruszenie ochrony danych osobowych stwierdzone zostanie przez IOD w trakcie prowadzonych przez niego czynności monitorujących stosowanie przepisów prawa w zakresie ochrony danych osobowych, tryb podstępowania w zakresie dokumentacji, informowania ADO oraz notyfikacji naruszeń jest analogiczny jak opisany w § 5.

5. W przypadku konieczności zgłoszenia naruszenia organowi nadzorczemu, zgłoszenie zgodnie ze wzorem, o którym mowa w ust. 2 niniejszego paragrafu musi co najmniej:

1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

2) zawierać imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych. Opis możliwych konsekwencji powinien odzwierciedlać ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić jej podjęcie niezbędnych działań zapobiegawczych.

4) opisywać środki zastosowane lub proponowane przez Administratora Danych Osobowych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

6. W przypadku, gdy w momencie zgłoszenia naruszenia ochrony danych osobowych nie da się udzielić organowi nadzorczemu wszystkich informacji Administrator Danych Osobowych , w tym zakresie, udziela je sukcesywnie bez zbędnej zwłoki.

7.Dokumentacja dotycząca naruszeń ochrony danych prowadzona przez ADO i musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania zasad zgłaszania naruszeń wynikających z RODO. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

8.Po przywróceniu normalnego stanu, Zespół przeprowadza szczegółową analizę zdarzenia, w celu określenia przedsięwzięcia kroków mających na celu wyeliminowanie podobnych zdarzeń w przyszłości. Jeżeli przyczyną zdarzenia był błąd osoby, należy przeprowadzić dodatkowe szkolenie; w przypadku świadomego działania lub zaniedbania, należy wyciągnąć konsekwencje wynikające z obowiązujących w Starostwie Powiatowym w Ropczycach polityk, regulaminów i instrukcji oraz przepisów prawa powszechnego.

9. Wyniki analizy przekazywane są Staroście Powiatu Ropczycko – Sędziszowskiego. Po wyjaśnieniu wszelkich okoliczności zdarzenia ADO podejmuje decyzje jakie środki zapobiegawcze wprowadzić i ewentualnie o wszczęciu postępowania lub ukaraniu osoby (osób) odpowiedzialnej.

§ 7.
ZAWIADOMIENIE O NARUSZENIU OSOBĘ, KTÓREJ DANE DOTYCZĄ

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, prowadzące do szkód fizycznych, materialnych i niematerialnych. Szkodami takimi są np.:

1) dyskryminacja;
2) kradzież tożsamości lub oszustwo dotyczące tożsamości;
3) nadużycia finansowe;
4) straty finansowe;
5) nieuprawnione cofnięcie pseudonimizacji;
6) utrata poufności danych osobowych chronionych tajemnicą zawodową;
7) naruszenie dobrego imienia;
8) lub inne znaczące skutki gospodarcze lub społeczne dla danej osoby fizycznej.

Jeżeli naruszenie dotyczy danych osobowych ujawniających:

1) pochodzenie etniczne;
2) poglądy polityczne;
3) przekonania religijne lub światopoglądowe;
4) przynależność do związków zawodowych;
5) dane genetyczne;
6) dane dotyczące zdrowia;
7) dane dotyczące życia seksualnego;

należy uznać, że występuje duże prawdopodobieństwo takiej szkody. ADO – poza zgłoszeniem takiego naruszenia do organu nadzorczego – bez zbędnej zwłoki zawiadamia o naruszeniu osobę, której dane dotyczą.

2.Zawiadomienie osoby, której dane dotyczą, jasnym i prostym językiem opisuje:

1) charakter naruszenia;
2) zawiera imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
3) możliwe konsekwencje naruszenia ochrony danych osobowych;
4) środki zastosowane lub proponowane przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3. Zawiadomienie osoby, której dane dotyczą, o którym mowa w ust. 1 niniejszego paragrafu, nie jest wymagane jeżeli:

1) ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do danych;
2) ADO zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
3) Skontaktowanie się z osobami, których dane dotyczą, wymagałoby niewspółmiernie dużego wysiłku, w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje środek, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób.

4. Zawiadomienia o naruszeniu osoby, której dane dotyczą, może zażądać od ADO również organ nadzorczy w przypadku, gdy stwierdzi, że powyższe jest konieczne, a nie został spełniony żaden z warunków wskazanych w ust. 3 niniejszego paragrafu.
5. Informacje należy przekazywać osobom, których dane dotyczą, tak szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z organem nadzorczym, z poszanowaniem wskazówek przekazanych przez ten organ lub inne odpowiednie organy, takie jak organy ścigania.

§ 8.
ZOBOWIĄZANIE PODMIOTÓW PRZETWARZAJĄCYCH DO ZGŁASZANIA NARUSZEŃ

1.Administrator ponosi odpowiedzialność prawną za przetwarzanie danych osobowych prowadzone przez niego samego lub w jego imieniu czyli przez podmioty przetwarzające.
2.Zobowiązuje się więc pracowników do korzystania z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom RODO, w tym wymogom bezpieczeństwa przetwarzania.
3. Zgodnie z art. 33 ust. 2 RODO, podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi. Bez zbędnej zwłoki oznacza najszybciej jak to możliwe i taki termin wywiązywania się z tego obowiązku **powinien być nałożony na podmioty przetwarzające w umowach powierzenia.**
4. Termin i zasady powiadomienia o naruszeniach w umowach powierzenia, o którym mowa w ust. 3 winny być tak określone, by ADO mógł dochować terminu, o którym mowa w § 6 ust. 1 i spełnić wszystkie warunki postępowania określone w niniejszej instrukcji.

§ 9.
POSTANOWIENIA KOŃCOWE

1. Za prawidłowość realizacji niniejszej instrukcji i obowiązków wynikających z jej unormowań odpowiedzialni są wszyscy pracownicy.
2. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych oraz mogą stanowić podstawę do pociągnięcia osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, do odpowiedzialności dyscyplinarnej, odszkodowawczej lub karnej, w trybie i na zasadach przewidzianych przepisami prawa.

STAROSTA
Witold Darłak

Załącznik nr 1

Raport z incydentu Nr .....
naruszającego bezpieczeństwa danych osobowych

1. Data: ..... Godzina: .....
(dd.mm.rrrr) 00:00)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(Imię, nazwisko, stanowisko służbowe, funkcja, nazwa użytkownika - jeśli dotyczy)

3. Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia, piętro)

4. Osoby powodujące naruszenie (które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia ochrony danych osobowych):

.....

5. Osoby, które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych osobowych:

.....

6. Informacje o danych, które zostały lub mogły zostać ujawnione:

.....

7. Zabezpieczone materiały lub inne dowody związane z wydarzeniem:

.....

8. Krótki opis wydarzenia związanego z naruszeniem ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania korygujące, zapobiegawcze):

.....

Data:.....

Podpis:.....

STAROSTA
Witold Darłak

Załącznik nr 2

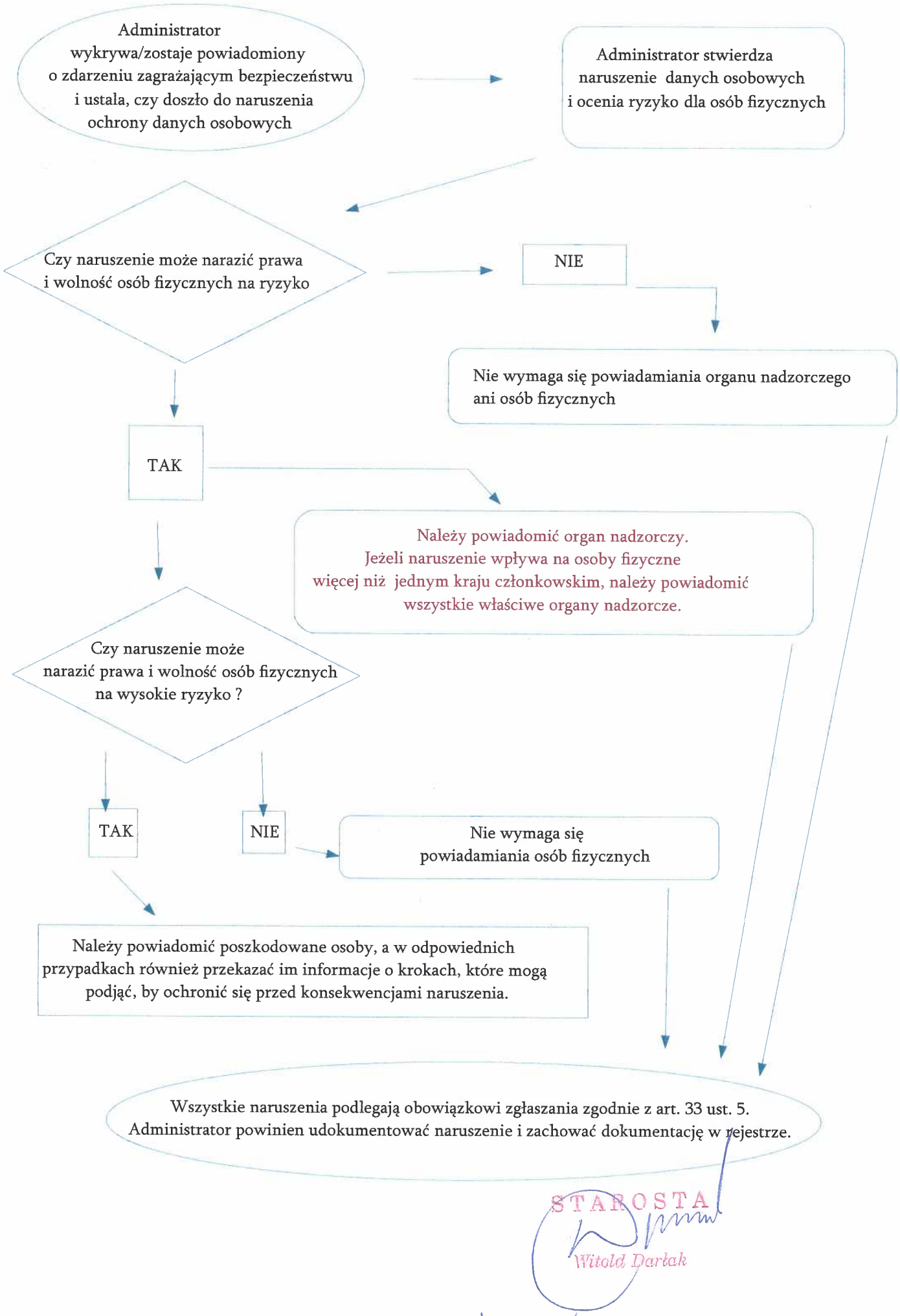
Nr:

REJESTR
przypadków naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania danych osobowych

Data zgłoszenia Naruszenia (dzień i godzina)	Zgłaszający	Rodzaj naruszenia	Miejsce naruszenia	Opis naruszenia	Skutki naruszenia	Czy naruszenie podlega zgłoszeniu do organu nadzorczego	Czy naruszenie podlega zgłoszeniu osobie, której dane dotyczą	Podjęte działania – sposób usunięcia naruszenie	Data zakończenia czynności	Status

STAROSTA
Witold Darłak

Załącznik nr 3



STAROSTA
Witold Darłak

Zgłoszenie naruszenia ochrony danych osobowych

Załącznik nr 4

1. Dane wnioskodawcy

A. Podaj 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.

- (●) Zg?oszenie kompletne/jednorazowe
- ( ) Zg?oszenie wst?pne
- ( ) Zg?oszenie uzupe?niaj?ce/zmieniaj?ce

Podaj datę poprzedniego zgłoszenia (opcjonalnie – jeśli zgłoszenie jest uzupełniające/zmieniające)

2. Podmiot zgłaszający

A. Dane administratora danych

Pełna nazwa administratora	Kliknij tutaj, aby wprowadzić tekst.
REGON – jeśli został podany (opcjonalnie)	Kliknij tutaj, aby wprowadzić tekst.
Sektor (opcjonalnie)	Dla sektora publicznego: Wybierz element. / Dla sektora prywatnego: Wybierz element.

B. Adres siedziby administratora danych

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

C. Osoby uprawnione do reprezentowania administratora

1.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.

(Aby dopisać kolejne osoby, należy po kliknięciu na powyższe pole kliknąć przycisk ✚, który pojawi się po prawej stronie)

D. Pełnomocnik

☐ Wniosek wypełniany przez pełnomocnika (opcjonalnie)

Pełnomocnictwo udzielone w formie elektronicznej oraz dowód uiszczenia opłaty skarbowej należy załączyć podczas składania wniosku przez portal biznes.gov.pl.
Pełnomocnictwo opatrzone kwalifikowanym podpisem elektronicznym osoby udzielającej pełnomocnictwa.

E. Inspektor ochrony danych

Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.
Numer telefonu	Kliknij tutaj, aby wprowadzić tekst.
Adres e-mail	Kliknij tutaj, aby wprowadzić tekst.

☐ 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.

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

STAROSTA
Witold Darłak

Podaj nazwy podmiotów, dane kontaktowe i wyjaśnij ich rolę w procesie przetwarzania, którego dotyczy naruszenie

Kliknij tutaj, aby wprowadzić tekst.

3. Czas naruszenia

A. Wykrycie naruszenia i powiadomienie organu nadzorczego

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

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.

B. Czas naruszenia

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

Kliknij tutaj, aby wprowadzić tekst.

☐ **Trwające naruszenie**
Zaznacz to pole, jeśli naruszenie trwa nadal w momencie zgłaszania.

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

Kliknij tutaj, aby wprowadzić tekst.

C. Komentarz do czasu naruszenia (opcjonalnie)

Możesz podać więcej szczegółów dotyczących czasu naruszenia i uzasadnić dlaczego nie są znane dokładne terminy zaistnienia naruszenia.

Kliknij tutaj, aby wprowadzić tekst.

4. Charakter naruszenia

A. 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

B. Na czym polegało naruszenie?

☐ Zgubienie lub kradzież nośnika/urządzenia

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

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

☐ Nieuprawnione uzyskanie dostępu do informacji

☐ Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń

☐ Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych

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

☐ Nieprawidłowa anonimizacja danych osobowych w dokumencie

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

☐ Niezamierzona publikacja

☐ Dane osobowe wysłane do niewłaściwego odbiorcy

☐ Ujawnienie danych niewłaściwej osoby

☐ Ustne ujawnienie danych osobowych

Opisz na czym polegało naruszenie.

Kliknij tutaj, aby wprowadzić tekst.

C. Dzieci

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

(opcjonalnie)

D. Przyczyna naruszenia

☐ Wewnętrzne działanie niezamierzone

☐ Wewnętrzne działanie zamierzone

☐ Zewnętrzne działanie niezamierzone

☐ Zewnętrzne działanie zamierzone

Inne przyczyny (w tym nieznane)

Kliknij tutaj, aby wprowadzić tekst.

4.1. Kategorie danych osobowych

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

A. Kategorie danych

Szczegółowy opis kategorii danych, których dotyczy naruszenie

Wymień jakie dane uległy naruszeniu: np. w przypadku sklepu internetowego profil użytkownika, w skład którego wchodzą:nazwa użytkownika, imię, nazwisko, hasło (zapisane otwartym tekstem lub hashowane), adres e-mail, oraz historia transakcji - kwota, data i nazwa kupionego produktu.

Kliknij tutaj, aby wprowadzić tekst.

B. Dane podstawowe

☐ Dane identyfikacyjne

np. imię, nazwisko, nr dowodu osobistego, adres IP

☐ Krajowy numer identyfikacyjny

np. PESEL, SSN

☐ Dane kontaktowe

np. e-mail, numer telefonu, adres korespondencyjny

☐ Dane ekonomiczne i finansowe

np. historie transakcji, faktury, dane o rachunkach bankowych, wnioski o wsparcie finansowe

☐ Oficjalne dokumenty

np. akty notarialne, dowody osobiste, prawa jazdy, karty pobytu, legitymacje

☐ Dane lokalizacyjne

np. GPS, dane o przemieszczaniu, miejsce zamieszkania

☐ Inne

Opisz poniżej kategorie danych:

Kliknij tutaj, aby wprowadzić tekst.

C. 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

D. Dane, o których mowa w art. 10 RODO

☐ Dane dotyczące wyroków skazujących

☐ Dane dotyczące czynów zabronionych

☐ Inne

Opisz poniżej kategorie danych:

Kliknij tutaj, aby wprowadzić tekst.

E. Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie

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.

4.2. Kategorie osób

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

A. Kategorie osób, których dane dotyczą

☐ 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

Kliknij tutaj, aby wprowadzić tekst.

B. Liczba osób, których mogło dotyczyć naruszenie

Przybliżona liczba osób, których mogło dotyczyć naruszenie — Kliknij tutaj, aby wprowadzić tekst.

5. Środki bezpieczeństwa zastosowane przed naruszeniem

A. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa stosowanych przez administratora przed naruszeniem (opcjonalnie)

Kliknij tutaj, aby wprowadzić tekst.

6. Możliwe konsekwencje

A. 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.

B. Ryzyko naruszenia praw i wolności osób fizycznych

○ Niskie ◉ ?rednie ○ Wysokie

7. Środki zaradcze

A. Komunikacja z osobami, których dane dotyczą

Czy osoby, których dane dotyczą, zostały powiadomione o naruszeniu?

◉ Tak | ○ Nie, ale zostan? powiadomione | ○ Nie, nie zostan? powiadomione | ○ Nie oceni?em jeszcze

Czy indywidualnie?

○ Tak

○ Nie, gdy? indywidualne powiadomienie ka?dej osoby, której dane dotycz? wymaga? oby niewspó?miernie du?ego wysi?ku. W zwi?zku z tym zosta? wydany publiczny komunikat lub zastosowano podobny ?rodek, za pomoc? którego osoby, których dane dotycz?, zosta?y poinformowane w równie skuteczny sposób.

Powód niezawiadomienia osób, których dane dotyczą:

○ Przed naruszeniem wdro?ono odpowiednie techniczne i organizacyjne ?rodki ochrony i ? rodki te zosta?y zastosowane do danych osobowych, których dotyczy naruszenie, w szczególno?ci ?rodki takie jak szyfrowanie, anonimizacja czy pseudonimizacja uniemo? liwiaj?ce odczyt osobom nieuprawnionym do dost?pu do tych danych osobowych.

○ Po naruszeniu zastosowano ?rodki eliminuj? ce prawdopodobie?stwo wysokiego ryzyka naruszenia praw lub wolno?ci osoby, której dane dotycz?.

Jeśli jeszcze nie oceniłeś, czy zamierzasz zawiadomić podmioty danych, pamiętaj, że po podjęciu takiej decyzji będziesz musiał złożyć zgłoszenie uzupełniające.

Wskaż datę kiedy osoby, których dane dotyczą, zostały powiadomione o naruszeniu

Wskaż datę kiedy zamierzasz powiadomić osoby, których dane dotyczą, o naruszeniu

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

Liczba zawiadomionych osób, których dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

Opis tych środków

Kliknij tutaj, aby wprowadzić tekst.

Środki komunikacji wykorzystane do zawiadomienia osoby, której dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

Treść zawiadomienia

Kliknij tutaj, aby wprowadzić tekst.

B. Środki w celu zaradzenia naruszeniu ochrony danych osobowych

Opisz dodatkowe środki (poza poinformowaniem osób) zastosowane lub proponowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia i jego ponownego wystąpienia.

Kliknij tutaj, aby wprowadzić tekst.

C. Transgraniczne przetwarzanie i inne powiadomienia

Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorczemu UE (oopcjonalnie)

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

Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorczemu spoza UE (oopcjonalnie)

Wymień inne organy nadzorcze spoza UE, którym naruszenie zostało lub zostanie zgłoszone

Kliknij tutaj, aby wprowadzić tekst.

Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorczemu UE z powodu innych zobowiązań prawnych (oopcjonalnie)

Np. obowiązek zgłoszenia incydentu wynikający z ustawy o krajowym systemie cyberbezpieczeństwa. Wymień inne organy, którym naruszenie zostało lub zostanie zgłoszone z powodu innych zobowiązań prawnych.

Kliknij tutaj, aby wprowadzić tekst.

Informacja:

jmowania działań określonych w art. 34 ust. 4 oraz art. 58 ust. 2 RODO1, a także prowadzenia przez organ wewnętrznego rejestru naruszeń na podstawie art. 57 ust. 1 lit. u RODO. Następnie Państwa da

niem przez Prezesa UODO z systemu elektronicznego zarządzania dokumentacją (EZD PUW).

ie 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 v

ınia władzy publicznej;

ɔostępowania administracyjnego.

takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) oraz podjętych działań.