

PROCEDURA POSTĘPOWANIA Z NARUSZENIAMI

w Pszczyńskim Towarzystwie Budownictwa Społecznego Sp. z o.o.

Zgodnie z RODO pojęcie „**naruszenie ochrony danych osobowych**” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem:

- zniszczenia danych osobowych,
- utracenia danych osobowych,
- zmodyfikowania danych osobowych,
- nieuprawnionego ujawnienia danych osobowych lub
- nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Wyżej wymienione przypadki występują m. in. gdy:

zauważono kradzież urządzeń takich jak komputery stacjonarne, serwery, urządzenia mobilne, nośniki danych,
stwierdzono naruszenie zabezpieczenia systemu informatycznego,
stwierdzono występowanie zniszczenia danych poprzez np. zalanie, pożar itp.,
stwierdzono celowe lub nieświadome przekazanie zbioru danych nieupoważnionym podmiotom.

1. Ocena wystąpienia naruszenia

Oceną naruszeń ochrony danych osobowych zajmuje się Inspektor Ochrony Danych Osobowych. Do jego zadań z zakresu oceny naruszeń należy w szczególności:

- a) dokonanie czynności pozwalających na ustaleniu okoliczności powstania zdarzenia w tym jeśli zachodzi taka potrzeba nawiązanie kontaktu ze specjalistami spoza Pszczyńskiego Towarzystwa Budownictwa Społecznego Sp. z o.o. w Pszczynie;
- b) zbieranie materiałów dowodowych dotyczących naruszenia;
- c) podjęcie działań korygujących i zapobiegawczych przed kolejnym naruszeniem;
- d) ustalanie środków i działań mających zminimalizować negatywne skutki naruszenia;
- e) dokumentowanie swoich działań;

f) powiadamianie o naruszeniu Administrator.

W przypadku stwierdzenia przez osobę posiadającą upoważnienie do przetwarzania danych osobowych naruszenia przepisów o ochronie danych osobowych należy:

- zgłosić naruszenie do Inspektora Ochrony Danych Osobowych drogą mailową iod@ptbspszczyzna.pl lub telefoniczną 32 212 85 55 oraz Administratora Danych;
- rozważyć wstrzymanie bieżącej pracy i pozostawić miejsce zdarzenia w stanie nienaruszonym do czasu przybycia Inspektora Ochrony Danych Osobowych;
- zaniechać- o ile to możliwe- dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudniać udokumentowanie i analizę;
- pisemnie określić okoliczności i sposób wykrycia naruszenia;
- nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia IOD;

2. Inspektor Ochrony Danych Osobowych ma obowiązek dokonać wstępnej oceny i analizy okoliczności zdarzenia tj.:

- sporządzić notatki z przeprowadzonego oględzin miejsca zgłoszenia;
- ewentualnie sporządzić kopię obrazu wyświetlonego na ekranie monitora komputera związanego z naruszeniem;
- przesłuchać osobę zgłaszającą naruszenie oraz świadków zdarzenia;
- wyjaśnić okoliczności zdarzenia i dokonać oceny skutków naruszenia w czasie nie dłuższym niż 48 godzin od momentu zgłoszenia;
- sporządzić raport i przedłożyć go Administratorowi Danych a w przypadku jego nieobecności osobie uprawnionej;
- zgłosić naruszenie do Urzędu Ochrony Danych Osobowych w Warszawie - nie później jednak niż w terminie 72 godzin od stwierdzenia naruszenia lub zaniechać zgłoszenie w przypadku stwierdzenia, że jest mało prawdopodobne, aby naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych;

3. Administrator wyciąga konsekwencje dyscyplinarne względem osób, które dokonały naruszenia świadomie lub gdy naruszenie powstało w skutek rażącego niedbalstwa. Administrator może wyciągać konsekwencje dyscyplinarne także względem tych osób, które przyczyniły się do powstania naruszenia w wyniku niestosowania się do obowiązujących reguł i zasad postępowania w zakresie ochrony danych osobowych w Spółce.

4. Powiadomienie osoby, której dane dotyczą

- A. Naruszenia przepisów o ochronie danych osobowych, które mogą skutkować wysokim ryzykiem naruszenia praw i wolności osoby, której dane dotyczą, Administrator lub Inspektor Ochrony Danych Osobowych w imieniu Administratora zawiadamia o naruszeniu tę osobę w sposób jasny, zrozumiały, który opisuje charakter naruszenia ochrony danych osobowych, możliwe konsekwencje i zastosowane środki minimalizujące skutki naruszenia.
- B. Administrator odstępuje od zawiadomienia osób o zaistniałym naruszeniu ochrony danych, jeżeli dokonana ocena wykazuje, że:
- a) naruszenie przepisów o ochronie danych nie stanowi naruszenia ochrony danych osobowych lub gdy jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych;
 - b) naruszenie danych osobowych dotyczyło danych, przy których wdrożono odpowiednie środki techniczne i organizacyjne, w szczególności takie jak szyfrowanie uniemożliwiające odczyt danych osobowych przez osoby nieuprawnione.
- C. W przypadku naruszenia dotyczącego wielu osób Administrator wydaje publiczny komunikat lub zamieszcza go na stronie internetowej Spółki.

5. Rodzaje zdarzeń:

Uchybienie – jest to celowe lub nieświadome działanie, na skutek którego **może dojść** do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych;

Naruszenie – jest to celowe lub nieświadome działanie, na skutek którego **doszło** do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.

6. W przypadku stwierdzenia **uchybienia** należy:

- odnotować je w odpowiednim rejestrze;
- zastosować działania korygujące uniemożliwiające ponowne powstanie tego zdarzenia.

7. W przypadku stwierdzenia **naruszenia**:

- ✓ Zabezpieczyć dane osobowe, nośniki danych oraz wszelkie inne możliwe do zabezpieczenia dowody.

- ✓ Odnosić naruszenie w odpowiednim rejestrze naruszeń.

Po wystąpieniu w Spółce uchybienia lub naruszenia Inspektor Ochrony Danych winien zaproponować działania i/lub rozwiązania proceduralne, organizacyjne, kadrowe i techniczne, które zapobiegałyby podobnym zdarzeniom w przyszłości oraz podjąć próbę przywrócenia stanu sprzed powstania zagrożenia.

Nie kopiować

TABELA UCHYBIEŃ I ZAGROŻEŃ

Kod uchybienia lub zagrożenia	Uchybienia i zagrożenia nieświadome wewnętrzne i zewnętrzne
01	Pomieszczenie, w którym przechowywane są dane osobowe pozostaje bez nadzoru.
02	Komputer nie jest zabezpieczony hasłem.
03	Dostęp do danych osobowych mają osoby nieposiadające upoważnienia.
04	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym.
05	Próba kradzieży lub kradzież danych osobowych przetwarzanych w formie elektronicznej.
06	Próba kradzieży lub kradzież danych osobowych w formie papierowej (łącznie z kradzieżą pośrednią, np. kradzież samochodu z dokumentami w środku)
07	Nieuprawniony dostęp do danych osobowych w formie papierowej.
08	Dane osobowe przechowywane są w niezabezpieczonym pomieszczeniu.
09	Próba włamania do pomieszczenia/budynku.
10	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania.
11	Brak aktywnego oprogramowania antywirusowego.
12	Zniszczenie lub modyfikacja danych osobowych w formie papierowej.
13	Zniszczenie lub modyfikacja danych osobowych w systemie informatycznym.
14	Uszkodzenie komputerów, nośników danych.
15	Próba nieuprawnionej interwencji przy sprzęcie komputerowym.
16	Zdarzenia losowe.
17	Podjęte (nietypowe) działanie komputera lub sprzętu.

18	Próba wyłudzenia lub wyłudzenie informacji przez osobę nieuprawnioną (telefonicznie, mailowo, osobiście)
19	Zagubienie nośnika danych osobowych (dokumentu, dysku, komórki, komputera)
20	Nieuprawnione udostępnienie danych (np. przesłanie wiadomości e-mail na niepoprawny adres, niepoprawne zaadresowanie poczty tradycyjnej)

Nie kopiować

Pszczyna, dnia r.

Inspektor Ochrony Danych:

.....

PROTOKÓŁ UCHYBIENIA

Pszczynskiego Towarzystwa Budownictwa Społecznego Sp. z o. o. w Pszczynie

Data i godzina wystąpienia uchybienia:

Miejsce wystąpienia uchybienia:

Osoba zgłaszająca:

Kod uchybienia :

Szczegółowy zdarzenia:

.....
.....
.....
.....

Przyczyny powstania uchybienia:

.....
.....
.....
.....

Skutki uchybienia:

.....

.....

.....

.....

Podjęte działania naprawczo-zapobiegawcze:

.....

.....

.....

.....

Uwagi dodatkowe:

.....

Inspektor Ochrony Danych Osobowych

.....

Administrator

Pszczyna, dnia r.

Inspektor Ochrony Danych Osobowych:

.....

RAPORT Z NARUSZENIA

Pszczyńskiego Towarzystwa Budownictwa Społecznego Sp. z o. o. w Pszczynie

Data i godzina wystąpienia naruszenia:

Miejsce wystąpienia naruszenia:

Osoba zgłaszająca:

Kod naruszenia (i/lub informacja dot. charakteru naruszenia):

Szczegółowy zdarzenia:

.....
.....
.....
.....

Możliwa przyczyny powstania naruszenia:

.....
.....
.....
.....

Skutki naruszenia:

.....
.....

.....
.....

Podjęte działania naprawczo-zapobiegawcze:

.....
.....
.....
.....

Uwagi dodatkowe:

.....
.....
.....
.....

Nie kopiować

.....
Inspektor Ochrony Danych Osobowych

.....
Administrator