Załącznik Nr 1 do Uchwały
Zarządu Nr 191/2020
z dnia 21 grudnia 2020 r.

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Spis treści:

I. Istota naruszenia danych osobowych

§ 1

Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych. 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. nieautoryzowany dostęp do danych,
2. nieautoryzowane modyfikacje lub zniszczenie danych,
3. udostępnienie danych nieautoryzowanym podmiotom,
4. nielegalne ujawnienie danych,
5. pozyskiwanie danych z nielegalnych źródeł.

II. Postępowanie w przypadku naruszenia danych osobowych

§ 2

1. Każdy pracownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych jest zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu. Przełożony zgłasza fakt osobie pełniącej obowiązki Inspektora Ochrony Danych.
2. Typowe sytuacje, w których użytkownik powinien powiadomić osobę pełniącą obowiązki Inspektora ochrony danych:
    a) ślady na drzwiach, oknach i szafach wskazujące na próbę włamania;
    b) niszczenie dokumentacji 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, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.
e) niewylogowanie się z programu przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, posługiwanie się informacjami służbowymi w celach prywatnych;
f) ustawienie monitorów pozwalających na wgląd osób postronnych w dane osobowe;
g) wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz Spółdzielni bez upoważnienia;
h) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
i) stwierdzenie próby modyfikacji danych lub dokonanie zmian w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
j) telefoniczne próby wyłudzenia danych osobowych;
k) kradzież komputerów lub twardych dysków z danymi osobowymi;
l) utrata kontroli nad kopią danych osobowych;
m) maile zachęcające do ujawnienia identyfikatora i/lub hasła;
n) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
o) istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki";
p) przechowywanie haseł w pobliżu komputera.

§ 3

Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutki naruszenia.

§ 4

W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia lub udokumentowania zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia osoby pełniącej obowiązki Inspektora Ochrony Danych lub innej osoby upoważnionej przez Administratora Danych.

§ 5

Administrator Systemu Informatycznego jest zobowiązany do informowania osoby pełniącej obowiązki Inspektora Ochrony Danych o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

§ 6

Osoba pełniąca obowiązki Inspektora Ochrony Danych podejmuje następujące kroki:

1. zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy,
2. odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
3. nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).

§ 7

Osoba pełniąca obowiązki Inspektora Ochrony Danych dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając Raport z naruszenia ochrony danych - Załącznik nr 1.

.

§ 8

Osoba pełniąca obowiązki Inspektora Ochrony Danych zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych ich zabezpieczenia oraz terminu wznowienia przetwarzania danych osobowych) - Załącznik nr 2 - Rejestr incydentów i działań korygujących i zapobiegawczych.

III. Naruszenie danych osobowych - odpowiedzialność

§ 9

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. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. 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.

IV. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

§ 10

1. W przypadku naruszenia ochrony danych osobowych Administrator bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia zgłasza je Urzędowi Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego

organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Wzór zgłoszenia – Załącznik nr 3.

2. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
    a) 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;
    b) zawierać imię i nazwisko oraz dane kontaktowe osoby pełniącej obowiązki inspektora ochrony danych lub oznaczenie innego punktu kontaktowego od którego można uzyskać więcej informacji;
    c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
    d) opisywać środki zastosowane lub proponowane przez Administratora w celu zapobiegania naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków;
3. Jeżeli informacji nie da się udzielić w tym samym czasie i w pełnym zakresie, można je udzielać sukcesywnie bez zbędnej zwłoki.
4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania niniejszego paragrafu.

V. Zawiadamianie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych

§ 11

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego paragrafu jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w § 10 ust. 2 lit. b), c) i d).
3. Zawiadomienie, o którym mowa w ust. 1 nie jest wymagane w następujących przypadkach:

a) Administrator 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;
b) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
c) Gdy wymagałoby 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.

Załącznik nr 1

Raport z naruszenia danych osobowych

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 osoby pełniącej obowiązki Inspektora Ochrony Danych).....

Załącznik nr 2

Rejestr incydentów bezpieczeństwa oraz działań korygujących i zapobiegawczych

Zadanie / problem / incydent…….....
(podać opis incydentu)
Źródło zgłoszenia…….....
.....
(podać źródło zgłoszenia np. zawiadomienie, kontrola, itd.)
Data rozpoczęcia ……..
Data zakończenia …….....
Odpowiedzialny za realizację…….....
(podać dane osoby lub funkcje osoby odpowiedzialnej)
Przyczyna niezgodności…….....
.....
(podać przyczynę powstania incydentu

Działanie korygujące / zapobiegawcze .....
…….....
(opisać działania jakie podjęto w celu przywrócenia bezpieczeństwa)

Ocena skuteczności …….....
.....
(opisać jakie skutki przyniosło działanie korygujące)

Załącznik nr 3

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

Organem właściwym do zgłaszania naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO).
Zgłoszenie naruszenia dokonuje się elektronicznie za pomocą odpowiedniego formularza dostępnego pod adresem https://uodo.gov.pl/pl/134/233, który należy wypełnić, a następnie załączyć do pisma ogólnego dostępnego na platformie biznes.gov.pl

VI. Postanowienia ogólne

1. W sprawach nieuregulowanych niniejszą Instrukcją należy stosować powszechnie obowiązujące przepisy prawne.

2. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych została przyjęta Uchwałą Zarządu SBM WARDOM Nr 191/2020 z dnia 21 grudnia 2020 roku i obowiązuje od dnia wejścia w życie Uchwały.

…….. …….. ……..

Zarząd SBM WARDOM