Załącznik nr 6
do zarządzenia nr 75/2020
Starosty Jaworskiego
z dnia 13 października 2020 r.

Instrukcja postępowania w sytuacji naruszenia zasad ochrony danych osobowych

§ 1.

Zastosowane w instrukcji określenia zostały zdefiniowane w zarządzeniu ODO.

§ 2.

1. Naruszeniem zasad organizacyjnej ochrony danych osobowych, jest złamanie zasad zapewniających bezpieczeństwo danych osobowych, w szczególności:
   1) nieuprawniony dostęp lub próba dostępu do pomieszczeń, w których odbywa się przetwarzanie danych osobowych;
   2) niezmykanie drzwi w przypadku opuszczenia pomieszczenia przez pracownika Starostwa;
   3) pozostawianie klucza w drzwiach pomieszczenia, w którym przetwarzane są dane osobowe;
   4) praca przy przetwarzaniu danych osobowych osoby nieprzeszkolonej lub/i nieposiadającej upoważnienia do przetwarzania danych osobowych, wydanego przez ADO;
   5) udzielenie informacji telefonicznie osobie nieuprawnionej do uzyskania tych informacji;
   6) przebywanie osób nieuprawnionych w pomieszczeniu, gdzie przetwarza się dane osobowe bez nadzoru osoby upoważnionej przez ADO;
   7) celowe lub nieświadome przekazanie danych osobowych osobie nieuprawnionej do ich otrzymania;
   8) nienależyte zabezpieczenie danych, w tym niechowanie dokumentów do zamykanych szaf i pozostawianie w miejscu ogólnie dostępnym, przechowywanie dokumentów i nośników cyfrowych zawierających dane osobowe w szafach z niesprawnymi zamkami;
   9) wyrzucanie dokumentów zawierających dane osobowe bez uprzedniego ich zniszczenia w stopniu uniemożliwiającym odczytanie danych;
   10) przebywanie pracowników obsługi informatycznej lub technicznej firm zewnętrznych w budynku, bez nadzoru ASI lub uprawnionych pracowników Starostwa;
   11) kradzież dokumentów lub nośników cyfrowych zawierających dane osobowe.
2. Naruszeniem zasad technicznej ochrony danych osobowych są w szczególności działania:
   1) naruszenie lub próby naruszenia integralności Systemu Informatycznego Starostwa przez osoby nieuprawnione do dostępu do systemu informatycznego;
   2) nieautoryzowane logowanie do Systemu Informatycznego Starostwa;
   3) nieuprawnione prace na koncie użytkownika dopuszczonego do przetwarzania danych osobowych przez osobę do tego nieuprawnioną;
   4) ujawnienie hasła funkcjonującego w Systemie Informatycznym Starostwa osobie nieuprawnionej;
   5) istnienie nieautoryzowanych kont dostępu do Systemu Informatycznego Starostwa, w tym nieblokowanie kont osób z cofniętym upoważnieniem do przetwarzania danych

osobowych lub/i z cofniętym upoważnieniem do pracy w Systemie Informatycznym Starostwa;
6) włamanie lub próba włamania z zewnątrz sieci;
7) nieautoryzowane zmiany danych w Systemie Informatycznym Starostwa;
8) niezablokowanie stacji roboczej przez użytkownika podczas nieobecności przy stacji roboczej;
9) nieautoryzowana zmiana lub usunięcie danych zapisanych na kopiach bezpieczeństwa lub kopiach archiwalnych;
10) brak lub niepełna ochrona antywirusowa elementów Systemu Informatycznego Starostwa;
11) niewykonywanie kopii zapasowych w przewidzianym terminie;
12) wykonywanie uszkodzonych kopii zapasowych;
13) niewłaściwe lub nieuprawnione uszkadzanie, niszczenie nośników zawierających dane osobowe;
14) brak zastosowania, przy przekazywaniu danych z Systemu Informatycznego Starostwa lub łączenia się z Systemem Informatycznym Starostwa z zewnątrz, kryptograficznych środków ochrony danych;
15) zła jakość komunikacji w sieci telekomunikacyjnej.

§ 3.

1. W przypadku wystąpienia okoliczności wskazujących na możliwość naruszenia zasad ochrony danych, o których mowa w § 2., pracownicy Starostwa zobowiązani są do natychmiastowego reagowania w sposób określony w ust. 2 do ust. 4.
2. W sytuacji wskazującej na naruszenie ochrony danych osobowych należy:
   1) w miarę możliwości zabezpieczyć dane osobowe przed dalszą podatnością na naruszenie;
   2) natychmiast poinformować IOD oraz swojego bezpośredniego przełożonego;
   3) w przypadku naruszenia zasad ochrony organizacyjnej zgłosić ten fakt do pracownika Starostwa odpowiedzialnego za ochronę budynku Starostwa;
   4) w przypadku naruszenia zasad ochrony technicznej zgłosić ten fakt ASI.
3. Po pierwszej reakcji na potencjalne naruszenie zasad ochrony danych osobowych, osoba stwierdzająca naruszenie wraz z IOD zobowiązane są do:
   1) podjęcia czynności zmierzających do zabezpieczenia miejsca zdarzenia, zabezpieczenia ewentualnych dowodów naruszenia i minimalizacji zaistniałych szkód, w szczególności poprzez:
      a) wstrzymanie przekazywania i udostępniania danych osobowych,
      b) usunięcie uchybień,
      c) zastosowanie dodatkowych środków technicznych i organizacyjnych zabezpieczających dane osobowe,
      d) zwiększenie kontroli podczas przetwarzania danych osobowych;
   2) możliwie pełnego udokumentowania zdarzenia celem precyzyjnego określenia przyczyn i ewentualnych skutków naruszenia obowiązujących zasad.
4. W sytuacji naruszenia zasad ochrony danych osobowych, niezwłocznie, po wcześniejszym wykonaniu czynności opisanych w ust. 2 i ust. 3, dokonuje się oceny, czy naruszenie skutkuje lub może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, w szczególności:
   1) oceny, czy naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych dokonuje zespół składający się z:
      a) Starosty,
      b) IOD,

c) kierowników komórek organizacyjnych Starostwa merytorycznie odpowiedzialnych za dane osobowe, których naruszenie dotyczy;
d) ASI, jeśli naruszenie dotyczy danych osobowych przetwarzanych w Systemie Informatycznym Starostwa;

2) dokonuje się oceny prawdopodobieństwa ryzyka naruszenia praw lub wolności osób fizycznych;
3) zespół o którym mowa w punkcie 1 winien dokonać oceny bez zbędnej zwłoki, w miarę możliwości, nie później niż w terminie 24 godzin od stwierdzenia naruszenia i przekazać tę ocenę ADO.

5. W przypadku naruszenia ochrony danych osobowych, ADO bez zbędnej zwłoki (w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia) zgłasza je (zgodnie z art. 33 RODO) organowi nadzorczemu właściwemu zgodnie z art. 55 RODO, chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych – prawdopodobieństwo określone jest zgodnie z art. 34 ust. 4.
6. Jeśli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO, bez zbędnej zwłoki, zawiadamiania osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych zgodnie z art. 34 RODO.