Załącznik Nr 2 do Polityki bezpieczeństwa danych osobowych Uniwersytetu Przyrodniczego w Lublinie

Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych

1. Przez naruszenie ochrony danych osobowych rozumie się:
   1) stwierdzone naruszenie zabezpieczenia systemu informatycznego;
   2) sytuacje, gdy stan urządzeń, zawartość zbioru danych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczenia danych;
   3) udostępnienie nieupoważnionym instytucjom lub osobom danych osobowych podlegających ochronie.
2. Każdy pracownik Uniwersytetu Przyrodniczego w Lublinie a w szczególności osoba zatrudniona przy przetwarzaniu danych osobowych, jest obowiązana niezwłocznie powiadomić o zaistniałym przypadku naruszenia ochrony danych osobowych Administratora Danych Osobowych oraz Inspektora Ochrony Danych.
3. Zgłoszenie incydentu może być wykonane osobiście, telefonicznie lub za pośrednictwem poczty elektronicznej i powinno zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia –pracownik zgłaszający naruszenie może zostać poproszony o opisanie zdarzenia na piśmie lub w innej utrwalonej formie
4. W przypadku stwierdzenia, że istnieje wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO, IODO albo inna osoba upoważniona przez Administratora Danych Osobowych, bez zbędnej zwłoki zgłasza naruszenie do organu nadzorczego – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.
5. IOD na podstawie poziomu ryzyka dotyczącego naruszenia praw lub wolności osób fizycznych decyduje o konieczności i jeżeli jest to zasadne, bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu, jasnym i prostym językiem opisując charakter naruszenia ochrony danych osobowych.
6. Inspektor Ochrony Danych Osobowych ma obowiązek:
   1) zarejestrować fakt naruszenia danych osobowych podając miejsce, datę oraz przypuszczalny zakres ich naruszenia;
   2) w miarę możliwości ustalić osobę odpowiedzialną za zaistniałą sytuację;
   3) przeanalizować istniejący sposób zabezpieczenia i przedsięwziąć działania eliminujące w przyszłości podobne sytuacje;
   4) podjąć w miarę możliwości, działania zmierzające do usunięcia ewentualnych skutków naruszenia ochrony danych.