Załącznik Nr 1
do Zarządzenia Rektora Nr 12/2002
z dnia 10 czerwca 2002r.

Instrukcja
w sprawie ochrony danych osobowych

Rozdział I
Przepisy ogólne

1. Każdy ma prawo do ochrony dotyczących go danych osobowych.
2. W rozumieniu ustawy za dane osobowe uważa się każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby.
3. Ilekroć w instrukcji jest mowa o:
   a) administratorze danych – rozumie się przez to Akademię Rolniczą im. Hugona Kołłątaja w Krakowie;
   b) zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
   c) przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
   d) usuwaniu danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
   e) zgodzie osoby, której dane dotyczą – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści;
   f) systemie informatycznym – rozumie się przez to system przetwarzania informacji wraz ze związanymi z nim ludźmi oraz zasobami technicznymi i finansowymi, który dostarcza i rozprowadza informacje;
   g) zabezpieczeniu systemu informatycznego – rozumie się przez to wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przez modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.
4. Zgodnie z art. 27 ust. 1 ustawy o ochronie danych osobowych - zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym.
5. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były:
   a) przetwarzane zgodnie z prawem;
   b) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem pkt. 6 niniejszej instrukcji;
   c) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
   d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

6. Przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje:
   a) w celach naukowych, dydaktycznych, historycznych lub statystycznych;
   b) z zachowaniem przepisów art. 23 i art. 25 ustawy o ochronie danych osobowych.

Rozdział II
Sposób zarządzania systemem informatycznym

7. W zakresie działalności podległych jednostek organizacyjnych Uczelni lokalni administratorzy danych o których mowa w § 2 ust. 3 Zarządzenia, zobowiązani są:
   a) ustalić - działając wspólnie z właściwym lokalnym administratorem bezpieczeństwa informacji - sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz wskazać osobę odpowiedzialną za te czynności;
   b) ustalić sposób rejestrowania i wyrejestrowywania użytkowników oraz wskazać osobę odpowiedzialną za te czynności;
   c) określić procedurę rozpoczęcia i zakończenia pracy;
   d) doraźnie określić metodę i częstotliwość tworzenia kopii awaryjnych oraz sposób ich przechowywania i niszczenia;
      natomiast docelowo, po zabezpieczeniu Uczelni w odpowiedni sprzęt i oprogramowanie – lokalnie ustalić zasady tworzenia kopii bezpieczeństwa na dyskach i na głównym serwerze po jego wdrożeniu;
   e) określić metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania.
8. Ponadto lokalni administratorzy danych zapewniają właściwe warunki organizacyjno-techniczne zapewniające bezpieczeństwo przetwarzanych danych m.in. poprzez:
   a) zabezpieczanie pomieszczeń lub ich części w których przetwarzane są dane osobowe przed dostępem osób nieuprawnionych;
   b) eliminowanie dowolnego przemieszczania komputerów z zainstalowanymi systemami przetwarzającymi dane osobowe poza obszar objęty szczególną ochroną;
   c) stałą współpracę z administratorami bezpieczeństwa informacji (tj. właściwym lokalnym oraz uczelnianym).
9. Nośniki informacji, w tym kopie informatyczne i wydruki zawierające dane osobowe przechowywane są w Uczelni przez jeden miesiąc:
   a) w Tajnej Kancelarii, jeżeli dane te zawierają informacje niejawne stanowiące tajemnicę służbową oznaczoną odpowiednią klauzulą tajności;
   b) lub w innym miejscu, w szafie (skrzyni) metalowej zabezpieczonej zgodnie z odpowiednimi przepisami.
10. Lokalni administratorzy danych odpowiedzialni są za zabezpieczenie zbiorów danych osobowych zgromadzonych na elektronicznych nośnikach informacji w przypadkach wykonywania czynności serwisowych (naprawa, konserwacja) lub likwidacji sprzętu. W takich sytuacjach naprawa/konserwacja powinna być dokonywana na miejscu, w obecności użytkownika sprzętu. Sprzęt oddawany do punktu serwisowego lub do likwidacji powinien zostać pozbawiony zapisów zbiorów danych osobowych.
11. W Uczelni dane osobowe mogą być przesyłane w sieci wyłącznie w postaci zaszyfrowanej.

Rozdział III

Postępowanie w sytuacji naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych

12. Przez naruszenie ochrony danych osobowych rozumieć należy:
    a) stwierdzone naruszenie zabezpieczenia systemu informatycznego;
    b) sytuacje, gdy zawartość zbioru danych, stan urządzeń, ujawnione metody pracy lub sposób działania programu mogą wskazywać na naruszenie zabezpieczenia danych;
    c) udostępnienie nieupoważnionym osobom fizycznym lub prawnym danych osobowych podlegających ochronie.
13. Każdy pracownik Uczelni, w szczególności zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest niezwłocznie powiadomić właściwego lokalnego administratora danych osobowych o stwierdzonym przypadku naruszenia ochrony danych osobowych.
14. W sytuacjach o których mowa w pkt. 13 instrukcji, lokalny administrator danych osobowych wspólnie z lokalnym administratorem bezpieczeństwa informacji oraz pracownikiem, który stwierdził naruszenie ochrony danych protokolarnie ustalają:
    a) zakres naruszenia ochrony danych,
    b) przyczyny naruszenia,
    c) ewentualny stopień winy pracownika.
15. W przypadku, gdy naruszenie nastąpiło bez winy pracownika, lokalny administrator danych osobowych - po analizie zaistniałej sytuacji - może wystąpić do bezpośredniego przełożonego o zwiększenie zabezpieczeń systemu informatycznego.

Kraków, 10 czerwiec 2002 r.