

Załącznik nr 1
Do zarządzenia Rektora nr R-0121-20/2003
z dnia 25 kwietnia 2003 roku

I n s t r u k c j a
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 Ekonomiczną 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 jakiejkolwiek 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) Usuwanie 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 stosowanych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed 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,



- partijną 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 wyrejestrowania użytkowników oraz wskazać osobę odpowiedzialną za te czynności;
 - c) Określić procedurę rozpoczęcia i zakończenia pracy;
 - d) Określić metodę i częstotliwość tworzenia kopii awaryjnych oraz sposób ich przechowywania i niszczenia;
 - 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) Zabezpieczenie 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 siedzibie Pełnomocnika Rektora ds. Informacji Niejawnych, jeżeli dane te zawierają informacje niejawne stanowiące tajemnicę służbową oznaczoną odpowiednią klauzurą 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 / napraw, 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.
12. Likwidacji nośników informacji /dyskietek, CD – ROM-ów itp./ dokonuje Uczelniana Komisja Likwidacyjna.

Rozdział III

Postępowanie w sytuacji naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych

13. 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.
14. Każdy pracownik Uczelni, w szczególności zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest niezwłocznie powiadomić właściwego lokalnego administratora danych osobowych o stwierdzonym przypadku naruszenia danych osobowych.
15. 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 osobowych,
 - b) Przyczyny naruszenia,
 - c) Ewentualny stopień winy pracownika.
16. 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.



Załącznik Nr 2
Do zarządzenia Rektora Nr R-0121-20/2003
Z dnia 25 kwietnia 2003 roku

.....
(imię i nazwisko, stanowisko)

.....
(jednostka organizacyjna)

O Ś W I A D C Z E N I E

Oświadczam, że w związku z wykonywaniem obowiązków służbowych związanych z gromadzeniem, przetwarzaniem i przechowywaniem danych osobowych, zostałem zapoznany z obowiązującymi w zakresie ochrony danych osobowych przepisami państwowymi i wewnętrznymi Akademii Ekonomicznej w Krakowie i zobowiązuję się do ich przestrzegania i stosowania.

Kraków, dnia.....

.....
(podpis)



Załącznik Nr 3
Do zarządzenia Rektora Nr R-0121-20/2003
z dnia 25 kwietnia 2003 roku

.....
(nazwa jednostki organizacyjnej)

Wykaz pomieszczeń oraz osób zatrudnionych przy przetwarzaniu danych osobowych

Lp.	Postać danych osobowych*	Lokalizacja (budynek nr. pokoju)	Sposób zabezpieczenia dostępu do danych osobowych	Osoba odpowiedzialna za zabezpieczenie dostępu do danych osobowych	Osoby zatrudnione przy przetwarzaniu danych osobowych lub mające do nich dostęp	Uwagi

- *) wpisać
-) dokumenty źródłowe
-) dane przetworzone (podać formę przetworzenia)

