Załącznik nr 2
do Polityki ochrony danych osobowych
w WSPiA Rzeszowskiej Szkole Wyższej

Szczegółowe zasady postępowania osób upoważnionych w WSPiA Rzeszowskiej Szkole Wyższej do przetwarzania danych osobowych

I. Postanowienia ogólne

1. Niniejszy dokument określa szczegółowo obowiązki osób upoważnionych w Uczelni do przetwarzania danych osobowych, których przestrzeganie zapewni bezpieczeństwo tych danych.
2. Zasady te obejmują reguły postępowania w zakresie przetwarzania danych osobowych zarówno w tradycyjnych zbiorach danych tj. na papierowych nośnikach jak też w systemach informatycznych i na nośnikach cyfrowych.

II. Reguły postępowania dotyczące przetwarzania danych osobowych w tradycyjnych zbiorach danych

1. Niedozwolone jest – co do zasady, wynoszenie dokumentów w formie papierowej zawierających dane osobowe poza teren Uczelni. Jeżeli jednak zachodzi konieczność przeniesienia dokumentów zawierających dane osobowe np. między budynkami Uczelni lub do instytucji publicznej czy kontrahenta, należy je odpowiednio zabezpieczyć, w szczególności przed rozsypaniem, zamoczeniem, upuszczeniem i nie należy ich pozostawiać bez kontroli. Konieczność przeniesienia dokumentów z budynków Uczelni do innego miejsca należy ograniczyć do niezbędnego minimum.
2. Dokumenty w formie papierowej zawierające dane osobowe, muszą pozostawać w pomieszczeniach przeznaczonych do ich przetwarzania.
3. Jeżeli dokumenty w formie papierowej nie pozostają pod nadzorem osoby upoważnionej do przetwarzania danych, muszą być przechowywane zawsze w zamkniętych na klucz szafach, przy czym klucz nie może być pozostawiony w zamku.
4. Wszelkie dokumenty w formie papierowej zawierające dane osobowe należy przed opuszczeniem miejsca pracy i po zakończeniu dnia pracy zniszczyć w niszczarce lub umieścić w szafach zamykanych na klucz.
5. Wszelkie akta zawierające dane osobowe należy przed opuszczeniem miejsca pracy i po zakończeniu dnia pracy schować do szaf zamykanych na klucz (zasada czystego biurka).
6. Klucze do szaf, w których przechowywane są dane osobowe, należy po zakończeniu dnia pracy umieścić w ustalonym, przeznaczonym do tego miejscu – uzgodnionym z kierownikiem komórki organizacyjnej.

III. Reguły postępowania dotyczące przetwarzania danych osobowych w systemach informatycznych i na cyfrowych nośnikach informacji

1. Ekrany komputerów należy ustawiać tak, by osoby niepowołane nie mogły oglądać informacji wyświetlonych na ich ekranach. Nie należy ustawiać ekranów naprzeciwko wejścia do pomieszczenia (zwróconych w kierunku wejścia).
2. Wyłącznym miejscem przechowywania danych osobowych w formie elektronicznej są dedykowane systemy informatyczne oraz przydzielona przestrzeń dyskowa na serwerze Uczelni. Zabronione jest utrzymywanie danych osobowych na dyskach twardych komputerów oraz innych nośnikach danych.
3. Pracownicy wykorzystujący komputery stacjonarne lub przenośne komputery służbowe korzystają z konta użytkownika systemu. Tylko w wyjątkowych, uzasadnionych okolicznościach Administrator systemu informatycznego może umożliwić użytkownikowi czasowy dostęp do konta administratora systemu operacyjnego.
4. Administrator systemu informatycznego odpowiada za konfigurację komputerów oraz szyfrowanie dysków.
5. Przenośne komputery służbowe mogą być wykorzystywane poza terenem Uczelni wyłącznie za zgodą kierownika danej jednostki organizacyjnej.
6. Z uwagi na zadania realizowane w Uczelni przez różne grupy pracowników, dopuszcza się stosowanie prywatnych komputerów stacjonarnych lub przenośnych. Prywatne urządzenia wykorzystywane do przetwarzania danych osobowych muszą być zabezpieczone hasłem, a użytkownicy muszą przestrzegać zasad postępowania osób upoważnionych do przetwarzania danych osobowych.
7. Wszystkie tymczasowe zbiory danych osobowych muszą zostać usunięte niezwłocznie po osiągnięciu celu przetwarzania.
8. Nie należy używać do drukowania danych osobowych powtórnie dokumentów uprzednio zadrukowanych jednostronnie, a wydruki dokumentów zawierających dane osobowe należy ograniczyć do niezbędnego minimum.
9. Hasła wykorzystywane do logowania się do systemów, komputera i urządzeń mobilnych muszą być utrzymywane w tajemnicy i nie mogą być udostępniane osobom trzecim pod żadnym pozorem. Niezależnie od wymuszenia zmiany hasła przez system teleinformatyczny użytkownik ma obowiązek dokonywania zmiany przynajmniej co 90 dni. W każdym przypadku, gdy hasło zostało ujawnione osobie trzeciej, osoba upoważniona do przetwarzania danych jest zobowiązana do jego zmiany.
10. Nie można ingerować w oprogramowanie i konfigurację powierzonego sprzętu informatycznego. Wszelkie konieczne zmiany – w tym aktualizacje oprogramowania systemowego i antywirusowego, jeżeli nie są dokonywane automatycznie, należy zgłaszać Administratorowi systemu informatycznego.
11. Zabrania się instalowania na powierzonym sprzęcie programów komputerowych pochodzących z niewiadomego lub nielegalnego źródła, bez pozyskania uprawnienia do korzystania z oprogramowania (licencji).
12. Osoby upoważnione do przetwarzania danych osobowych powinny przestrzegać swoich uprawnień w systemie informatycznym i zgodnie z tymi uprawnieniami korzystać z baz danych. Należy korzystać tylko z własnego

identyfikatora i hasła, nie przekazywać swojego hasła innym pracownikom i nie pozyskiwać hasła innych pracowników oraz należy stosować się do zaleceń Inspektora ochrony danych.

13. Podczas przetwarzania danych osobowych można opuścić stanowisko pracy dopiero po aktywizowaniu wygaszacza ekranu blokującego pracę komputera lub po zablokowaniu stacji roboczej.
14. Obowiązuje zakaz wykonywania kopii zbiorów danych osobowych lub ich części, za wyjątkiem jednoznacznego upoważnienia.
15. W przypadku koniecznego transferu danych osobowych konieczne jest podjęcie czynności zapewniających ochronę danych, takich jak ich pseudoanonimizacja, szyfrowanie komunikacji elektronicznej (e-mail) lub szyfrowanie pliku i przekazanie hasła innym kanałem komunikacyjnym (np. SMS, informacja telefoniczna).
16. Służbowa poczta elektroniczna może być wykorzystywana wyłącznie do celów służbowych. Niedopuszczalne jest wykorzystywanie poczty służbowej do celów prywatnych. Zabronione jest również wykorzystywanie prywatnej poczty elektronicznej do celów służbowych.
17. Niedozwolone jest kopiowanie danych osobowych na dyski komputerów i inne nośniki.
18. Kopie zasobów informacyjnych wykonywane są zgodnie z przyjętymi zasadami, za co odpowiada Administrator systemu informatycznego.
19. Pracę na stacji roboczej należy zakończyć po zapisaniu przetwarzanych danych w sposób właściwy dla wykorzystywanego systemu, a następnie prawidłowym wylogowaniu się z konta użytkownika i uśpieniu lub wyłączeniu komputera.

IV. Reguły postępowania dotyczące przetwarzania danych osobowych w tradycyjnych zbiorach danych i w systemach informatycznych i na cyfrowych nośnikach informacji

1. Osoby postronne nie mogą przebywać w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych.
2. Należy zachować poufność przetwarzanych danych osobowych, w tym także wobec osób najbliższych.
3. Należy zamykać okna w czasie opadów, silnych wiatrów i w innych sytuacjach, które mogłyby zagrozić bezpieczeństwu danych osobowych.
4. Należy zamykać okna przed opuszczeniem pomieszczenia, w szczególności po zakończeniu dnia pracy.
5. Klucze do pomieszczeń, w których przetwarzane są dane osobowe każdorazowo są pobierane z portierni; zabrania się wytwarzania, posiadania i używania kopii kluczy.
6. Należy zamykać na klucz drzwi pomieszczeń po ich całkowitym opuszczeniu; po zakończeniu dnia pracy. Klucz należy zwrócić pracownikowi portierni. Jeśli przed zakończeniem dnia pracy niemożliwe jest umieszczenie wszystkich dokumentów zawierających dane osobowe w zamykanych szafach, należy powiadomić o tym kierownika komórki organizacyjnej, który zgłasza osobom

sprzątającym jednorazową rezygnację z wykonania usługi sprzątania. W takim przypadku także należy zostawić klucz pracownikowi portierni.

7. Wszelkie naruszenia związane z bezpieczeństwem danych osobowych muszą być zgłaszane Inspektorowi ochrony danych.

REKTOR

Prof. Jerzy Posłuszny