Regulamin Ochrony Danych Osobowych

1. Uprawnionymi do przetwarzania danych osobowych mogą być osoby, które odbyły szkolenie z zakresu ochrony danych osobowych, złożyły oświadczenie o przeszkoleniu i zachowaniu poufności oraz otrzymały stosowne upoważnienie do przetwarzania danych osobowych. Przetwarzanie danych osobowych bez upoważnienia jest niezgodne z prawem.
2. Upoważnienia do przetwarzania danych osobowych dla osób przetwarzających te dane na innej podstawie niż umowa o pracę (np. umowy cywilnoprawnej, umowy stażowej, porozumienia ws. praktyk studenckich, zatrudnienia w projektach itp.) wydawane są zgodnie z procedurami obowiązującymi u Administratora.
3. Za bezpieczeństwo przetwarzanych danych osobowych odpowiedzialny jest każdy pracownik oraz kierownicy poszczególnych jednostek organizacyjnych. Wszyscy zobowiązani są do przestrzegania procedur bezpieczeństwa oraz do zachowania poufności danych i sposobów ich zabezpieczania, także po ustaniu stosunku pracy lub współpracy.
4. Każda osoba przetwarzająca dane osobowe zobowiązana jest do regularnego uczestnictwa w szkoleniach z zakresu ochrony danych osobowych.
5. Zabronione jest kopiowanie i wynoszenie dokumentów służbowych oraz ich przesyłanie drogą elektroniczną w celu innym niż służbowy.
6. Do korespondencji służbowej należy używać tylko służbowej skrzynki mailowej.
7. Przed wysłaniem wiadomości należy dokładnie zweryfikować adresata oraz treść przesyłanych dokumentów.
8. Korespondencję seryjną należy wysyłać z użyciem opcji „UDW”.
9. Zaleca się stosowanie szyfrowania dysków, plików, transmisji oraz nośników zawierających dane osobowe, w tym również służbowych telefonów komórkowych. Wysyłając dokumenty za pomocą skrzynki e-mail należy stosować odpowiednie zabezpieczenia, np. szyfrowanie lub zabezpieczenie hasłem wysłanym innym źródłem.
10. Praca w systemach informatycznych odbywa się na kontach przypisanych danemu użytkownikowi. Zabronione jest udostępnianie haseł innym osobom. Nie zaleca się włączania opcji autouzupełniania oraz zapamiętywania haseł w przeglądarkach internetowych.
11. Hasła dostępu do kont i systemów należy ustalać zgodnie z polityką haseł.
12. Nie należy instalować i korzystać z programów pochodzących z niesprawdzonych źródeł.
13. Podczas odbierania poczty elektronicznej (e-mail) należy zwracać szczególną uwagę na załączniki pochodzące od nieznanych nadawców, mogą bowiem zawierać złośliwe oprogramowanie. W razie wątpliwości należy wstrzymać się z otwieraniem załącznika i skontaktować z osobą odpowiedzialną za obsługę informatyczną.
14. W przypadku podłączenia urządzeń lub nośników zewnętrznych, konieczne jest ich uprzednie sprawdzenie pod kątem potencjalnych zagrożeń. Nie wolno korzystać z nośników z nieznanego źródła, np. znalezionych, podarowanych.
15. Przed opuszczeniem pomieszczenia należy zablokować komputer. W przypadku dłuższej nieobecności w pomieszczeniu konieczne jest wylogowanie z systemu.
16. Osoby nieuprawnione nie mogą pozostać same w pomieszczeniu pod nieobecność pracownika. Przy każdorazowym opuszczeniu pomieszczenia drzwi należy zamknąć na klucz.

17. Nie należy pozostawiać dokumentów papierowych ani nośników danych bez nadzoru. Po zakończonej pracy wszystkie dokumenty i nośniki danych powinny zostać odpowiednio zabezpieczone. W przypadku, w którym sprzątanie pomieszczeń, w których przetwarzane są dane osobowe, odbywa się poza godzinami pracy, dostęp do danych osobowych powinien zostać uniemożliwiony poprzez umieszczenie ich w szafie zamykanej na klucz – zasada czystego biurka.
18. Dokumenty zawierające dane osobowe powinny być zabierane z drukarek zaraz po ich wydrukowaniu. W szczególności zasada ta dotyczy dokumentów drukowanych na drukarkach znajdujących się w innym pomieszczeniu.
19. Niszczenie dokumentów zawierających dane osobowe zawsze powinno odbywać się za pomocą niszczarek. Zabronione jest wyrzucanie do kosza dokumentów lub elektronicznych nośników zawierających dane osobowe. Jeżeli konieczne jest jednorazowe zniszczenie większej ilości dokumentów, należy skontaktować się z kierownikiem obiektu, w celu ustalenia terminu ich utylizacji przez firmę zewnętrzną.
20. Żadnych dokumentów zawierających dane osobowe nie należy umieszczać w miejscach, do których wgląd lub dostęp mogą mieć osoby nieupoważnione. Podczas obsługi interesanta należy zwrócić uwagę, czy nie ma on możliwości wglądu do dokumentów z danymi osobowymi leżącymi np. na biurku lub wyświetlonymi na monitorze komputera. Ekran komputera powinien być ustawiony tak, by uniemożliwić wgląd osobom nieuprawnionym.
21. Zaleca się ustalenie „strefy bezpieczeństwa” w pomieszczeniach, w których dokonywana jest obsługa interesanta, w taki sposób, aby uniemożliwić osobom nieupoważnionym pozyskanie informacji na temat danych osoby obsługiwanej. Dane osobowe, np. zawarte w dowodzie tożsamości nie powinny być odczytywane na głos.
22. Niedozwolone jest kopiowanie, skanowanie i czasowe zatrzymywanie dowodów tożsamości.
23. Oceny z egzaminów powinny być udostępniane studentom indywidualnie poprzez system USOS. Niedopuszczalne jest, aby wgląd do ocen poszczególnych osób mieli wszyscy studenci.
24. Każde naruszenie ochrony danych osobowych (czyli naruszenie bezpieczeństwa mogące prowadzić do przypadkowego lub niezgodnego z prawem przetwarzania danych osobowych) lub postępowanie niezgodne w niniejszym Regulaminem należy niezwłocznie zgłosić bezpośredniemu przełożonemu oraz Inspektorowi Ochrony Danych.
    Zgłoszenie powinno zawierać opis działania wskazującego na naruszenie ochrony danych osobowych, określenie miejsca oraz czasu w jakim nastąpiło naruszenie, informację czy podjęto jakieś działania korygujące oraz dane kontaktowe osoby zgłaszającej naruszenie.