Zasady ochrony danych osobowych

24.02.2020

1. Możesz przetwarzać dane osobowe wyłącznie w zakresie i celu związanym z wykonywaniem przez Ciebie obowiązków służbowych lub zadań związanych z realizowaniem umowy, będącej podstawą Twojej współpracy z Narodową Agencją Wymiany Akademickiej (NAWA). Nie możesz wykorzystywać danych osobowych dla celów prywatnych.
2. W związku z dostępem do danych osobowych (imion, nazwisk, numerów PESEL, danych kontaktowych itd.) obowiązuje Cię ochrona danych osobowych. Oznacza to, że spoczywa na Tobie obowiązek:
    a) zabezpieczenia tych danych osobowych przed dostępem osób nieupoważnionych,
    b) zabezpieczenia ich przed zniszczeniem lub uszkodzeniem,
    c) zachowania ich w poufności w toku współpracy z NAWA i po jej zakończeniu.
3. Nie przekazuj danych osobom nieupoważnionym (np. bez zweryfikowania ich tożsamości lub uprawnień) ani nie postępuj w sposób, który może spowodować naruszenie poufności (np. podsłuchanie rozmowy w miejscu publicznym lub zabranie pozostawionych bez opieki dokumentów).
4. Pobyt osób postronnych w obszarze przetwarzania danych osobowych (pomieszczenia biurowe, archiwum, serwerownia itp.) jest dopuszczalny jedynie w obecności upoważnionego personelu. Dotyczy to wszystkich pomieszczeń, w których przechowywane są dokumenty lub nośniki z danymi osobowymi.
5. Jeżeli musisz opuścić pomieszczenie, gdzie przechowuje się dane osobowe w formie papierowej lub elektronicznej, pamiętaj o zamknięciu drzwi na klucz (lub ich zabezpieczeniu w inny sposób). Zabronione jest pozostawianie kluczy w zamkach w warunkach, w których mogą do nich uzyskać dostęp osoby nieupoważnione.
6. Nie zostawiaj osoby postronnej (np. gościa, kuriera) samej w pomieszczeniu, gdzie przechowuje się dane osobowe. Poproś inną osobę upoważnioną o pomoc lub, gdy nie jest to możliwe, poproś osobę postronną o zaczekanie na korytarzu.
7. Nie pozostawiaj dokumentacji bez nadzoru. Zabrania się pozostawiania dokumentacji w ogólnodostępnych miejscach bez nadzoru (np. korytarze, pomieszczenia niezamykane na klucz).
8. Nie wyrzucaj papierowych dokumentów, zawierających dane osobowe lub informacje poufne, do koszy, kartonów, kontenerów itp. – zawsze używaj niszczarki.

9. Po zakończeniu pracy chowaj wszystkie dokumenty i nośniki danych (dyski, pendrive'y, płyty CD) do szuflad, szafek lub szaf zamykanych na klucz. Klucze te przechowuj w ustalonym miejscu, niedostępnym dla osób nieupoważnionych, w tym personelu sprzątającego (zasada „czystego biurka").
10. Rozpoczynając pracę w aplikacji, programie lub systemie IT, użyj indywidualnego loginu i hasła (lub innego zabezpieczenia, uzgodnionego z działem IT). Odchodząc od komputera nawet na chwilę, pamiętaj o jego zablokowaniu (w systemie Windows służy temu kombinacja klawiszy **Win+L**).
11. Login i hasło mają służyć wyłącznie Tobie. Zachowaj je w poufności! Nie zapisuj swojego hasła ani udostępniaj go osobom trzecim, nawet współpracownikom, informatykowi ani bezpośredniemu przełożonemu.
12. Upewnij się, że monitor Twojego komputera jest tak ustawiony, by osoby postronne nie widziały tego, co jest wyświetlane na ekranie. Dotyczy to także innych urządzeń przenośnych, używanych w miejscach publicznych (kawiarnie, poczekalnie, pociągi itd.)
13. Zmieniaj swoje hasło dostępu do programu minimum raz na 90 dni, nawet jeżeli program automatycznie nie wymusza takiej zmiany.
14. Pamiętaj, aby Twoje hasło dostępu składało się z minimum 8 znaków, przynajmniej jednej wielkiej i jednej małej litery oraz z przynajmniej jednej cyfry lub jednego znaku specjalnego.
15. Jeżeli stwierdzisz lub podejrzewasz, że doszło do naruszenia bezpieczeństwa danych osobowych, niezwłocznie powiadom bezpośredniego przełożonego lub Inspektora Ochrony Danych (IOD). Do naruszenia bezpieczeństwa mogą prowadzić np. następujące sytuacje:
    a) ślady włamania na drzwiach, oknach lub szafach,
    b) wyrzucenie do śmieci dokumentacji w stanie niezniszczonym,
    c) fizyczna obecność w budynku osób zachowujących się podejrzanie,
    d) udostępnienie danych osobowych osobom nieupoważnionym,
    e) próby wyłudzenia danych osobowych (np. podszywanie się pod inną osobę),
    f) kradzież lub zagubienie dokumentacji papierowej albo nośnika danych z danymi osobowymi.

W razie pytań lub wątpliwości dotyczących ochrony danych osobowych skontaktuj się z Adamem Klimowskim, Inspektorem Ochrony Danych NAWA, pod adresem e-mail odo@nawa.gov.pl.