UNIWERSYTET WARSZAWSKI

Inspektor Ochrony Danych

Warszawa, dnia 15 lutego 2021 roku

DOZI-W-01/2021

Wskazówki Inspektora Ochrony Danych dotyczące przetwarzania danych osobowych podczas wykonywania pracy zdalnej

Wersja 1.0.1

ul. Krakowskie Przedmieście 26/28, 00-927 Warszawa
tel.: 22 55 22 042
e-mail: iod@adm.uw.edu.pl

UWAGA!
Wskazówki Inspektora Ochrony Danych nie stanowią prawa powszechnie obowiązującego natomiast są dobrymi praktykami w zakresie należytego przetwarzania danych osobowych i informacji.

I. Warunki jakie musi spełniać miejsce wykonywania pracy zdalnej

1. Pracownik musi zapewnić warunki umożliwiające mu skuteczną pracę zdalną z zachowaniem właściwego poziomu bezpieczeństwa informacji.
2. Niedozwolone jest podejmowanie pracy zdalnej w miejscach publicznych, jak kawiarnie, restauracje, galerie handlowe, gdzie osoby postronne mogłyby usłyszeć fragmenty służbowych rozmów lub zapoznać się z dokumentami związanymi z wykonywaną pracą.
3. Pracując w domu należy zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera oraz telefonu, a także zapewnienie pracy z dokumentami w sposób uniemożliwiający wgląd domowników w ich treść.
4. Praca zdalna powinna odbywać się zgodnie z harmonogramem ustalonym z pracodawcą, co oznacza, że pracownik jest dostępny i realizuje swoje działania w ustalonych godzinach.
5. Odchodząc od komputera lub kończąc korzystanie z telefonu należy upewnić się, że urządzenie zostało zablokowane.

II. Bezpieczeństwo pracy zdalnej

1. Każdy pracownik wykonujący pracę zdalną powinien posiadać służbowe konto e-mail oraz upoważnienie do przetwarzania danych osobowych oraz uczestniczyć w szkoleniu z ochrony danych osobowych.
2. Dane służbowe bez względu na ich formę powinny być zawsze odseparowane od danych prywatnych.
3. Materiały dydaktyczne udostępniane za pośrednictwem Internetu powinny zostać oznaczone przez autora informacją o pochodzeniu oraz nie mogą naruszać praw autorskich innych osób lub podmiotów.
4. Materiały dydaktyczne udostępniane studentom i pracownikom w ramach systemów umożliwiających pracę zdalną i wideokonferencje podlegają ochronie prawnej, w szczególności przewidzianej w przepisach o prawie autorskim i prawach pokrewnych.
5. Naruszenia bezpieczeństwa informacji należy zgłaszać do Działu Organizacji Zasobów Informacyjnych za pośrednictwem formularza na stronie: https://odo.uw.edu.pl/zglaszanie-naruszen-ochrony-danych/.
6. Przed rozpoczęciem pracy należy zweryfikować czy miejsce zdalnego łączenia spełnia odpowiednie warunki bezpieczeństwa np. łączenie z zabezpieczoną siecią Wi-Fi.
7. Należy wydzielić sieć Wi-Fi wyłącznie przeznaczoną do pracy zdalnej. Dostęp do sieci powinien być zabezpieczony skomplikowanym hasłem i jeżeli to możliwe należy włączyć szyfrowanie WPA2.
8. Należy zmienić domyślne hasło administratora do panelu sterowania routerem.
9. Należy na bieżąco aktualizować system operacyjny oraz oprogramowanie wykorzystywane do pracy zdalnej w tym oprogramowanie antywirusowe.
10. Należy wykorzystywać oprogramowanie pochodzące z legalnych źródeł. Zabronione jest przetwarzanie danych służbowych z wykorzystaniem nieautoryzowanego oprogramowania.
11. W przypadku korzystania z prywatnego komputera, zaleca się aby zapewniał on odrębne profile użytkowników chronione hasłem.
12. Należy unikać korzystania z nieznanych i przypadkowych stron internetowych.

13. Zabrania się otwierania załączników z nieznanych źródeł dostarczanych pocztą elektroniczną.
14. Nie należy stosować tych samych haseł w różnych systemach teleinformatycznych.
15. Nie należy logować się do uczelnianych systemów informatycznych w przypadkowych miejscach z niezaufanych urządzeń lub publicznych niezabezpieczonych sieci Wi-Fi.
16. Należy regularnie wykonywać kopie zapasowe.
17. Należy szyfrować dane osobowe i inne informacje chronione przesyłane pocztą elektroniczną.
18. Należy szyfrować dyski twarde w komputerach przenośnych i inne nośniki wymienne, na których przechowywane są dane niezbędne do wykonywania pracy zdalnej.
19. Przy pracy zdalnej należy korzystać z szyfrowanego połączenia VPN. Korzystanie z VPN należy zgłosić zgodnie z zasadami określonymi na stronie: https://it.uw.edu.pl/pl/uslugi/UslugiInternetVPN.
20. Należy blokować komputer za każdym razem kiedy zamierza się opuścić stanowisko pracy.
21. Należy korzystać z automatycznego blokowania komputera po krótkim czasie bezczynności.
22. Przy wykonywaniu zadań służbowych należy unikać uruchamiania aplikacji do celów prywatnych aby zredukować ryzyko omyłkowego udostępnienia danych.
23. Nie należy korzystać z nośników danych nieznanego pochodzenia.
24. Problemy w działaniu sprzętu lub oprogramowania należy niezwłocznie zgłaszać informatykom w jednostkach organizacyjnych lub do właściwej jednostki IT.

III. Bezpieczeństwo fizyczne i osobowe

1. Sprzęt wykorzystywany do pracy zdalnej należy przechowywać w nadzorowanym miejscu i nie pozostawiać go bez opieki.
2. Po zakończonej pracy sprzęt wykorzystywany do pracy zdalnej należy zabezpieczyć przed możliwością skorzystania przez osoby nieuprawnione.
3. Wydruki dokumentów służbowych na urządzeniach prywatnych należy zabezpieczyć zaraz po wydrukowaniu i nie pozostawiać ich w urządzeniu.
4. Nie należy wykonywać zdjęć dokumentów służbowych za pomocą prywatnych telefonów.
5. Rozmowy telefoniczne lub wideokonferencje powinny odbywać się w sposób który uniemożliwia zapoznanie się z omawianymi treściami przez osoby postronne.
6. Przewożenie dokumentów między siedzibą pracodawcy a miejscem wykonywania pracy zdalnej wymaga zachowania ostrożności i należytego zabezpieczenia dokumentów przed przypadkową utratą i wglądem przez osoby nieuprawnione.
7. Praca na dokumentach nie może odbywać się w miejscu publicznym.
8. Po zakończeniu pracy zdalnej wszystkie dokumenty wytworzone w ramach jej wykonywania należy przekazać pracodawcy.
9. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie w dniu zdarzenia zgłosić zdarzenie do kierownika jednostki organizacyjnej, Inspektora Ochrony Danych, a także informatyka w jednostce organizacyjnej lub właściwej jednostki IT.

IV. Zasady prowadzenia wideokonferencji

1. Wideokonferencje prowadzi się z wykorzystaniem narzędzi informatycznych autoryzowanych i udostępnianych przez Uniwersytet lub przez podmiot będący gospodarzem wideokonferencji.
2. Uczestnicząc w wideokonferencjach należy zadbać, aby obszar objęty transmisją obrazu zapewniał prywatność uczestnika.
3. W przypadku czasowego opuszczenia wideokonferencji należy się z niej rozłączyć lub wyłączyć kamerę i mikrofon na czas nieobecności.

4. Nagrywanie wideokonferencji musi być prawnie uzasadnione i nie może naruszać praw i wolności osób, których dane dotyczą.
5. Prowadzący wideokonferencję informuje uczestników o jej nagrywaniu przed rozpoczęciem nagrania.
6. Udostępniając pulpit własny innym uczestnikom należy upewnić się, że nie zostaną udostępnione informacje służbowe w tym podlegające ochronie.
7. Przed rozpoczęciem wideokonferencji o ile to możliwe należy ustawić ochronę hasłem spotkania online.
8. Logując się do wideokonferencji, należy wyłączyć kamerę i mikrofon.
9. Po zakończeniu wideokonferencji należy wyłączyć kamerę i mikrofon, upewnić się że spotkanie online zostało zakończone, a aplikacja została zamknięta i nie działa w tle.
10. Na potrzeby połączeń wideokonferencyjnych wykorzystuje się:
    1) ogólnouczelniane aplikacje stanowiące funkcjonalność platformy e-learningowej (np. BigBlueButton);
    2) ogólnouczelniane aplikacje od dostawców z którymi Uniwersytet ma zawarte umowy o świadczenie usług w tym stosowne umowy powierzenia przetwarzania danych osobowych (https://it.uw.edu.pl/pl/praca-zdalna/);
    3) aplikacje wykorzystywane przez jednostki organizacyjne Uniwersytetu Warszawskiego o ile zostały uregulowane kwestie licencyjne i spełniają standardy RODO.

V. Bezpieczeństwo urządzeń mobilnych

1. Urządzenie mobilne powinno być zabezpieczone co najmniej blokadą ekranu i/lub innym mechanizmem kontroli dostępu.
2. Urządzenie mobilne powinno znajdować się pod stałym nadzorem pracownika.
3. W zakresie urządzeń mobilnych zabrania się w szczególności:
    1) pozostawiania urządzeń mobilnych bez nadzoru;
    2) synchronizacji urządzeń z kontem prywatnym;
    3) udostępniania urządzeń osobom trzecim;
    4) przechowywania danych służbowych w tzw. usługach chmurowych na serwerach nieautoryzowanych przez Uniwersytet;
    5) nagrywania rozmów służbowych bez uprzednio uzyskanej zgody;
    6) przechowywania w pamięci urządzenia danych chronionych.

VI. Przesyłanie danych osobowych z wykorzystaniem poczty elektronicznej

1. Przesyłanie danych osobowych np. studentów/pracowników powinno odbywać się z wykorzystaniem szyfrowania plików.
2. Przed wysyłką pliku z danymi osobowymi lub innymi informacjami wymagającymi ochrony należy go uprzednio zaszyfrować.
3. Wskazówki dot. szyfrowania plików znajdują się na stronie: https://odo.uw.edu.pl/wp-content/uploads/sites/10/2020/03/praca-zdalna-poradnik.pdf
4. Przed wysyłką maila należy upewnić się czy został podany właściwy adres e-mail adresata.
5. Hasła do plików należy przekazywać inną formą kontaktu np. telefonicznie, sms lub wiadomość mail na inny adres odbiorcy.

VII. Działania niedozwolone

Za działanie niedozwolone należy uznać:

1) udostępnianie osobom trzecim danych służących do uwierzytelniania do systemów i usług wewnętrznych Uniwersytetu Warszawskiego;
2) przekazywanie informacji chronionych, w szczególności danych osobowych bez zabezpieczenia hasłem, w szczególności w treści wiadomości elektronicznej;
3) przekazywanie hasła do zabezpieczonych informacji tą samą drogą komunikacji, którą przekazywany jest zabezpieczony hasłem plik lub pliki;
4) dzielenie się poufnymi informacjami służbowymi z osobami trzecimi w tym z domownikami;
5) logowanie na konta innych pracowników;
6) niezwrócenie dokumentów służbowych do siedziby pracodawcy po zakończeniu pracy zdalnej.