2020

OCHRONA DANYCH OSOBOWYCH PODCZAS PRACY ZDALNEJ

PORADNIK

UNIWERSYTET HUMANISTYCZNO-PRZYRODNICZY
IM. JANA DŁUGOSZA W CZĘSTOCHOWIE

30.04.2020

- Pracując zdalnie, można przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.

- Należy pamiętać o bezpiecznym korzystaniu z komputerów i innych urządzeń zarówno wtedy, gdy zapewnił je pracodawca, jak i wtedy, gdy korzysta się z własnego sprzętu komputerowego.

- RODO nie zabrania wykorzystywania prywatnego komputera, tabletu czy telefonu do przetwarzania danych osobowych w związku z pracą zdalną. Urządzenia te muszą być jednak odpowiednio zabezpieczone, a pracownik powinien postępować zgodnie z polityką bezpieczeństwa wprowadzoną w tym zakresie w Uczelni.

- Jeżeli używamy własnego urządzenia, powinniśmy samodzielnie spełnić podstawowe wymogi bezpieczeństwa. Przede wszystkim należy sprawdzić, czy wykorzystywane urządzenie ma aktualny system operacyjny, czy używane są na nim programy antywirusowe, czy dokonane są niezbędne aktualizacje.

- Na bieżąco aktualizowane powinny być także zainstalowane programy antymalware i antyspyware. Należy rozważnie instalować na swoich urządzeniach oprogramowanie i pobierać je tylko z wiarygodnych źródeł (ze stron producentów).

- Przechowując dane na sprzęcie, do którego mogą mieć dostęp inne osoby, należy używać mocnych haseł dostępowych, a przed odejściem od stanowiska pracy urządzenie powinno zostać zablokowane.

- Zalecane jest także skonfigurowanie automatycznego blokowania komputera po pewnym czasie bezczynności oraz założenie odrębnych kont użytkowników w przypadku korzystania z komputera przez wiele osób.

- Podczas korzystania z programów lub aplikacji mobilnych należy korzystać z możliwych do zastosowania w nich mechanizmów ochrony prywatności użytkowników.

- Jeśli użycie jakiegoś programu wymaga logowania, warto zadbać o silne hasło dostępu, a dodatkowo chronić je przed utratą czy dostępem osób nieuprawnionych.

- Gdy dane są przechowywane na urządzeniach przenośnych (np. pamięć USB), muszą być bezwzględnie szyfrowane i chronione hasłem, by zapewnić odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.

- Jeśli przenośne urządzenie zostało skradzione, trzeba natychmiast podjąć odpowiednie kroki, aby, o ile to możliwie, zdalnie wyczyścić jego pamięć.

- Prowadzenie zajęć zdalnych może wymagać korzystania przez pracowników z poczty elektronicznej do kontaktu ze studentami. Pracownik powinien prowadzić taką korespondencję ze służbowej skrzynki pocztowej.

- Jeżeli pracownik wykorzystuje do celów służbowych prywatną skrzynkę pocztową musi pamiętać, aby korzystać z niej w sposób rozważny i bezpieczny.

- Szczególną uwagę trzeba zwrócić na zabezpieczenie danych osobowych udostępnianych w przesyłanych wiadomościach.

- Zawsze przed wysłaniem wiadomości, należy upewnić się, czy niezbędne jest wysłanie danych osobowych oraz czy wysyłamy je do właściwego adresata.

- Ponadto trzeba sprawdzić, czy w nazwie adresu e-mail adresata nie ma np. przestawionych lub pominiętych znaków tak, aby nie wysłać takiej wiadomości do osób nieupoważnionych.

- Podczas wysyłania korespondencji zbiorczej poza Uczelnię powinno się korzystać z opcji „UDW", dzięki której odbiorcy wiadomości nie będą widzieć wzajemnie swoich adresów e-mail.

- Należy dokładnie sprawdzić nadawcę maila. Nie otwierać wiadomości, a zwłaszcza załączników, od nieznanych adresatów oraz nie klikać w link zawarty w takiej wiadomości. To może być atak phishingowy.

- Nie należy przesyłać mailem informacji zaszyfrowanej razem z hasłem. Nawet w osobnej wiadomości. Ten, kto ma dostęp do Twojej poczty bez problemu odszyfruje wiadomość.

- Jeżeli prywatny sprzęt komputerowy, na którym przetwarzane były służbowe dane osobowe uległ uszkodzeniu, przed skorzystaniem z usług zewnętrznego serwisanta należy się skontaktować z Działem Infrastruktury Informatycznej Uczelni.

- Zawsze przy wyborze aplikacji lub innych narzędzi wykorzystywanych do zdalnej edukacji bądź komunikacji ze studentami należy się zastanowić, czy jest niezbędne, aby przetwarzały one dane osobowe, a jeżeli tak, czy można zminimalizować ich zakres bądź wykorzystywać tylko pseudonimy (np. pierwsza litera imienia itp.). Należy także sprawdzić zasady świadczenia usługi i zasady przetwarzania danych przez usługodawcę (politykę prywatności).

- Na ogólnie dostępnych portalach lub stronach internetowych pracownik może jedynie publikować materiały edukacyjne, natomiast nie może przetwarzać danych osobowych studentów.

- W celu sprawdzania i monitorowania obecności studentów na zajęciach prowadzonych zdalnie pracownik powinien zachować proporcjonalność i minimalizację danych. Np. nie może w tym celu korzystać z narzędzi zbierających dane biometryczne, w tym wykorzystujących systemy wykrywania twarzy.

- Pracownik powinien zadbać o bezpieczne archiwizowanie przetwarzanych danych osobowych.

- Dokumenty papierowe powinny być zabezpieczone w zamykanych szufladach bądź szafach i chronione przed zniszczeniem.

W opracowaniu korzystano z:
https://www.gov.pl/web/edukacja/zdalne-nauczanie-uodo
https://uodo.gov.pl/pl/138/1459