Newsletter Ochrony Danych Osobowych - 3/2020

- Janusz Wyspiański (Inspektor Ochrony Danych Osobowych)

TEMAT: „Ochrona danych osobowych podczas pracy zdalnej”.

Jak postępować podczas pracy zdalnej, aby nie naruszyć przepisów o ochronie danych? Jakie zabezpieczenia rekomendować pracownikom?

……

I. URZĄDZENIA KOMPUTEROWE

- Urządzenia i oprogramowanie przekazane przez pracodawcę do pracy zdalnej służą do wykonywania obowiązków służbowych dlatego też należy postępować zgodnie z przyjętą w organizacji procedurą bezpieczeństwa (Polityka Bezpieczeństwa Informacji, Instrukcja Zarządzania Systemem Informatyczny).
- Nie można instalować dodatkowych aplikacji i oprogramowania niezgodnych z procedurą bezpieczeństwa, a jeżeli nie wiemy czy aplikacja jest bezpieczna należy skontaktować się ze swoim informatykiem lub inspektorem ochrony danych osobowych.
- Należy upewnić się, że wszystkie urządzenia z jakich korzystamy mają niezbędne aktualizacje systemu operacyjnego, oprogramowania oraz systemu antywirusowego. W razie wątpliwości należy skontaktować się ze swoim informatykiem lub inspektorem ochrony danych osobowych.
- Zanim przystąpimy do pracy, należy wydzielić sobie odpowiednią przestrzeń, tak aby ewentualne osoby postronne, nie miały dostępu do dokumentów, nad którymi pracujemy. Odchodząc od stanowiska pracy każdorazowo należy blokować urządzenie, na którym pracujemy !!!.
- Należy zabezpieczyć swój komputer poprzez używanie silnych haseł dostępu lub wielopoziomowego uwierzytelniania. Pozwoli to na ograniczenia dostępu do urządzenia, a jednocześnie na ograniczenia ryzyka utraty danych w przypadku kradzieży lub zgubienia urządzenia co jest obowiązkiem każdego pracownia.
  W razie wątpliwości należy skontaktować się ze swoim informatykiem lub inspektorem ochrony danych osobowych.
- **Należy podejmować szczególne środki ostrożności, aby urządzenia z których korzystamy podczas pracy, szczególnie te wykorzystywane do przenoszenia danych, jak pendrive i dyski zewnętrzne nie zostały zgubione. !!!**
- Jeśli zgubiono urządzenie, na którym pracujemy lub zostało skradzione natychmiast należy podjąć kroki a w tym przede wszystkim powiadomić Inspektora Ochrony Danych – januszwyspianski@abi24.eu, +48 600 246 497 !!!

  oraz o ile jest to możliwie, zdalnie wyczyścić jego pamięć !!

II. POCZTA ELEKTRONICZNA - EMAIL, KOMUNIKACJA ZDALNA, MEETING.

- Należy przede wszystkim używać służbowych kont email.
  Jeśli pracujemy i przetwarzamy dane osobowe i musimy używać prywatnego e-maila, to bezwzględnie należy upewnić się, że treść i załączniki są właściwie szyfrowane !!!.
- **Nigdy nie można używać danych osobowych lub poufnych informacji w temacie wiadomości i otwartym tekście w wiadomości... !!!**
- Przed wysłaniem wiadomości mail należy upewnić się, że wysyłamy go do właściwego adresata, zwłaszcza jeśli wiadomość zawiera dane osobowe lub dane wrażliwe. !!!
- Kiedy otrzymujemy wiadomość e-mail, należy dokładnie sprawdzić nadawcę !!!
- Nie można otwierać wiadomości od nieznanych adresatów, a zwłaszcza nie można otwierać załączników oraz klikać w link zawarty w takiej wiadomości.
  To może być atak phishingowy - CYBERATAK, doprowadzający do wycieku danych osobowych i w konsekwencji naruszenia skutkującego kontrolą organu nadzorczego, nałożeniem kary przez Urząd Ochrony Danych Osobowych.
- Nie można przesyłać mailem informacji zaszyfrowanej razem z hasłem. Nawet w osobnej wiadomości. Ten kto ma dostęp do Twojej poczty bez problemu odszyfruje wiadomość.

III. DOSTĘP DO SIECI I CHMURY

- Należy używać tylko zaufanego dostępu do sieci lub chmury (internet) oraz przestrzegać wszelkich zasad i procedur dotyczących logowania i udostępniania danych.
- Obowiązkiem każdego jest zadbanie do bezpieczne przechowywanie i archiwizowanie tworzonych zbiorów danych, jeżeli pracujemy lokalnie bez automatycznej kopii danych np. w chmurze.

Z poważaniem.
Janusz Wyspiański

ŹRÓDŁO DANYCH:

Strona internetowa UODO (uodo.gov.pl). https://uodo.gov.pl/pl/138/1459