Newsletter Ochrony Danych Osobowych - 10/2020

- Janusz Wyspiański (Inspektor Ochrony Danych Osobowych)

TEMAT: „Wyzwania w świetle zagrożeń związanych z PANDEMIĄ”
- CYBERBEZPIECZEŃSTWO PRACY ZDALNEJ

……

ZADANIA i WYZWANIA DLA PRACODAWCY:

- Zapewnienie pracownikom narzędzi umożliwiających prowadzenie pracy zdalnej oraz bezpieczną komunikację z siedzibą Firmy.

- Przeprowadzenie analizy zagrożeń zawracając szczególną uwagę na bezpieczeństwo danych oraz zapewnienie odpowiednich gwarancji praw osób, których dane dotyczą.

- Zabezpieczenie danych przez zastosowanie odpowiednich środków technicznych i organizacyjnych, np. pseudonimizacja*, szyfrowanie danych*.

- Przetwarzanie danych zgodnie z zasadami określonymi w RODO – **ścisła współpraca z Inspektorem Ochrony Danych Osobowych przy wyborze środków technicznych i organizacyjnych mających być stosowanych w pracy zdalnej !!!!**

* **PSEUDONIMIZACJA** - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie, której one dotyczą, bez użycia dodatkowego „klucza”. Mówiąc prościej, to użycie zamiast np. imienia i nazwiska – liczby. Wymóg jest jeden, klucz z właściwymi danymi do odszyfrowania powinny być przechowywane osobno. Dzięki czemu nawet jeśli doszłoby do wycieku, osoba nieupoważniona niewiele by się z tych danych dowiedziała.

* **SZYFROWANIE DANYCH** - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie, której one dotyczą, bez użycia dodatkowego „klucza”. Mówiąc prościej, to użycie zamiast np. imienia i nazwiska – liczby. Wymóg jest jeden, klucz z właściwymi danymi do odszyfrowania powinny być przechowywane osobno. Dzięki czemu nawet jeśli doszłoby do wycieku, osoba nieupoważniona niewiele by się z tych danych dowiedziała.

- Jedną z metod szyfrowania danych jest **anonimizacja** polegająca na zamazywaniu niektórych danych, by pozostałe widoczne dane, nie umożliwiały ich połączenia z konkretną osobą. RODO na pierwszym miejscu, jako przykład szyfrowania danych podaje pseudonimizację, czyli rozdzielenie danych z jednego zbioru na kilka plików, tak by w jednym pliku nie znalazły się dane umożliwiające identyfikację danej osoby. Połączenie ich kluczami dopiero daje taką możliwość.

ZADANIA i WYZWANIA DLA PRACOWNIKA:

- Pracownik może korzystać z własnego laptopa podczas pracy zdalnej, ale musi zadbać o to, aby jego sprzęt był odpowiednio zabezpieczony.

- Korzystając z własnego urządzenia musi zadbać o podstawowe wymogi bezpieczeństwa (aktualny system operacyjny, programy antywirusowe, aktualizacje, instalowanie na swoich urządzeniach oprogramowania i pobierania ich tylko z wiarygodnych źródeł).

- Powinien zabezpieczyć sprzęt przed dostępem innych osób np domowników.

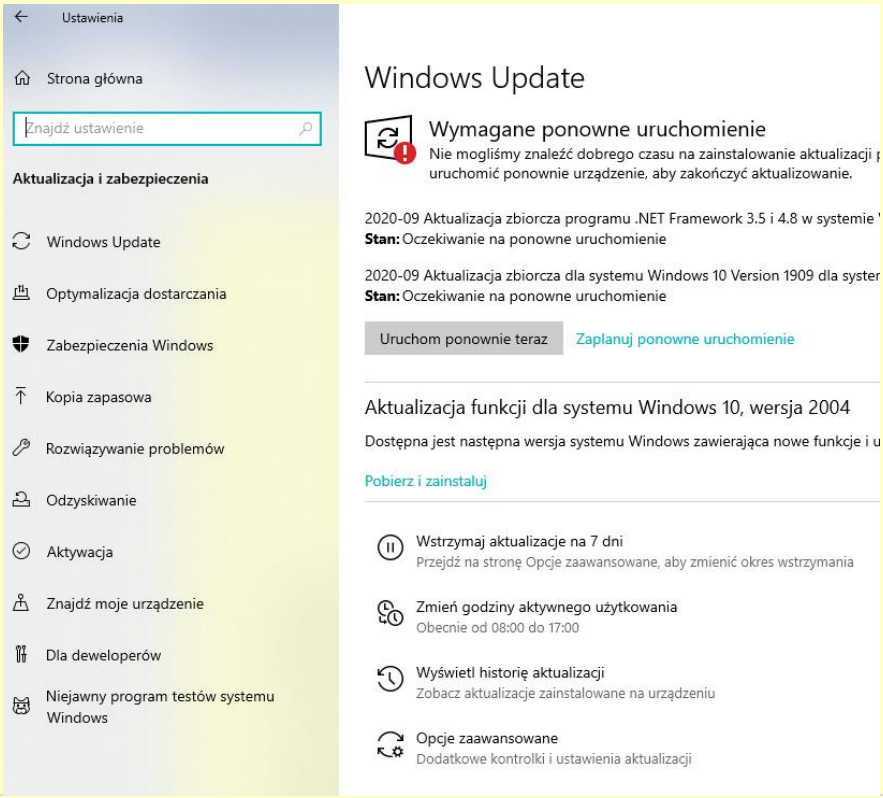
- Przechowywane dane na urządzeniach przenośnych (np. pamięć USB) powinny być zaszyfrowanie i zabezpieczone hasłem*.

* **ZABEZPIECZENIE DANYCH NA PENDRIVE** – możliwe jest stosowanie darmowego oprogramowania 7-zip do zaszyfrowania folderu, w którym znajdują się dane poufne, w ten sposób na „zwykłym" pendrive możliwe jest przechowywanie danych w zaszyfrowanych hasłem folderach, tym samym spełniając wymóg RODO dotyczących poufności i integralności danych.

Poradnik jak zaszyfrować folder w programie 7-zip znajduje się pod linkiem:

https://www.pum.edu.pl/__data/assets/pdf_file/0017/102428/instrukcja.pdf

* **AKTUALIZACJE SYSTEMU WINDOWS 10 -** aby go uruchomić należy włączyć Ustawienia i z menu głównego wybrać: Aktualizacja i zabezpieczenia.



KORZYSTANIE Z NOWOCZESNYCH TECHNOLOGI W PRACY ZDALNEJ

- Decydując się na zastosowanie jakiegoś narzędzia pomocnego np. podczas zdalnej pracy, **FIRMY powinny przy udziale swoich inspektorów ochrony danych osobowych** dokładnie **przeprowadzić analizę zagrożeń związanych z tego typu rozwiązaniami**.

- RODO, które jest neutralne technologicznie, daje dużą samodzielność administratorowi, który sam może dobierać środki oraz narzędzia, przy pomocy których przetwarza dane.

- Należy zwrócić uwagę, czy dane będą przekazywane danych do państw trzecich, np. do Stanów Zjednoczonych.

INFORMOWANIE PRACOWNIKÓW O ZAKAŻENIU KORONAWIRUSEM

- Nie ma podstaw, aby informowani byli wszyscy pracownicy, że konkretny pracownik jest zakażony, wystarczy ogólna informacja, że wystąpił przypadek zakażenia.

- Nie należy każdorazowo przyjmować, że w sytuacji wystąpienia zakażenia u jednego pracownika wszyscy pozostali pracownicy powinni czy też muszą być informowani przez pracodawcę o tym, że u konkretnego pracownika potwierdzono zakażenie.

- Współpraca służb sanitarnych z pracodawcami, analiza konkretnego przypadku, wywiad epidemiologiczny to środki jakie powinny być podejmowane przez Pracodawcę, aby przeciwdziałać rozprzestrzenianiu się Pandemii.

- Szczera rozmowa z zakażonym pracownikiem, który potwierdzi najbliższy kontakt ze współpracownikami powinna być pierwszą linią stosowania DOBROWOLNEJ KWARANTANNY – nie nakazanej przez służby epidemiologiczne.

Z poważaniem.
Janusz Wyspiański

ŹRÓDŁO DANYCH:

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