**Dane osobowe bezpieczne podczas zdalnego nauczania**

**W związku z pandemią koronawirusa poczta elektroniczna i inne elementy pracy grupowej, takie jak narzędzia konferencyjne lub komunikatory internetowe stały się wsparciem dla wielu uczniów i nauczycieli, wykorzystujących zdalne metody nauczania. Korzystając z nich, warto pamiętać o bezpiecznym przetwarzaniu danych.**

**Rodzicu**

─ Szkoła może wymagać od ucznia jedynie danych niezbędnych do założenia przez niego konta w odpowiednim systemie zdalnego nauczania oraz w celu realizacji obowiązku nauki w formie zdalnej (na podstawie art. 35 ustawy – Prawa oświatowego w związku z art. 6 ust. 1 lit. e RODO).

─ Rodzic (opiekun prawny) ma prawo wiedzieć, jak szkoła jako administrator będzie przetwarzała dane osobowe jego dziecka w trakcie nauki zdalnej oraz jakie w związku z tym przysługują mu prawa.

─ Jeżeli platformy wykorzystywane do zdalnego nauczania są odrębnymi od szkoły administratorami przetwarzanych przez siebie danych, to rodzice i dzieci powinni od nich otrzymać klauzulę informacyjną o podstawowych zasadach i zakresie zbierania danych oraz administratorze, np. podczas zakładania konta.

**Podstawę prawną realizacji zajęć szkolnych w formie pracy zdalnej określa rozporządzenie Ministra Edukacji Narodowej z 20 marca 2020 r. w sprawie szczególnych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz.U. poz. 493).**

**Dobre praktyki pomagające zachować bezpieczeństwo danych podczas lekcji online**

20 zasad bezpieczeństwa, o których powinni pamiętać zarówno szkolni administratorzy, jak i nauczyciele oraz uczniowie, przygotowując się do lekcji online, aby chronić swoje dane:

1) Na bieżąco aktualizuj systemy operacyjne.

2) Systematycznie aktualizuj programy antywirusowe, antymalware i antyspyware.

3) Regularnie skanuj stacje robocze programami antywirusowymi, antymalware i antyspyware.

4) Pobieraj oprogramowanie wyłącznie ze stron producentów.

5) Nie otwieraj załączników z nieznanych źródeł dostarczanych poprzez korespondencję elektroniczną.

6) Nie zapamiętuj haseł w aplikacjach webowych.

7) Nie zapisuj haseł na kartkach.

8) Nie używaj tych samych haseł w różnych systemach informatycznych.

9) Zabezpieczaj serwery plików czy inne zasoby sieciowe.

10) Zabezpieczaj sieci bezprzewodowe – Access Point.

11) Dostosuj złożoność haseł odpowiednio do zagrożeń.

12) Unikaj wchodzenia na nieznane czy przypadkowe strony internetowe.

13) Nie loguj się do systemów informatycznych w przypadkowych miejscach z niezaufanych urządzeń lub publicznych niezabezpieczonych sieci Wi-Fi.

14) Wykonuj regularne kopie zapasowe.

15 Korzystaj ze sprawdzonego oprogramowania do szyfrowania e-maili lub nośników danych.

16) Szyfruj dane przesyłane pocztą elektroniczną.

17) Szyfruj dyski twarde w komputerach przenośnych.

18) Przy pracy zdalnej korzystaj z szyfrowanego połączenia VPN.

19) Odchodząc od komputera, blokuj stację komputerową.

20) Nie umieszczaj w komputerze przypadkowo znalezionych nośników USB. Może znajdować się na nich złośliwe oprogramowanie.

Załączniki:
<https://www.gov.pl/web/edukacja/zdalne-nauczanie-uodo>