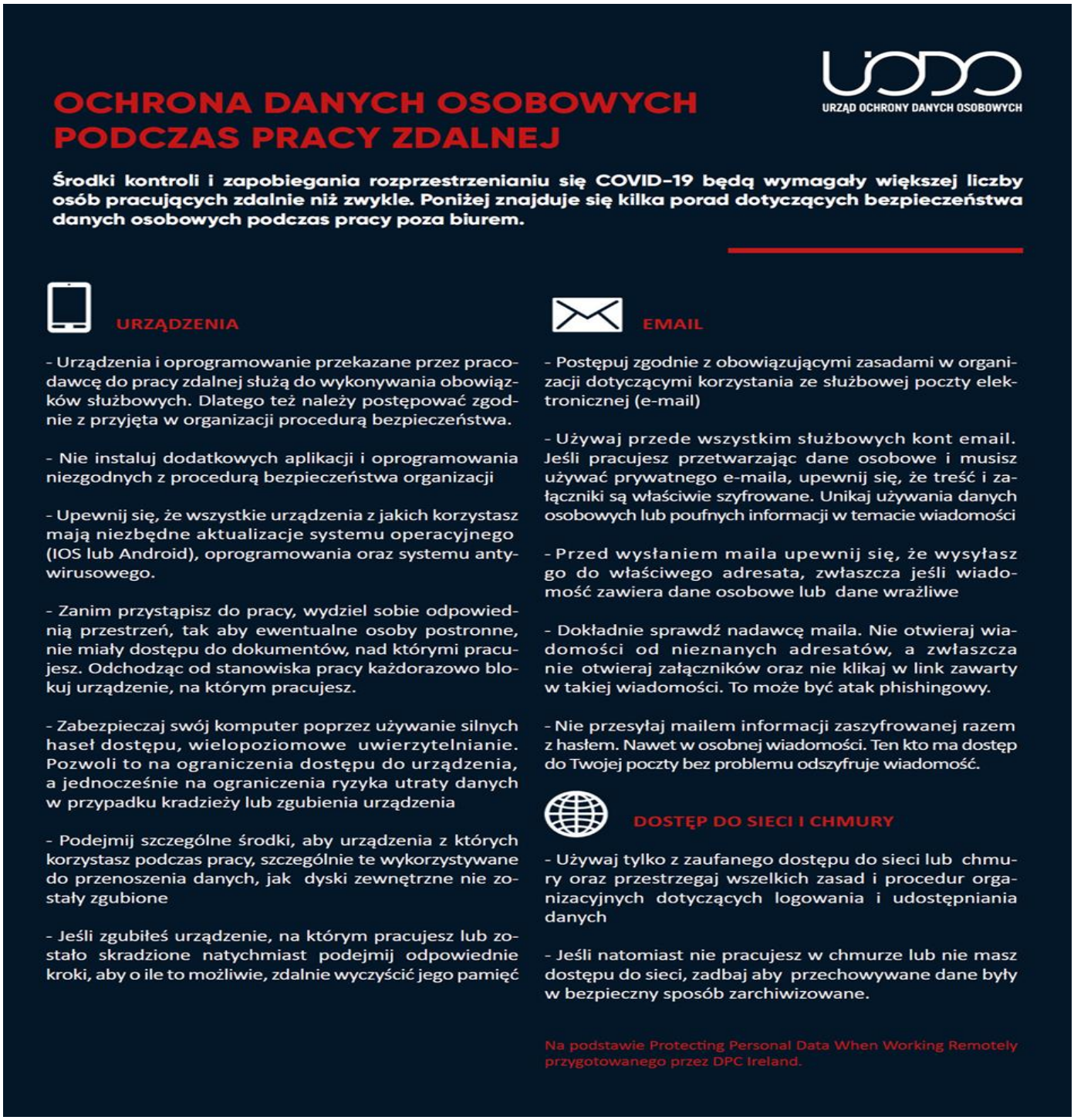
Podstawę prawną realizacji zajęć szkolnych w formie pracy zdalnej określa rozporządzenie Ministra Edukacji Narodowej z 20 marca 2020 r. w sprawie szczególnych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem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

Pracownicy wykonujący obowiązki służbowe w formie zdalnej muszą pamiętać i zaleca się im, aby odpowiednio zabezpieczali dane osobowe, które przetwarzają.

Urząd Ochrony Danych Osobowych przygotował wskazówki i porady, jak pracować poza szkołą i dbać o bezpieczne przetwarzanie danych.

OCHRONA DANYCH OSOBOWYCH PODCZAS PRACY ZDALNEJ



https://uodo.gov.pl/pl/138/1459

DOBRE PRAKTYKI POMAGAJĄCE ZACHOWAĆ BEZPIECZEŃSTWO DANYCH PODCZAS LEKCJI ONLINE

źródło: https://uodo.gov.pl/pl/138/1473

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.

Zapraszamy również do zapoznania się z poradnikiem UODO dla szkół pt. -

DANE OSOBOWE BEZPIECZNE PODCZAS ZDALNEGO NAUCZANIA

https://uodo.gov.pl/pl/138/1473

Warto także przeczytać:

- dane dzieci bezpieczne w sieci → https://uodo.gov.pl/pl/138/1363
- ochrona danych osobowych w szkole → https://uodo.gov.pl/pl/383/479
- tworzenie haseł dostępowych → https://uodo.gov.pl/pl/138/1285