

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



OCHRONA DANYCH OSOBOWYCH PODCZAS PRACY ZDALNEJ

Środki kontroli i zapobiegania rozprzestrzenianiu się COVID-19 będą wymagały większej liczby osób pracujących zdalnie niż zwykle. Poniżej znajduje się kilka porad dotyczących bezpieczeństwa danych osobowych podczas pracy poza biurem.



URZĄDZENIA

- 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.

- Nie instaluj dodatkowych aplikacji i oprogramowania niezgodnych z procedurą bezpieczeństwa organizacji

- Upewnij się, że wszystkie urządzenia z jakich korzystasz mają niezbędne aktualizacje systemu operacyjnego (IOS lub Android), oprogramowania oraz systemu antywirusowego.

- Zanim przystąpisz do pracy, wydziel sobie odpowiednią przestrzeń, tak aby ewentualne osoby postronne, nie miały dostępu do dokumentów, nad którymi pracujesz. Odchodząc od stanowiska pracy każdorazowo blokuj urządzenie, na którym pracujesz.

- Zabezpieczaj swój komputer poprzez używanie silnych haseł dostępu, wielopoziomowe uwierzytelnianie. Pozwoli to na ograniczenia dostępu do urządzenia, a jednocześnie na ograniczenia ryzyka utraty danych w przypadku kradzieży lub zgubienia urządzenia

- Podejmij szczególne środki, aby urządzenia z których korzystasz podczas pracy, szczególnie te wykorzystywane do przenoszenia danych, jak dyski zewnętrzne nie zostały zgubione

- Jeśli zgubiłeś urządzenie, na którym pracujesz lub zostało skradzione natychmiast podejmij odpowiednie kroki, aby o ile to możliwe, zdalnie wyczyścić jego pamięć



EMAIL

- Postępuj zgodnie z obowiązującymi zasadami w organizacji dotyczącymi korzystania ze służbowej poczty elektronicznej (e-mail)

- Używaj przede wszystkim służbowych kont email. Jeśli pracujesz przetwarzając dane osobowe i musisz używać prywatnego e-maila, upewnij się, że treść i załączniki są właściwie szyfrowane. Unikaj używania danych osobowych lub poufnych informacji w temacie wiadomości

- Przed wysłaniem maila upewnij się, że wysyłasz go do właściwego adresata, zwłaszcza jeśli wiadomość zawiera dane osobowe lub dane wrażliwe

- Dokładnie sprawdź nadawcę maila. Nie otwieraj wiadomości od nieznanego adresata, a zwłaszcza nie otwieraj załączników oraz nie klikaj w link zawarty w takiej wiadomości. To może być atak phishingowy.

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



DOSTĘP DO SIECI I CHMURY

- Używaj tylko z zaufanego dostępu do sieci lub chmury oraz przestrzegaj wszelkich zasad i procedur organizacyjnych dotyczących logowania i udostępniania danych

- Jeśli natomiast nie pracujesz w chmurze lub nie masz dostępu do sieci, zadбай aby przechowywane dane były w bezpieczny sposób zarchiwizowane.

Na podstawie Protecting Personal Data When Working Remotely przygotowanego przez DPC Ireland.

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 nieznanymi źródłami 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>