REKOMENDACJE POMAGAJĄCE ZACHOWAĆ BEZPIECZEŃSTWO DANYCH OSOBOWYCH PRZETWARZANYCH PODCZAS LEKCJI ONLINE

dla Administratorów, nauczycieli oraz uczniów

źródło: www.uodo.gov.pl

1. Aktualizuj na bieżąco systemy operacyjne.
2. Aktualizuj systematycznie programy antywirusowe (skonfiguruj program tak by aktualizowały się automatycznie).
3. Skanuj regularnie stacje robocze programami antywirusowymi (najlepiej ustaw automatyczne skanowanie).
4. Pobieraj oprogramowanie wyłącznie ze stron producentów (nie używaj stron typu „instalki", „dobre programy", „torrenty").
5. Nie otwieraj załączników z nieznanych źródeł dostarczanych poprzez korespondencję elektroniczną.
6. Nie zapamiętuj haseł w przeglądarce (bezpieczniej jest użyć menedżera haseł np. LastPass).
7. Nie zapisuj haseł na kartkach i tablicach, przechowuj je zawsze w miejscach niedostępnych dla osób postronnych.
8. Unikaj używania tych samych haseł w różnych systemach informatycznych.
9. Zabezpieczaj serwery plików czy inne zasoby sieciowe.
10. Zabezpieczaj sieci bezprzewodowe skomplikowanym hasłem.
11. Stosuj złożone hasła odpowiednio do zagrożeń (małe i duże litery, cyfry i znaki specjalne).
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 (np. 7-Zip).
16. Szyfruj dyski twarde w komputerach przenośnych.
17. Odchodząc od komputera, blokuj stację komputerową używając skrótu Windows + L .
18. Nie umieszczaj w komputerze przypadkowo znalezionych nośników USB. Może znajdować się na nich złośliwe oprogramowanie.
19. Założenie odrębnych kont użytkowników w przypadku korzystania z komputera przez wiele osób.
20. Przed wysłaniem maila upewnij się, że wysyłasz go do właściwego adresata, zwłaszcza jeśli wiadomość zawiera dane osobowe lub dane wrażliwe.

Dyrektorze szkoły:

- Szkoła informuje nauczycieli, rodziców oraz uczniów o sposobie realizacji nauki zdalnej. Informacja ta powinna zostać przekazana w prosty sposób, tak aby była zrozumiała dla wszystkich, do których skierowany jest komunikat.
- Szkoła powinna zapewnić narzędzia umożliwiające nauczycielom prowadzenie zajęć zdalnych oraz bezpieczną komunikację z uczniami i rodzicami, wdrażając je kompleksowo w całej placówce.
- Szkoła może wymagać od ucznia lub reprezentującego go rodzica (opiekuna prawnego) podania danych do założenia konta w systemie zdalnego nauczania, ale tylko w zakresie niezbędnym do tego, aby to konto założyć. Nie należy przy takiej okazji gromadzić danych nadmiarowych bądź służących do realizacji innych celów.
- Szkoła musi zadbać o zabezpieczenie danych przez zastosowanie odpowiednich środków technicznych i organizacyjnych. Chodzi o to, aby dane te nie były udostępniane osobom nieupoważnionym oraz nie uległy zniszczeniu, zmodyfikowaniu lub utracie.
- W razie wykonywania obowiązków służbowych przez nauczycieli poza szkołą jej dyrektor w każdym wypadku musi rozważyć możliwości odpowiedniego zabezpieczenia danych osobowych , uwzględniając stopień ryzyka naruszenia ochrony danych osobowych i ewentualnie wdrożyć odpowiednie środki minimalizujące to ryzyko lub zrezygnować z tego rodzaju praktyki, np. umożliwiając nauczycielowi, który nie ma właściwych warunków do pracy zdalnej, korzystanie ze sprzętu znajdującego się w szkole.
- Rekomenduje się, by nauczyciele do korespondencji e-mailowej z uczniami korzystali ze służbowych adresów e-mail. Dyrektor szkoły nie powinien zalecać nauczycielom używania przez nich prywatnych adresów poczty elektronicznej do kontaktu z uczniami lub ich rodzicami (opiekunami prawnymi).
  W obu przypadkach powinni odpowiednio zabezpieczać dane osobowe udostępniane w przesyłanych wiadomościach.
- Należy pamiętać, że za przetwarzanie danych uczniów przy wykorzystaniu narzędzi wdrożonych samodzielnie przez nauczyciela zawsze odpowiedzialność ponosi szkoła. Dlatego przyjmowanie określonego rozwiązania powinno się odbywać w uzgodnieniu z dyrektorem szkoły, który musi mieć świadomość, jakie narzędzia są wykorzystywane do prowadzenia zdalnej edukacji w szkole, lub wyznaczonym przez niego koordynatorem pracy zdalnej. Takie rozwiązanie powinno być traktowane jako tymczasowe.
- Przy wyborze aplikacji lub innych narzędzi wykorzystywanych do zdalnej edukacji bądź komunikacji z uczniami, zawsze należy się zastanowić, czy jest niezbędne, aby przetwarzały one dane osobowe, a jeżeli tak, czy można zminimalizować ich zakres, bądź wykorzystywać tylko pseudonimy (np. pierwsza litera imienia itp.). Należy także sprawdzić zasady świadczenia usługi i zasady przetwarzania danych przez usługodawcę (politykę prywatności).
- 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. **Nie jest to już zadanie szkoły**.

Nauczycielu:

- Pamiętaj, aby przetwarzać dane osobowe uczniów i ich rodziców tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.
- Pamiętaj aby w bezpieczny sposób korzystać z komputerów i innych urządzeń zarówno wtedy, gdy zapewnił je pracodawca, jak i wtedy, gdy korzystasz z własnych. Urządzenia te muszą być odpowiednio zabezpieczone i użytkowane zgodnie z polityką lub inną procedurą wprowadzoną w tym zakresie w szkole.
- Jeżeli używasz własnego urządzenia, powinieneś samodzielnie spełnić podstawowe wymogi bezpieczeństwa, tj. dbać o aktualizację systemu operacyjnego, o właściwe działanie programów antywirusowaych, programów typu antymalware i antyspyware, a także instalowanie na swoich urządzeniach oprogramowania i pobierania go tylko z wiarygodnych źródeł (ze stron producentów).
- Używaj mocnych (złożonych) haseł dostępowych, blokuj urządzenie przed odejściem od stanowiska pracy (zalecana konfiguracja automatycznego blokowania komputera po pewnym czasie bezczynności).
- Gdy przechowujesz dane na urządzeniach przenośnych (np. pamięć USB), muszą być one bezwzględnie szyfrowane i chronione hasłem, by zapewnić odpowiednie bezpieczeństwo danych osobowych.
- Korespondencja którą prowadzisz z uczniami lub rodzicami powinna być prowadzona ze służbowej skrzynki pocztowej. Jeżeli do celów służbowych wykorzystujesz prywatną skrzynkę pocztową, pamiętaj, aby korzystać z niej w sposób rozważny i bezpieczny.
- Szczególną uwagę musisz zwrócić na zabezpieczenie danych osobowych udostępnianych w przesyłanych wiadomościach. Zawsze przed wysłaniem wiadomości, upewnij się , czy niezbędne jest wysłanie danych osobowych, oraz że zamierzasz wysyłać ją do właściwego adresata. Podczas wysyłania korespondencji zbiorczej korzystaj z opcji „UDW" (ukryty odbiorca), dzięki której odbiorcy wiadomości nie będą widzieć wzajemnie swoich adresów e-mail.
- Uwzględnij, w porozumieniu z dyrektorem szkoły, jakie realne możliwości komunikowania się z Tobą mają uczniowie lub rodzice, pod warunkiem, że wskazany przez nich konkretny rodzaj komunikatora internetowego zapewnia bezpieczeństwo komunikacji.
- Na ogólnie dostępnych portalach lub stronach internetowych można jedynie publikować materiały edukacyjne, natomiast nie można przetwarzać danych osobowych uczniów lub rodziców.
- W celu sprawdzania i monitorowania obecności uczniów w zajęciach prowadzonych zdalnie, należy zachować proporcjonalność i minimalizację danych. Dla przykładu nie można w tym celu korzystać z narzędzi zbierających dane biometryczne.