



Kielce 2020-04-02

DOBRE PRAKTYKI POMAGAJĄCE ZACHOWAĆ BEZPIECZEŃSTWO DANYCH PODCZAS DOSTĘPU ZDALNEGO

Zasady bezpieczeństwa, o których powinni pamiętać zarówno Dyrektorzy szkół, jak i nauczyciele oraz uczniowie, przygotowując się do lekcji online, aby chronić swoje dane:

- Na bieżąco aktualizuj systemy operacyjne.
- Systematycznie aktualizuj programy antywirusowe, antymalware i antyspyware.
- Regularnie skanuj stacje robocze programami antywirusowymi, antymalware i antyspyware (zalecane przynajmniej raz w miesiącu).
- Pobieraj oprogramowanie wyłącznie ze stron producentów.
- Weryfikuj nadawcę emaili i nie otwieraj załączników z nieznanych źródeł dostarczanych poprzez korespondencję elektroniczną.
- Nie zapamiętuj haseł w aplikacjach webowych oraz na kartkach.
- Nie używaj tych samych haseł w różnych systemach informatycznych oraz zadбай aby hasło miało przynajmniej 8 znaków (w tym jedną dużą literę, cyfrę i znak specjalny).
- Zabezpieczaj serwery plików czy inne zasoby sieciowe.



- Zabezpieczaj sieci bezprzewodowe.
- Unikaj wchodzenia na nieznane czy przypadkowe strony internetowe.
- Nie loguj się do systemów informatycznych w przypadkowych miejscach z niezaufanych urządzeń lub publicznych niezabezpieczonych sieci Wi-Fi.
- Wykonuj regularne kopie zapasowe.
- Korzystaj ze sprawdzonego oprogramowania do szyfrowania e-maili lub nośników danych.
- Szyfruj dane przesyłane pocztą elektroniczną.
- Szyfruj dyski twarde w komputerach przenośnych.
- Przy pracy zdalnej korzystaj z szyfrowanego połączenia VPN.
- Odchodząc od komputera, blokuj stację komputerową.
- Nie umieszczaj w komputerze przypadkowo znalezionych nośników USB. Może znajdować się na nich złośliwe oprogramowanie.



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.

JEŚLI JESTEŚ DYREKTOREM SZKOŁY...

- Szkoły znalazły się obecnie w sytuacji, w której muszą sprostać wymogom związanym z pracą zdalną. Nowe przepisy dotyczące realizacji zajęć szkolnych w formie pracy zdalnej dają szeroką możliwość realizowania przez nauczycieli zajęć z wykorzystaniem metod i technik kształcenia na odległość lub innego sposobu kształcenia, w tym z wykorzystaniem środków komunikacji elektronicznej. Pozostawione zatem zostało szkołom duża swoboda odnośnie do wyboru właściwego narzędzia przy uwzględnieniu wszystkich aspektów związanych z możliwościami placówki, nauczycieli, a przede wszystkim, biorąc pod uwagę możliwości techniczne i organizacyjne rodziców i uczniów.
- Szkoła ma obowiązek poinformować 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 tylko niezbędnych do założenia konta w systemie zdalnego nauczania.
- Szkoła, która chce skorzystać z usług przetwarzania danych z wykorzystaniem innych niż wcześniej używane narzędzia, powinna wraz z pomocą wyznaczonego inspektora ochrony danych, w pierwszej kolejności przeprowadzić analizę zagrożeń. Szczególna uwaga powinna zostać zwrócona na bezpieczeństwo danych oraz zapewnienie odpowiednich gwarancji praw osób, których dane dotyczą.
- Jednym z głównych obowiązków szkoły – związanych z ochroną danych osobowych jest 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. Przykładowe środki służące zabezpieczeniu danych to: pseudonimizacja, szyfrowanie danych.

- Gdy szkoła powierzyła podmiotowi zewnętrznemu np. obsługę dziennika elektronicznego, dyrektor musi oszacować ryzyko i z takim podmiotem zawrzeć umowę o powierzeniu danych osobowych.
- Dyrektor szkoły nie powinien zalecać nauczycielom używania przez nich prywatnych adresów poczty elektronicznej do kontaktu z uczniami lub ich rodzicami (opiekunami prawnymi). Rekomendowane jest, by nauczyciele do korespondencji e-mailowej z uczniami korzystali ze służbowych adresów e-mail. Niemniej w obu przypadkach powinni odpowiednio zabezpieczać dane osobowe udostępniane w przesyłanych wiadomościach.

JEŚLI JESTEŚ NAUCZYCIELEM...

- Nauczyciel może przetwarzać dane osobowe uczniów i ich rodziców tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.
- Nauczyciel musi pamiętać o bezpiecznym korzystaniu z komputerów i innych urządzeń zarówno wtedy, gdy zapewnił mu je pracodawca, jak i wtedy, gdy korzysta z własnych.
- RODO nie zabrania wykorzystywania przez nauczyciela prywatnego komputera, tabletu, czy telefonu do przetwarzania danych osobowych w związku ze zdalnym prowadzeniem zajęć. Urządzenia te muszą być jednak odpowiednio zabezpieczone, a nauczyciel powinien postępować zgodnie z polityką lub inną procedurą wprowadzoną w tym zakresie w szkole.
- Jeżeli nauczyciel używa własnego urządzenia, powinien samodzielnie spełnić podstawowe wymogi bezpieczeństwa (dostosować się do zasad bezpieczeństwa podanych wyżej).
- Gdy dane są przechowywane na urządzeniach przenośnych (np. pamięć USB), muszą być bezwzględnie szyfrowane i chronione hasłem, by zapewnić odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.
- Prowadzenie zajęć zdalnych może wymagać korzystania przez nauczyciela z poczty elektronicznej do kontaktu z uczniami lub rodzicami. Nauczyciel powinien prowadzić taką korespondencję ze służbowej skrzynki pocztowej, którą powinna zapewnić mu szkoła. Jeżeli szkoła nie zapewniła nauczycielom służbowych skrzynek poczty elektronicznej, to jeżeli wykorzystują oni do celów służbowych prywatną skrzynkę pocztową muszą pamiętać, aby korzystać z niej w sposób rozważny i bezpieczny.
- Szczególną uwagę nauczyciel musi zwrócić na zabezpieczenie danych osobowych udostępnianych w przesyłanych wiadomościach. Zawsze przed wysłaniem wiadomości, należy



upewnić się, czy niezbędne jest wysłanie danych osobowych, oraz że zamierza wysłać ją do właściwego adresata. Ponadto trzeba sprawdzić, czy w nazwie adresu e-mail adresata nie ma np. przedstawionych lub pominiętych znaków tak, aby nie wysłać takiej wiadomości do osób nie-upoważnionych. Podczas wysyłania korespondencji zbiorczej powinno się korzystać z opcji „UDW”, dzięki której odbiorcy wiadomości nie będą widzieć wzajemnie swoich adresów e-mail.

- Szkoła powinna samodzielnie wdrożyć wybraną spośród dostępnych metodę i technikę kształcenia na odległość lub inny sposób realizacji zadań zdalnie. Nauczyciele nie powinni jednak sami decydować o korzystaniu z konkretnych rozwiązań (np. prowadzenie lekcji za pomocą komunikatorów czy wideo narzędzi). Biorąc jednak pod uwagę nadzwyczajną sytuację i konieczność natychmiastowego rozpoczęcia zajęć zdalnych, może to być w niektórych sytuacjach uzasadnione. Należy jednak 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.
- Na ogólnie dostępnych portalach lub stronach internetowych nauczyciel może jedynie publikować materiały edukacyjne, natomiast nie może przetwarzać danych osobowych uczniów lub rodziców.

JEŚLI JESTEŚ RODZICEM...

- 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.



UWAGA

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).

Z poważaniem

INSPEKTOR OCHRONY DANYCH

Sylwester Cieśla

CENTRUM ZABEZPIECZENIA INFORMACJI
Sylwester Cieśla
ul. Wapiennikowa 2 lok. 4, 25-112 Kielce
NIP 662-171-24-15, REGON 260124539
tel. (41) 300 55 99, kom. 512 666 944
www.czi24.pl, email: biuro@czi24.pl