DANE OSOBOWE A NAUKA ZDALNA. PORADNIK DLA SZKÓŁ I NAUCZYCIELI

Przed dyrektorami szkół, nauczycielami, uczniami, ale również i przed rodzicami postawiono wyzwanie w postaci nauki online. Oprócz technicznych aspektów i koniecznych zmian w formie nauczania należy zwrócić uwagę na aspekty bezpieczeństwa związane z ochroną danych. Z pomocą przychodzi Urząd Ochrony Danych Osobowych, który przygotował listę dobrych praktyk pomagających zachować bezpieczeństwo danych podczas lekcji online.

Urząd Ochrony Danych Osobowych przygotował szereg szczegółowych porad dla dyrektorów szkół, nauczycieli i rodziców, z objaśnieniem koniecznych działań, które spoczywają na nich w związku z realizacją zadań w sposób zdalny w kontekście ochrony danych osobowych. Jakie obowiązki spoczywają zatem na dyrektorach szkół, jakie działania są niedozwolone w trakcie zdalnej nauki a jakie prawa przysługują rodzicom? Urząd śpieszy z przypomnieniem najważniejszych kwestii związanych z RODO i bezpiecznymi zachowaniami w sieci.

Zdalne nauczanie a obowiązku dyrektora szkoły

UODO przypomina, że podstawowym obowiązkiem dyrekcji szkoły jest poinformowanie nauczycieli, rodziców oraz uczniów o sposobie realizacji nauki zdalnej. Przypomina również, że musi być ona przekazana w taki sposób, aby była zrozumiała dla wszystkich. Obowiązek informacyjny, związany z zakresem przetwarzania danych osobowych, dotyczy również nowych narzędzi lub usług, które będą świadczone przez podmioty zewnętrzne.

Szkoła odpowiedzialna jest również za zapewnienie narzędzi umożliwiających nauczycielom prowadzenie zajęć w sposób zdalny oraz bezpieczną komunikację z uczniami i rodzicami, wdrażając je kompleksowo w całej placówce.

W kontekście systemów zdalnego nauczania, szkoła może wymagać od ucznia (reprezentującego go rodzica lub opiekuna prawnego) podania tylko tych danych, które są niezbędne do założenia konta w tym systemie. Urząd przypomina, że nie należy gromadzić danych nadmiarowych lub mających służyć do realizacji innych celów.

Jeśli szkoła będzie korzystać z usług przetwarzania danych innych niż wcześniej używane narzędzia powinna przeprowadzić analizę zagrożeń. Taka analiza powinna odbywać się wraz z wyznaczonym inspektorem ochrony danych. Urząd zwraca uwagę, że szczególna uwaga powinna zostać zwrócona na bezpieczeństwo danych oraz zapewnienie odpowiednich gwarancji praw osób, których dane dotyczą.

Urząd po raz kolejny przypomina o konieczności zabezpieczenia danych – poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych. Zebrane dane nie mogą zostać udostępnione osobom nieupoważnionym do ich przeglądania a także nie mogą ulec zniszczeniu, zmodyfikowaniu lub

utracie.

Dyrekcja szkoły zobowiązana jest również do wdrożenia środków mających zminimalizować ryzyko naruszenia danych osobowych w trakcie wykonywania obowiązków służbowych przez nauczycieli poza szkołą. Jeżeli nauczyciel nie posiada warunków do pracy zdalnej, dyrekcja powinna umożliwić nauczycielowi np. korzystanie ze sprzętu znajdującego się w szkole.

Dyrekcja musi mieć pewność, że podmiot zewnętrzny któremu powierzyła obsługę narzędzi – np. dziennika elektronicznego, zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi wskazane w RODO i chroniło prawa osób, których dane dotyczą.

Jednocześnie Urząd przypomina, że dyrekcja nie powinna zalecać nauczycielom używania przez nich prywatnych adresów poczty elektronicznej do kontaktu z uczniami (reprezentujących ich rodziców lub opiekunów prawnych). UODO rekomenduje, aby nauczyciele do korespondencji e-mailowej z uczniami korzystali ze służbowych adresów e-mail.

Porady dla nauczycieli

Urząd przypomina, że nauczyciel może przetwarzać dane osobowe uczniów i ich rodziców tylko w celach związanych z wykonywaniem swoich obowiązków służbowych. Jednocześnie przypomina, że przepisy RODO nie zabraniają wykorzystywania przez nauczyciela prywatnego komputera, tabletu, czy telefonu do przetwarzania danych osobowych w związku ze zdalnym prowadzeniem zajęć. Jednak prywatny sprzęt jak i służbowy muszą być odpowiednio zabezpieczone a nauczyciel powinien postępować zgodnie z polityką lub inną procedurą wprowadzoną w tym zakresie w szkole. W szczególności Urząd przypomina o konieczności sprawdzenia swojego sprzętu czy spełnia podstawowe wymogi bezpieczeństwa.

Nauczyciel powinien wykorzystywać w zdalnym prowadzeniu zajęć te platformy edukacyjne lub narzędzia do e-learningu, które zostały wdrożone w szkole – informuje Urząd. Jednocześnie nauczyciel na ogólnie dostępnych portalach lub stronach internetowych, może jedynie publikować materiały edukacyjne, natomiast nie może przetwarzać danych osobowych uczniów lub rodziców. Jednocześnie co zostało jasno podkreślone do monitorowania obecności uczniów nie można wykorzystywać narzędzia zbierające dane biometryczne, w tym wykorzystujących systemy wykrywania twarzy.

Nauczyciel zobowiązany jest również zabezpieczyć sprzęt przed dostępem innych osób. Zalecane jest skonfigurowanie automatycznego blokowania komputera po pewnym czasie bezczynności oraz założenie odrębnych kont użytkowników w przypadku korzystania z komputera przez wiele osób – rekomenduje w swoich wytycznych Urząd. Jednocześnie przypomina o stosowaniu silnych haseł dostępowych oraz o szyfrowaniu i zabezpieczeniu hasłem danych, które są przechowywane na urządzeniach przenośnych (np. pamięć USB).

Jednocześnie nauczyciele zobowiązani są do prowadzenia korespondencji z uczniami i rodzicami poprzez wdrożone w szkole rozwiązania teleinformatyczne, np. dzienniki elektroniczne. Jednocześnie, jeżeli konieczny jest kontakt za sprawą poczty e-mail nauczyciel powinien prowadzić korespondencję ze służbowej skrzynki pocztowej, którą powinna zapewnić mu szkoła. Jeśli jednak jej nie zapewniła i nauczyciel wykorzystuje do tego celu prywatną skrzynkę pocztową konieczne jest, aby korzystać z niej w sposób rozważny i bezpieczny. Urząd przygotował również wskazówki co do zachowania bezpieczeństwa przesyłanych danych osobowych - przed wysłaniem wiadomości, należy upewnić się:

- czy niezbędne jest wysłanie danych osobowych, oraz że zamierza wysyłać ją do właściwego adresata.

- czy w nazwie adresu e-mail adresata nie ma np. przestawionych lub pominiętych znaków tak, aby nie wysłać takiej wiadomości do osób nieupoważnionych.

Podczas wysyłania korespondencji zbiorczej powinno się korzystać z opcji „UDW", dzięki której odbiorcy wiadomości nie będą widzieć wzajemnie swoich adresów e-mail – rekomenduje UODO.

O jakich prawach powinien pamiętać rodzic (opiekun prawny) nadzorujący dziecko?

Przede wszystkim, że w ramach korzystania z systemów zdalnego nauczania oraz do realizacji obowiązku nauki szkoła może wymagać od ucznia jedynie tych danych, które są niezbędne do założenia przez niego konta w odpowiednim systemie.

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

Rodzice powinni zostać poinformowani również o podstawowych zasadach i zakresie zbierania danych oraz administratorze (np. podczas zakładania konta) jeśli platformy wykorzystywane do zdalnego nauczania są odrębnymi od szkoły administratorami przetwarzanych przez siebie danych.

Ale to nie wszystko co przygotował UODO, chcąc wspomóc dyrektorów, nauczycieli, ale i uczniów w tym nadzwyczajnym dla nich czasie.

Urząd Ochrony Danych Osobowych wychodząc naprzeciw potrzebom nauczycieli, uczniów oraz rodziców przygotował 20 zasad bezpieczeństwa o których powinna pamiętać każda ze stron przygotowując się do lekcji online. Każda z tych rad ma na celu pomoc w zachowaniu bezpieczeństwa danych osobowych.

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. Nie używaj tych samych haseł w różnych systemach informatycznych.
8. Zabezpieczaj serwery plików czy inne zasoby sieciowe.
9. Zabezpieczaj sieci bezprzewodowe – Access Point.
10. Dostosuj złożoność haseł odpowiednio do zagrożeń.
11. Unikaj wchodzenia na nieznane czy przypadkowe strony internetowe.
12. Nie loguj się do systemów informatycznych w przypadkowych miejscach z niezaufanych urządzeń lub publicznych niezabezpieczonych sieci Wi-Fi.
13. Wykonuj regularne kopie zapasowe.
14. Korzystaj ze sprawdzonego oprogramowania do szyfrowania e-maili lub nośników danych.
15. Szyfruj dane przesyłane pocztą elektroniczną.
16. Szyfruj dyski twarde w komputerach przenośnych.
17. Przy pracy zdalnej korzystaj z szyfrowanego połączenia VPN.
18. Odchodząc od komputera, blokuj stację komputerową.
19. Nie umieszczaj w komputerze przypadkowo znalezionych nośników USB.
20. Może znajdować się na nich złośliwe oprogramowanie.