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 wyjątkowej sytuacji, w której muszą stawić czoła nowym wymaganiom 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. Pozostawiają zatem szkołom dużą swobodę 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. Jeżeli szkoła w celu realizacji nauki zdalnej będzie korzystać z nowych narzędzi lub usług świadczonych przez podmioty zewnętrzne, to musi także poinformować o tym, jak w tym zakresie będą przetwarzane dane osobowe.

– 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, 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, anonimizacja, szyfrowanie danych.

– 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.

– Gdy szkoła powierzyła podmiotowi zewnętrznemu np. obsługę dziennika elektronicznego, dyrektor musi mieć pewność, że usługodawca zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi wskazane w RODO i chroniło prawa osób, których dane dotyczą. Dlatego też, przed podjęciem takiej decyzji szkoła powinna przeanalizować wszystkie możliwe rozwiązania oraz oszacować ryzyko.

– 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. Przede wszystkim należy sprawdzić, czy wykorzystywane urządzenie ma aktualny system operacyjny, czy używane są na nim programy, w szczególności programy antywirusowe, czy dokonane są niezbędne aktualizacje. Na bieżąco aktualizowane powinny być także zainstalowane programy antymalware i antyspyware. Należy rozważnie instalować na swoich urządzeniach oprogramowanie i pobierać je tylko z wiarygodnych źródeł (ze stron producentów).

– Przechowując dane na sprzęcie, do którego mogą mieć dostęp inne osoby, należy używać mocnych haseł dostępowych, a przed odejściem od stanowiska pracy urządzenie powinno zostać zablokowane. Zalecane jest także skonfigurowanie automatycznego blokowania komputera po pewnym czasie bezczynności oraz założenie odrębnych kont użytkowników w przypadku korzystania z komputera przez wiele osób.

– Podczas korzystania z programów lub aplikacji mobilnych należy korzystać z możliwych do zastosowania w nich mechanizmów ochrony prywatności użytkowników. Jeśli użycie jakiegoś

programu wymaga logowania, warto zadbać o silne hasło dostępu, a dodatkowo chronić je przed utratą czy dostępem osób nieuprawnionych.

– 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.

– W podstawowym zakresie komunikację z uczniami i rodzicami prowadzi się poprzez wdrożone w szkole rozwiązania teleinformatyczne, np. dzienniki elektroniczne. W takiej sytuacji nauczyciel musi nadal zachowywać podstawowe zasady bezpieczeństwa przy zdalnym łączeniu się z dziennikiem elektronicznym ze swojego urządzenia w domu.

– 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 wysyłać ją do właściwego adresata. Ponadto trzeba sprawdzić, 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.

– Nauczyciel powinien wykorzystywać w zdalnym prowadzeniu zajęć te platformy edukacyjne lub narzędzia do e-learningu, które zostały wdrożone w szkole. W takiej sytuacji może oczekiwać, że prowadzenie zajęć zdalnych będzie bezpieczne. Powinien wtedy przestrzegać przyjętych przez szkołę instrukcji i procedur dotyczących ochrony danych osobowych oraz musi zachować podstawowe zasady bezpieczeństwa przy zdalnym łączeniu się z taką platformą ze swojego urządzenia w domu.

– 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 wideonarzędzi). 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 w szkole. Takie rozwiązanie powinno być traktowane jako tymczasowe.

– Zawsze przy wyborze aplikacji lub innych narzędzi wykorzystywanych do zdalnej edukacji bądź komunikacji z uczniami 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).

– W obecnej sytuacji nauczyciel w porozumieniu z dyrektorem szkoły powinien uwzględnić, jakie realne możliwości komunikowania się z nim mają uczniowie lub rodzice, pod warunkiem, że wskazany przez nich konkretny rodzaj komunikatora internetowego zapewnia bezpieczeństwo komunikacji.

– Na ogólnie dostępnych portalach lub stronach internetowych nauczyciel może jedynie publikować materiały edukacyjne, natomiast nie może przetwarzać danych osobowych uczniów lub rodziców.

– W celu sprawdzania i monitorowania obecności uczniów w zajęciach prowadzonych zdalnie nauczyciel powinien zachować proporcjonalność i minimalizację danych. Dla przykładu nie może w tym celu korzystać z narzędzi zbierających dane biometryczne, w tym wykorzystujących systemy wykrywania twarzy.

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

– 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).

Warto przeczytać:

- ochrona danych osobowych podczas pracy zdalnej>> https://uodo.gov.pl/pl/138/1459
- 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