URZĄD OCHRONY DANYCH OSOBOWYCH

EDUKACJA ZDALNA - PRACA ZDALNA A OCHRONA DANYCH OSOBOWYCH

PORADY DLA NAUCZYCIELI

Piotr Drobek

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl

Plan webinarium

- Wstęp
- Obowiązki szkoły jako administratora danych a zdalna edukacja
- Obowiązki nauczycieli związane z pracą zdalną
- Praca zdalna a dokumenty papierowe
- Wykorzystywanie przez nauczycieli prywatnego sprzętu
- Bezpieczne korzystanie z wideokonferencji
- Nagrywanie wizerunku

Realizacja edukacji zdalnej w szkołach

- „Są szkoły, w których dyrekcja dała nauczycielom wolną rękę w wyborze metod i narzędzi realizowania edukacji zdalnej. Taka sytuacja generuje chaos – uczniowie gubią się w mnogości platform i komunikatorów, a nauczyciele też nie mają pewności czy formuła, na którą się zdecydowali jest najlepsza”.

- „W szkołach, w których podjęto decyzję o uspójnieniu nauki zdalnej zarówno uczniowie jak i nauczyciele szybciej wdrożyli się w nowe realia. Sprawniej działa też system samopomocy pomiędzy nauczycielami”.

Centrum Cyfrowe, Edukacja zdalna w czasie pandemii. Raport z badań. kwiecień 2020

Szkoła jako administrator

- Szkoła reprezentowana przez jej dyrektora jest administratorem
  w rozumieniu RODO i to ona ponosi odpowiedzialność za przestrzeganie przepisów o ochronie danych osobowych
- Nauczyciele nie są samodzielnymi administratorami danych. Przetwarzają dane tylko w zakresie realizacji obowiązków służbowych

Źródła prawa

- Ogólne Rozporządzenie o ochronie danych (RODO)
- Prawo oświatowe (art. 30a)
- Rozporządzenie Ministra Edukacji Narodowej z 25.08.2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji
- **Rozporządzenie Ministra Edukacji Narodowej z 20.03.2020 r. w sprawie szczególnych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19**

Bezpieczny model zdalnego nauczania

- Szeroka możliwość realizowania przez nauczycieli zajęć z wykorzystaniem metod i technik kształcenia na odległość lub innego sposobu kształcenia, w tym z wykorzystaniem środków komunikacji elektronicznej.
- Szkoły mają swobodę co 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.
- Rola dyrektora szkoły
- Liderzy zdalnego nauczania
- Zespoły ds. zdalnego nauczania
- Rola inspektora ochrony danych w szkole

URZĄD OCHRONY DANYCH OSOBOWYCH

Bezpieczny model zdalnego nauczania

- 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).

Bezpieczny model zdalnego nauczania

- 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.

Bezpieczny model 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.
- 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.

Obowiązki nauczycieli związane z praca zdalną

- Bezpieczne korzystanie z komputerów i innych urządzeń zarówno wtedy, gdy zapewnił mu je pracodawca, jak i wtedy, gdy korzysta z własnych.
- 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.

Dokumentacja papierowa a praca zdalna

- Procedury postępowania przyjęte w Szkole
- Zabezpieczenie dokumentów
- Zasada niszczenia dokumentów papierowych

URZĄD OCHRONY DANYCH OSOBOWYCH

Wykorzystywanie własnego sprzętu

- 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.

Wykorzystywanie własnego sprzętu

- 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.

Bezpieczne korzystanie z wideokonferencji

Przed rozpoczęciem wideokonferencji

- 1. Zapoznaj się z ogólnymi warunkami użytkowania lub polityką prywatności programu, z którego chcesz skorzystać.
- 2. Sprawdź, czy Twoje rozmowy będą nagrywane i przechowywane.
- 3. Zweryfikuj, do jakich celów wykorzystywane będą Twoje dane osobowe.
- 4. Sprawdź, o jakie uprawnienia do danych jesteś proszony – lista kontaktów, lokalizacja itp.
- 5. Do zainstalowania aplikacji na komputerze użyj oficjalnej strony aplikacji z której chcesz korzystać; w przypadku urządzeń mobilnych wybierz oficjalny sklep – Google Play lub App Store.
- 6. Upewnij się, że osoby postronne nie mają dostępu do Twojego ekranu.
- 7. Sprawdź, czy aplikacja dysponuje niezbędnymi środkami bezpieczeństwa, takimi jak szyfrowanie.

Bezpieczne korzystanie z wideokonferencji

- Przed rozpoczęciem wideokonferencji
- 8. Korzystaj z aplikacji webowych, nie desktopowych.
- 9. Zabezpiecz sieć Wi-Fi silnym hasłem.
- 10. Przed udostępnieniem swojego ekranu podczas rozmowy zamknij wszystkie okna, tak aby inni uczestnicy konferencji ich nie zobaczyli.
- 11. Przy podłączeniu się do telekonferencji korzystaj z kodów dostępu/PIN-ów.
- 12. Przeskanuj program do telekonferencji systemem antywirusowym lub antymalware-owym.

Bezpieczne korzystanie z wideokonferencji

- W trakcie korzystania z wideokonferencji
- 1. Ogranicz ilość podawania danych osobowych – użyj pseudonimu i służbowego adresu e-mail.
- 2. Użyj innego hasła, niż używane przez Ciebie w innych usługach.
- 3. Nie udostępniaj linków do konferencji w mediach społecznościowych.
- 4. Włącz, jeśli to możliwe, domyślną ochronę hasłem spotkania on-line.
- 5. Zarządzaj opcjami udostępniania ekranu.
- 6. W celu wykonywania rozmów służbowych wykorzystuj dostęp do sieci za pomocą szyfrowanego połączenia VPN.
- 7. Nie udostępniaj dokumentów służbowych, za pomocą czatu, który może być publiczny.
- 8. Jeżeli to możliwe korzystaj z opcji zamazywania tła (tak, żeby rozmówcy nie widzieli Twojego otoczenia).
- 9. Korzystaj z opcji „poczekalnia” tak, abyś mógł kontrolować osoby uczestniczące w telekonferencji, unikniesz przypadkowych lub niechcianych osób.
- 10. Logując się do telekonferencji, wyłącz mikrofon i kamerę(włączysz je jak będzie to potrzebne)

Bezpieczne korzystanie z wideokonferencji

- Po skorzystaniu z wideokonferencji
- 1. Wyłącz mikrofon i kamerę.
- 2. Upewnij się, że zakończyłeś spotkanie on-line i zamknąłeś aplikację.
- 3. Sprawdź, czy program do telekonferencji nie działa w tle.

Nagrywanie wizerunku

- Wizerunek jako dana osobowa
- Ochrona wizerunku w Kodeksie cywilnym
- Ochrona wizerunku w Prawie autorskim

Materiały pomocnicze

- Dane osobowe bezpieczne podczas zdalnego nauczania – poradnik UODO dla szkół
- Jak bezpiecznie korzystać z wideokonferencji?
- Dokumentacja papierowa zawierająca dane osobowe a praca zdalna
- Ochrona danych osobowych podczas pracy zdalnej
- Jak bezpiecznie prowadzić lekcje online? Poradnik dla nauczycieli i dyrektorów
- Tips for selecting and using online communication tools
- Badanie edukacji zdalnej w czasie pandemii
- Jak uczyć zdalnie? Proste odpowiedzi na trudne pytania

URZĄD OCHRONY DANYCH OSOBOWYCH

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl