

PODSTAWOWE ZASADY PRACY ZDALNEJ NAUCZYCIELI SZKOŁY PODSTAWOWEJ NR 350 IM. ARMII KRAJOWEJ W WARSZAWIE

Zgodne z System ochrony danych osobowych jednostek oświatowych
w Dzielnicy Bemowo m. st. Warszawy

Nauczyciele, realizując pracę zdalną (domyślnie: w domu), wykonują czynności służbowe i działają w imieniu Szkoły, dlatego w takich przypadkach obowiązują ich wymogi dotyczące ochrony danych osobowych. Reprezentując Szkołę w zakresie przetwarzania danych osobowych, nauczyciele pracujący zdalnie są uprawnieni do:

1. Wykorzystania swoich prywatnych zasobów informacyjnych (komputery, dostęp do sieci Internet, itp.), o ile Dyrektor wyrazi na to zgodę i nie ma możliwości zapewnienia sprzętu służbowego, a samo wykorzystanie odbywać się będzie w sposób bezpieczny.
2. Zabezpieczania danych, którymi nauczyciel dysponuje w związku z realizacją swoich obowiązków.

*Czego w przypadku pracy zdalnej **nie należy robić**:*

1. Nie można zbierać danych dot. uczniów i ich rodziców bez konkretnej podstawy prawnej (np. poprzez wysyłanie nieautoryzowanych przez kierownictwo Szkoły dokumentów, formularzy do wypełnienia przez uczniów, czy ich rodziców).
2. Nie należy przechowywać jakichkolwiek danych osobowych na urządzeniach/zasobach prywatnych, jeżeli nie zachodzi taka konieczność (np. poprzez pobieranie, tworzenie dodatkowych raportów, zestawień uczniów, które miałyby być zapisywane lokalnie na Państwa komputerze, poza system dziennika elektronicznego).
3. Nie wolno, bez wiedzy i zgody dyrektora zabierać (do domu) oficjalnych dokumentów szkolnych,
4. Nie należy udostępniać informacji (np. poprzez Internet) osobom innym, niż do tego uprawnione (np. podawania grupowo ocen, publikacji wyników na otwartych stronach internetowych, mediach społecznościowych itp.).
5. Nie należy umożliwiać dostępu do systemów informatycznych (poczta e-mail, e-dziennik, platformy e-learningowe) osobom lub podmiotom nieuprawnionym (członkowie rodziny nauczyciela).
6. Nauczyciel nie jest uprawniony do przysyłania e-maili zawierających szczegółowe dane osobowe, w otwartej, niezabezpieczonej (niezaszyfrowanej) formie. W szczególności dotyczy to korespondencji zbiorowej, której należy unikać.

7. Nie należy przekazywać danych dzieci np. imion, nazwisk, numerów PESEL, ocen, adresów, telefonów - zarówno w formie tradycyjnej, jak i elektronicznej - jakimkolwiek nieuprawnionym osobom lub podmiotom.
8. Nie należy wymuszać na rodzicach, ucznia zakładania profili na wskazanych przez nauczyciela portalach społecznościowych (np., Facebook).
9. Nie należy zmuszać uczniów, rodziców do prowadzenia komunikacji poprzez środki, kanały nieautoryzowane przez kierownictwo Szkoły (np. narzucać komunikację przy pomocy aplikacji typu Messenger, Whatsapp zamiast systemu dziennika elektronicznego).

Najważniejsze zasady przetwarzania danych osobowych przez nauczycieli, obowiązujące także poza siedzibą Szkoły:

1. **Nauczyciel ma obowiązek zabezpieczania danych osobowych uczniów** związanych z realizacją obowiązków edukacyjno-wychowawczych przez nauczycieli (np. zawartych w notatkach, kserokopiach, dokumentach i systemach elektronicznych)
2. **Należy zwracać uwagę, kto potencjalnie może mieć dostęp danych.** Udostępnianie danych osobowych osobom do tego nieuprawnionym jest jedną z najczęstszych przyczyn naruszenia przepisów o ochronie danych osobowych. Jeżeli np. korzystamy z komputera wraz z innymi domownikami lub znajomymi, należy zapewnić, aby nie mieli oni dostępu do plików, systemów informatycznych, loginów i haseł.
3. Dokumenty papierowe, zawierające dane podlegające ochronie, **powinny pozostać w Szkole, nie wolno ich wnosić poza siedzibę Szkoły, bez uzgodnienia tego z kierownictwem Szkoły. Dokumenty należy trzymać w zamknięciu, w przeznaczonym do tego miejscu.** Wynoszenie dokumentów może spowodować ich utratę lub upublicznienie.
4. Niepotrzebnych kopii dokumentów zawierających dane osobowe **nie należy wyrzucać** bez uprzedniego ich zniszczenia lub zmodyfikowania uniemożliwiającego odtworzenie danych osobowych (np. zastosowania anonimizacji).
5. Należy zwrócić uwagę, czy **nikt nieupoważniony nie może podejrzeć dokumentów z danymi osobowymi** – narażanie danych na powszechny wgląd w miejscach publicznych, sklepach, kawiarniach lub innych łatwo dostępnych miejscach może spowodować nieuprawniony dostęp do danych.
6. Konieczne jest stosowanie regularnie aktualizowanego oprogramowania antywirusowego na wykorzystywanym prywatnym sprzęcie. Niezależnie od tego, czy stosowane systemy antywirusowe są płatne, czy darmowe, to są w stanie zapewnić lepszy poziom ochrony przed złośliwym oprogramowaniem niż całkowity ich brak.
7. Nie wolno zapisywać loginów i haseł w przeglądarkach internetowych, w szczególności w sytuacjach, gdy z Państwa komputerów korzystają osoby trzecie.
8. W przypadku użytkowania na komputerach prywatnych systemów operacyjnych typu Windows, zalecane jest wykorzystywanie min. systemu Windows 8, ponieważ starsze wersje nie są już uaktualniane pod kątem bezpieczeństwa.
9. **Przed podaniem do nowego systemu informatycznego danych osobowych (uczniów, rodziców) należy uzyskać autoryzację kierownictwa Szkoły, do wykorzystania takiego narzędzia. Zasada ta dotyczy np. nowych platform e-learningowych. W przypadku wątpliwości, w tej kwestii prosimy o kontakt z inspektorem ochrony danych osobowych.**
10. Do pracy zdalnej należy wykorzystywać jedynie sprawdzone, zabezpieczone hasłem sieci internetowe. W przypadku korzystania z połączenia bezprzewodowego (Wi-Fi) niezbędna

jest taka konfiguracja sieci, aby połączenie było szyfrowane, minimalnie na poziomie WPA2. Jeżeli będziecie Państwo zobligowani do skorzystania z dostępu do Internetu poza domem, to pamiętać należy, że z punktu widzenia bezpieczeństwa lepiej jest korzystać z tzw. Internetu mobilnego (np. udostępnianego przez smartfona), niż z nieznanej sieci Wi-Fi.

11. Należy aktualizować systemy operacyjne, programy antywirusowe, przeglądarki internetowe, oprogramowanie typu Java, Flash itp., ponieważ bardzo często są one uszczelniane pod kątem wykrytych niebezpieczeństw
12. Zachęcamy, aby praca zdalna z uczniami była prowadzona z wykorzystaniem jedynie podstawowych, niezbędnych danych osobowych (np. imię i nazwisko, klasa). Tam, gdzie jest to możliwe technicznie, rekomendujemy stosowanie szyfrowania bądź innych metod pseudonimizacji.

Osoby mające dostęp do danych w jednostce oświatowej mają obowiązek zachowania w poufności informacji uzyskanych w związku z wykonywaną pracą, dotyczących zdrowia, potrzeb rozwojowych i edukacyjnych, możliwości psychofizycznych, seksualności, orientacji seksualnej, pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub światopoglądowych uczniów/wychowanków. Wynika to z art. 30a ust. 2 Ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz.U. z 2019 poz. 1148) i dotyczy danych zarówno w formie papierowej, jak i elektronicznej.

Najważniejsze, praktyczne zasady przetwarzania danych z wykorzystaniem systemów informatycznych

1. W Szkole Podstawowej nr 350 im. Armii Krajowej podstawową platformą do przekazywania uczniom klas 2.-8. zadań do pracy zdalnej pozostaje aplikacja Share Point w Office 365.
2. W najbliższym czasie wskazane jest uruchomienie innych kanałów, które pozwolą na bezpośredni kontakt z uczniami i indywidualizować ich pracę. Mogą to być darmowe narzędzia telekonferencyjne. Dzięki nim można prowadzić wieloosobowe wideokonferencje, a nawet dzielić się zawartością ekranu z pozostałymi uczestnikami. Do takich narzędzi należą m.in.: Skype, Microsoft Teams, YouTube czy Google HangoutsMeet. Messenger czy WhatsApp to aplikacje, które dają możliwość stworzenia grupy, w której znajdzie się np. cała klasa. **We wszystkich tych przykładach należy uzyskać autoryzację kierownictwa Szkoły do wykorzystania takiego narzędzia. Obowiązkowe jest zebranie zgody od rodziców uczniów, którzy wraz z ze swoim dzieckiem potwierdzą zaznajomienie się z regulaminem instalacji i korzystania aplikacji.**
3. Przed rozpoczęciem pracy zalecane jest sprawdzenie, czy nie było ingerencji w wykorzystywany sprzęt komputerowy.
4. Stanowczo odradza się logowania do systemów internetowych z nieznanych komputerów.
5. Odchodząc od komputera ZAWSZE powinno się pamiętać o tym, aby się z systemu wylogować lub zablokować stację roboczą (menu start -> Wyloguj lub ikona Windows + klawisz „L”).
6. **Zalecana jest regularna zmiana haseł.** Należy mieć na uwadze, że jeżeli system nie wymusza zmiany hasła, użytkownik nie jest zwolniony z tego obowiązku.
7. Logując się do systemu powinno się zadbać o to, czy nikt nie widzi wpisywanego hasła.

8. Zaleca się używać haseł łatwych do zapamiętania dla właściciela – trudnych do odgadnięcia dla innych. Konstruując hasło, oprócz liter, powinno się używać także cyfr oraz znaków specjalnych takich jak: @, #, &, %, * itp.
9. Jeżeli występuje podejrzenie, że ktoś mógł poznać hasło, zaleca się zmienić je niezwłocznie. Powinno się pamiętać, że systemy, w których przetwarzane są dane osobowe posiadają tzw. logi, czyli historię zmian dokonanych w systemie przez danego użytkownika.
10. Nie wolno zapisywać haseł, szczególnie, jeżeli komputer jest współużytkowany. Tym bardziej odradza się zapisanie obok siebie loginu i hasła!
11. O ile użytkownik korzysta z wielu systemów, powinien używać różnych haseł w każdym z nich.
12. Korzystając z systemów internetowych do przekazywania danych, należy zwrócić uwagę, aby wykorzystywać połączenia szyfrowane (włączona opcja SSL w ustawieniach systemu).
13. W przypadku komputerów przenośnych, warto zwrócić uwagę na to, aby cenne dane były przechowywane w formie zaszyfrowanej.
14. Kategorycznie zabrania się korzystania z nieznanymi sieci Wi-Fi (powinno się korzystać tylko z wiarygodnych, zabezpieczonych i zaszyfrowanych sieci).
15. Zabrania się pobierania, przechowywania i rozpowszechniania na służbowym sprzęcie komputerowym treści zakazanych, nielegalnych lub treści z niewiadomego źródła.
16. Zabrania się umieszczania danych służbowych (w tym zdjęć z wycieczek szkolnych) na prywatnych portalach społecznościowych nauczycieli.
17. Nigdy nie należy blokować działań programu antywirusowego.
18. Załączniki zawierające informacje chronione, dołączane do maili, powinny być zabezpieczone hasłem, tak aby nikt niepowołany nie otworzył wysłanej zawartości.
19. Ważne dane powinny być zapisywane w miejscach bezpiecznych, tzn. takich, do których nie mają dostępu inne, niepowołane osoby.
20. Należy pamiętać, że jednym ze sposobów kradzieży danych może być podejrzenie np. na ekranie monitora.
21. Do przysyłania dokumentów służbowych nie można używać prywatnego konta e-mail.
22. Dokumenty elektroniczne zawierające dane osobowe, które są wykorzystywane do pracy poza siedzibą jednostki, muszą być w pełni szyfrowane (np. zabezpieczone hasłem dyski twarde komputerów, pamięci Flash, zaszyfrowane pliki czy dyski przenośne).
23. Zalecana jest daleko posunięta ostrożność w użytkowaniu prywatnych smartfonów w celach służbowych, np. robienie zdjęć, czy nagrywanie filmów. Przed jakimkolwiek służbowym użyciem smartfona należy upewnić się, że dane potencjalnie umieszczone na urządzeniu nie mają możliwości przedostania się do Internetu, np. poprzez wirusy komputerowe lub uprawnienia aplikacji mobilnych.
24. Praca z dokumentami elektronicznymi poza siedzibą jednostki, jest możliwa jedynie w przypadku zapewnienia przez pracownika odpowiedniego poziomu bezpieczeństwa danych.
25. Należy zwracać uwagę na wszystkie nietypowe sytuacje przy pracy, tj. spowolnienie pracy komputera, wyskakujące okienka, zawieszenie pracy komputera itp., ponieważ mogą one być przejawem próby kradzieży lub zniszczenia danych.
26. O zauważonych nieprawidłowościach należy zawsze niezwłocznie informować administratora systemu informatycznego, swojego przełożonego, a następnie Inspektora ochrony danych.

Źródło:

1. System ochrony danych osobowych jednostek oświatowych w Dzielnicy Bemowo m. st. Warszawy "Podstawowe zasady przetwarzania danych osobowych uczniów i ich rodziców w przypadku pracy zdalnej w sytuacji zamknięcia jednostek z powodu zagrożenia koronawirusem", EDUKOMPETENCJE
2. <https://www.gov.pl/web/zdalnelekcje/zdalna-klasa> z dnia 19.03.2020