Załącznik nr 2 do Zarządzenia

Procedura bezpiecznego przetwarzania danych osobowych w pracy zdalnej w Szkole Podstawowej nr 38 im. Ludwika Zamenhofa w Częstochowie

Celem niniejszej procedury jest zapewnienie bezpiecznego procesu przetwarzania danych osobowych w pracy zdalnej podczas wprowadzenia czasowego ograniczenia funkcjonowania jednostek oświatowych, zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – dalej „RODO" oraz ustawą z dnia 10 maja 2018 o ochronie danych osobowych (Dz. U. 2019 poz. 1789).

§ 1

Postanowienia ogólne

1. Pracownik jest zobowiązany do świadczenia pracy zdalnej po wydaniu przez pracodawcę polecenia w postaci papierowej lub elektronicznej dotyczącej wykonywania pracy zdalnej.
2. Pracownik, któremu wydano polecenie pracy zdalnej zobowiązany jest w jej trakcie do przetwarzania danych osobowych zgodnie z przepisami powszechnie obowiązującego. prawa, w szczególności z przepisami o ochronie danych osobowych oraz innymi przepisami regulującymi pracę Szkoły Podstawowej nr 38 im. Ludwika Zamenhofa zwłaszcza z polityką bezpieczeństwa przetwarzania danych osobowych, w tym instrukcją zarządzania systemami informatycznymi.
3. W ramach pracy zdalnej pracownik zobowiązany jest do przetwarzania udostępnionych mu danych osobowych jedynie w celach służbowych, określonych w umowie o pracę.
4. Zabronione jest wykorzystywanie przez pracownika udostępnionych mu danych osobowych w celach niezwiązanych z wykonywaniem zadań i obowiązków służbowych.
5. Wykonywanie pracy w formie zdalnej odbywa się na służbowym lub prywatnym sprzęcie komputerowym, za pisemną zgodą pracodawcy.

§ 2

Bezpieczeństwo obszaru przetwarzania

1. Pracownik jest odpowiedzialny za właściwe zabezpieczenie danych osobowych przetwarzanych przez niego w ramach pracy zdalnej.
2. Pracownik zobowiązany jest do zachowania poufności informacji, w szczególności podczas służbowych rozmów telefonicznych lub wideokonferencji.
3. Pracownik zobowiązany jest do zabezpieczania dostępu do posiadanych danych służbowych przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi oraz przed ich nieuprawnionym zniszczeniem lub modyfikacją.
4. Pracownik zobowiązany jest do uniemożliwienia wglądu osobom postronnym w treści wyświetlane na ekranie sprzętu komputerowego, na przykład poprzez odpowiednie ustawienie ekranu lub zastosowanie nakładki na ekran tzw. filtru / folii prywatyzującej.

5. Pracownik zobowiązany jest do stosowania polityki czystego ekranu, tj. blokowania sprzętu komputerowego w razie oddalenia się od miejsca pracy.
6. Pracownik zobowiązany jest po zakończeniu pracy na sprzęcie elektronicznym każdorazowo wylogować się z programów wykorzystywanych do pracy zdalnej oraz z systemu.
7. Pracownik zobowiązuje się do bezpiecznego przechowywania danych osobowych zawartych w dokumentacji w formie papierowej, na przykład w szafach zamykanych na klucz.

§ 3

Bezpieczeństwo domowej sieci

1. Sprzęt komputerowy powinien być podłączony do zabezpieczonej, domowej sieci WiFi. Zabronione jest korzystanie z otwartych sieci WiFi, na przykład WiFi hotelowe, w galeriach handlowych lub hot-spot w kawiarniach.
2. Dostęp do panelu konfiguracyjnego urządzenia sieciowego oraz dostęp do sieci bezprzewodowej (sieci WiFi) powinien być zabezpieczony silnym hasłem, którym nie jest hasło domyślne, zdefiniowane podczas pierwszej konfiguracji urządzenia.
3. Oprogramowanie urządzenia sieciowego powinno być regularnie aktualizowane.
4. Możliwość konfiguracji sprzętu sieciowego z urządzeniami znajdującymi się poza siecią LAN powinna być wyłączona lub ograniczona tylko do zdefiniowanych adresów IP.

§ 4

Procedura bezpiecznego logowania

1. Dostęp do sprzętu lub programu wykorzystywanego do pracy zdalnej powinien być możliwy wyłącznie z wykorzystaniem indywidualnego identyfikatora oraz hasła, na przykład poprzez ustawianie PIN-u lub innej formy uwierzytelnienia.
2. Hasło do sprzętu lub programu wykorzystywanego do pracy zdalnej powinno być odpowiednio długie i złożone. Nie powinno być ono zbudowane za pomocą ciągu znajdujących się obok siebie znaków na klawiaturze lub oparte na prostych skojarzeniach związanych z użytkownikiem, na przykład numer telefonu, data urodzenia, imiona lub nazwiska.
3. Hasło do sprzętu lub programu wykorzystywanego do pracy zdalnej powinno być zmieniane w cyklach 30-dniowych.
4. Zabronione jest udostępnianie osobom trzecim haseł oraz przechowywanie ich w miejscach nie gwarantujących ich poufności.
5. Zabronione jest domyślne zapamiętywanie hasła dostępu do konta użytkownika systemu na sprzęcie oraz programów wykorzystywanych w pracy zdalnej, w szczególności dziennika elektronicznego i platform wykorzystywanych w kształceniu na odległość.

§ 5

Bezpieczne korzystanie z programów i platform wykorzystywanych w pracy zdalnej (w tym wideokonferencji)

1. Użycie w pracy zdalnej danego programu/platformy wymaga pisemnej zgody pracodawcy.
2. Przetwarzanie danych osobowych w pracy zdalnej dopuszczalne jest jedynie w programach/platformach, z którymi jednostka systemu oświaty zawarła umowę powierzenia przetwarzania danych osobowych.
3. Przed rozpoczęciem korzystania z programu/platformy wykorzystywanej do pracy zdalnej pracownik zobowiązany jest do zapoznania się z ogólnymi warunkami jej użytkowania oraz polityką prywatności.
4. W przypadku korzystania z programów z funkcją wideokonferencji zaleca się wyłączenie opcji nagrywania i przechowywania.
5. Przy podłączaniu się do programu z funkcją telekonferencji zalecane jest korzystanie z kodów dostępu/PIN-ów.
6. Przed rozpoczęciem korzystania z programów z funkcją telekonferencji zalecane jest przeskanowanie ich systemem antywirusowym lub antymalwareowym.
7. W trakcie korzystania z programów lub platform do pracy zdalnej należy ograniczyć ilość podawanych danych osobowych (zasada minimalizacji danych).
8. W przypadku, kiedy pracownikowi został przydzielony służbowy adres e-mail zabronione jest korzystanie z prywatnego adresu e-mail do celów służbowych.
9. Zabrania się udostępniania dokumentów służbowych, za pomocą publicznego czatu lub innych komunikatorów.
10. Zabrania się udostępniania w mediach społecznościowych linków do konferencji, prowadzonych zajęć i innych aktywności realizowanych w ramach pracy zdalnej.
11. Zaleca się udostępnianie linków do konferencji, prowadzonych zajęć i innych aktywności realizowanych w ramach pracy zdalnej, na przykład poprzez wskazany adres e-mail lub dziennik elektroniczny.
12. Należy korzystać z opcji „poczekalnia” tak, aby kontrolować uczestników telekonferencji, w celu uniknięcia przypadkowych lub niechcianych osób.

§ 6

Bezpieczne przechowywanie danych

1. Sprzęt komputerowy i inne nośniki urządzeń mobilnych wykorzystywane w celach służbowych, w tym laptop, telefon lub tablet powinny być zaszyfrowane, na przykład za pomocą hasła i zabezpieczone przed dostępem osób trzecich.
2. Zewnętrzne karty pamięci, a także inne nośniki danych, takie jak pendrive lub dysk zewnętrzny, wykorzystywane w celach służbowych powinny być szyfrowane, na przykład za pomocą hasła i zabezpieczone przed dostępem osób trzecich.
3. Zabronione jest umieszczanie danych osobowych w publicznych chmurach obliczeniowych (np. Dysk Google), komunikatorach (np. Messenger lub Discord) lub innych usługach dostępnych w sieci oraz rekomendowanie zakładania tam kont.

§ 7

Ochrona przed cyberatakami

1. Sprzęt wykorzystywany do pracy zdalnej musi być wyposażony w uruchomione i zaktualizowane oprogramowanie antywirusowe.

2. Systemy, w tym system operacyjny wykorzystywany do pracy zdalnej musi być regularnie aktualizowany.
3. Komputer wykorzystywany do pracy zdalnej musi mieć uruchomioną zaporę sieciową.

§ 8

Procedury bezpieczeństwa podczas pracy zdalnej

1. Zabrania się samodzielnej lub z wykorzystaniem wsparcia podmiotów zewnętrznych naprawy sprzętu służbowego wykorzystywanego do pracy zdalnej. W celu naprawy uszkodzonego sprzętu służbowego należy bezzwłocznie zwrócić go pracodawcy.
2. Zabrania się drukowania dokumentów służbowych w punktach ksero lub z pomocą innych podmiotów czy osób trzecich.
3. Komunikacja z uczniami, rodzicami i innymi klientami jednostki systemu oświaty powinna być prowadzona przede wszystkim za pośrednictwem wdrożonych w jednostce rozwiązań teleinformatycznych, na przykład poprzez dziennik elektroniczny.
4. Pracownik zobowiązany jest do weryfikowania nadawców wiadomości e-mail. W przypadku wątpliwości co do tożsamości nadawcy zabronione jest otwieranie załączników do wiadomości e-mail oraz hiperłączy znajdujących się w tekście.
5. Podczas wysyłania korespondencji zbiorczej pracownik zobowiązany jest do korzystania z opcji „kopia ukryta” (pole UDW – Ukryci Do Wiadomości lub BCC – Blind Carbon Copy), dzięki której odbiorcy wiadomości nie zobaczą wzajemnie swoich adresów e-mail.
6. Pracownik zobowiązany jest do szyfrowania wiadomości e-mailowych zawierających dane osobowe i przekazywania hasła zawsze inną formą, na przykład telefonicznie.
7. Zabronione jest przesyłanie służbowych wiadomości e-mail na prywatne konta e-mail.
8. Zabrania się włączać opcję autouzupełniania formularzy w opcjach przeglądarki internetowej.
9. W przypadku korzystania z przeglądarki internetowej należy sprawdzić informacje o jej zabezpieczeniach. W tym celu należy kliknąć na symbol stanu bezpieczeństwa na lewo od adresu internetowego (Bezpieczna, Informacje lub Niezabezpieczona, Niezabezpieczona lub Niebezpieczna), gdzie wyświetli się informacja o stopniu prywatności połączenia.

§ 9

Dodatkowe zalecenia do pracy zdalnej na prywatnym sprzęcie komputerowym

1. Pracownik zobowiązany jest do stworzenia oddzielnego konta użytkownika systemu w pracy na prywatnym sprzęcie komputerowym, wykorzystywanym do pracy zdalnej. Konto użytkownika powinno posiadać ograniczone uprawnienia i być chronione silnym hasłem oraz nie udostępniane osobom trzecim.
2. Za legalność oprogramowania, w tym programu antywirusowego odpowiada właściciel sprzętu.

3. Po zakończeniu okresu pracy poza miejscem jej stałego wykonywania pracownik jest zobowiązany bezzwłocznie przekazać pracodawcy wszystkie dane związane z wykonywanymi zadaniami służbowymi zapisane na prywatnym sprzęcie (dokumenty służbowe tworzone i przechowywane w pamięci komputera, pliki oraz inne posiadane informacje), a następnie usunąć je w sposób trwały.

§ 10

Bezpieczne przetwarzanie danych osobowych zawartych w dokumentacji papierowej podczas pracy zdalnej

1. Dokumentacja papierowa zawierająca dane osobowe udostępniana jest pracownikowi w zakresie niezbędnym do realizacji obowiązków służbowych podczas pracy zdalnej, za pisemną zgodą pracodawcy.
2. Po otrzymaniu zgody na piśmie pracownik sporządza kopie dokumentów niezbędnych do realizacji jego obowiązków służbowych podczas pracy zdalnej.
3. Zabronione jest zabieranie poza siedzibę pracodawcy oryginałów dokumentów.
4. Po wykonaniu kopii dokumentów pracownik przygotowuje zestawienie określające jakie dokumenty, w jakiej liczbie zostały skopiowane, następnie przekazuje je pracodawcy.
5. Pracodawca prowadzi ewidencje wydanych pracownikom dokumentów zawierających dane osobowe.
6. Podczas przenoszenia dokumentów pracownik zobowiązany jest do odpowiedniego ich zabezpieczenia i przenoszenia w taki sposób, aby były niewidoczne dla osób trzecich, na przykład w teczce wykonanej z nieprzezroczystego materiału.
7. Praca z dokumentami nie może być wykonywana w miejscach publicznych, na przykład w kawiarni, galerii handlowej itp.
8. Podczas pracy zdalnej pracownik zobowiązany jest przechowywać udostępnione kopie dokumentów papierowych tylko przez okres niezbędny do wykonania określonego zadania podczas pracy zdalnej (zasada ograniczenia przetwarzania). Po tym czasie zobowiązany jest niezwłocznie zwrócić je pracodawcy.
9. Po weryfikacji kompletności dokumentów zwróconych przez pracownika, pracodawca brakuje je zgodnie z obowiązującymi przepisami prawa.
10. Zabrania się pracownikowi samodzielnego niszczenia dokumentacji uzyskanej od pracodawcy lub samodzielnie wytworzonej.
11. Pracownik zobowiązany jest zabezpieczyć posiadaną dokumentację i po zakończeniu pracy zdalnej niezwłocznie zwrócić ją do pracodawcy.

§ 11

Naruszenie ochrony danych osobowych podczas pracy zdalnej

1. Pracownik, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym lub w systemie tradycyjnym, zobowiązany jest do niezwłocznego pisemnego poinformowania o tym pracodawcę – administratora danych (załącznik nr 1).

2. W przypadku powzięcia informacji o naruszeniu ochrony danych osobowych Administrator danych prowadzi postępowanie wyjaśniające, podczas którego:
   a. ustala zakres i przyczyny naruszenia ochrony danych osobowych oraz jego ewentualne skutki;
   b. informuje i konsultuje tok postępowania z Inspektorem Ochrony Danych;
   c. podejmuje działania prewencyjne zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.

Zgłoszenie naruszenia ochrony danych osobowych

1. Imię i nazwisko osoby zgłaszającej:
   .....
2. Data i czas zaistnienia/ rozpoczęcia naruszenia
   ……
3. Naruszenie ochrony danych dotyczyło:
   a) zgubienia lub kradzieży nośnika/urządzenia;
   b) dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niebezpiecznej lokalizacji;
   c) korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem nadawcy;
   d) nieuprawnione uzyskanie dostępu do informacji;
   e) nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń;
   f) złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych;
   g) uzyskanie poufnych informacji poprzez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej;
   h) nieprawidłowa anonimizacja danych osobowych w dokumencie;
   i) nieprawidłowe usunięcie/ zniszczenie danych osobowych z nośnika/ urządzenia elektronicznego przed jego zbyciem przez administratora;
   j) niezamierzona publikacja;
   k) dane osobowe wysłane do niewłaściwego odbiorcy;
   l) ujawnienie danych niewłaściwej osobie;
   m) ustne ujawnienia danych osobowych;
   n) inne: …….

4. Szczegółowy opis kategorii osób (np. uczeń) i danych osobowych (np.: imię, nazwisko, data urodzenia, miejsce zamieszkanie, dane dotyczące zdrowia):

   ……
   …….

5. Opis okoliczności naruszenia

   ……
   ……
   ……
   ……
   …….