

**Procedura bezpiecznego przetwarzania danych osobowych
podczas pracy zdalnej w okresie epidemii COVID-19 w Zespole Szkół
Ponadpodstawowych nr 1 w Końskich.**

Celem niniejszej procedury jest zminimalizowanie wysokiego ryzyka naruszenia praw i wolności osób, których dane osobowe są przetwarzane w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19. Procedura ta została opracowana na podstawie przeprowadzonej wcześniej analizy ryzyka i oceny zagrożeń w świetle przepisów rozporządzenia 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 zwane w skrócie „RODO

§ 1.

Postanowienia ogólne

1. Przetwarzanie danych osobowych w ramach pracy zdalnej następuje na podstawie pisemnego polecenia pracy zdalnej wydanego przez pracodawcę.
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 jednostki systemu oświaty, zwłaszcza z polityką bezpieczeństwa przetwarzania danych osobowych i instrukcją zarządzania systemami informatycznymi.
3. Pracownik zobowiązuje się 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.

§ 2.

Bezpieczeństwo obszaru przetwarzania

1. Pracownik zobowiązuje się zorganizować stanowisko do pracy zdalnej w sposób zapewniający bezpieczne i higieniczne warunki pracy.
2. Pracownik jest odpowiedzialny za właściwe zabezpieczenie danych osobowych przetwarzanych przez niego w ramach pracy zdalnej.
3. Pracownik zobowiązany jest do zachowania poufności informacji, na przykład podczas służbowych rozmów telefonicznych lub wideokonferencji.
4. 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.

5. Pracownik zobowiązany jest do uniemożliwienia wglądu osobom postronnym w treści wyświetlane na ekranie sprzętu komputerowego, na przykład poprzez odpowiednie ustawienie ekranu lub zastosowanie filtra prywatyzującego.
6. Pracownik zobowiązany jest do stosowania polityki czystego ekranu, tj. blokowania sprzętu komputerowego w razie oddalenia się od miejsca pracy.
7. Po zakończeniu pracy na sprzęcie elektronicznym należy każdorazowo wylogować się z programów wykorzystywanych do pracy zdalnej oraz z systemu.
8. Pracownik zobowiązuje się do bezpiecznego przechowywania danych osobowych zawartych w dokumentacji w formie papierowej, na przykład w meblach 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 czy hot-spoty 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.
5. Zaleca się zdefiniowanie urządzeń, które mogą uzyskać dostęp do domowej sieci WiFi, na przykład z wykorzystaniem filtracji adresów MAC.

§ 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 niegwarantujących 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. W przypadku udostępniania danych osobowych w programach/platformach wykorzystywanych w pracy zdalnej Administrator danych zobowiązany jest do zawarcia umowy powierzenia przetwarzania danych osobowych. Umowa ta ma zapewniać wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, tak aby przetwarzanie spełniało wymogi wskazane w RODO i chroniło prawa osób, których dane dotyczą.
2. Programy/platformy w przypadku, których nie ma możliwości zawarcia umowy powierzenia przetwarzania danych osobowych nie mogą być wykorzystywane do przetwarzania danych osobowych.
3. W pracy zdalnej zalecane jest korzystanie z aplikacji webowych, nie desktopowych.
4. Przed rozpoczęciem korzystania z programu/platformy wykorzystywanej do pracy zdalnej pracownik zobowiązany jest do zapoznania się z ogólnymi warunkami jej użytkowania oraz polityką prywatności.
5. W przypadku korzystania z programów z funkcją wideokonferencji zaleca się wyłączenie opcji nagrywania i przechowywania.
6. Przy podłączaniu się do programu z funkcją telekonferencji zalecane jest korzystanie z kodów dostępu/PIN-ów.
7. Przed rozpoczęciem korzystania z programów z funkcją telekonferencji zalecane jest przeskanowanie ich systemem antywirusowym lub antymalwareowym.
8. W trakcie korzystania z programów lub platform do pracy zdalnej należy ograniczyć ilość podawanych danych osobowych (zasada minimalizacji danych).
9. W przypadku, kiedy pracownikowi został przydzielony służbowy adres e-mail zabronione jest korzystanie przez niego z prywatnego adresu e-mail do celów służbowych.
10. Zabrania się udostępniania dokumentów służbowych, za pomocą publicznego czatu lub innych komunikatorów.
11. Zabrania się udostępniania w mediach społecznościowych linków do konferencji, prowadzonych zajęć i innych aktywności realizowanych w ramach pracy zdalnej.
12. 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.
13. Należy korzystać z opcji „poczekalnia” tak, aby kontrolować uczestników telekonferencji, w celu uniknięcia przypadkowych lub niechcianych osób.

§ 6.

Bezpieczne przechowywanie danych

1. Nośniki urządzeń mobilnych wykorzystywane w celach służbowych, w tym komputer, telefon lub tablet powinny być zaszyfrowane, na przykład za pomocą hasła.

2. Zewnętrzne karty pamięci, a także inne nośniki danych, takie jak pendrive lub dysk zewnętrzny, wykorzystywane w celach służbowych powinny być szyfrowane za pomocą hasła.
3. Zabronione jest umieszczanie danych osobowych w publicznych chmurach obliczeniowych, komunikatorach lub innych usługach dostępnych w sieci. W przypadku nauczycieli mogą oni jedynie publikować tam materiały edukacyjne, natomiast nie mogą przetwarzać danych osobowych uczniów i ich rodziców.

§ 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 wykorzystywanego do pracy zdalnej. W celu naprawy uszkodzonego sprzętu 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 rozwiązań teleinformatycznych, na przykład poprzez dziennik elektroniczny.
4. Pracownik zobowiązany jest do weryfikowania nadawców wiadomości e-mailowych oraz w przypadku wątpliwości do nieotwierania załączników oraz hiperłączy znajdujących się w tekście.
5. Podczas wysyłania korespondencji zbiorczej należy korzystać 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-mailowe.
8. Zabrania się włączać opcję autouzupelniania formularzy w opcjach przeglądarki internetowej.
9. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki „kłódka”. W tej sytuacji należy „kliknąć” na ikonę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.

§ 9.

Dodatkowe zalecenia do pracy zdalnej na prywatnym sprzęcie komputerowym

1. Zalecane jest stworzenie oddzielnego konta użytkownika systemu w pracy na prywatnym sprzęcie, 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 zapisane na prywatnym sprzęcie (dokumenty służbowe tworzone i przechowywane w pamięci komputera, pliki oraz inne posiadane informacje) związane z wykonywanymi zadaniami służbowymi, 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 w zakresie pracy zdalnej, za zgodą pracodawcy.
2. Pracodawca zapewnia ewidencjonowanie wydanych pracownikom dokumentów zawierających dane osobowe.
3. Pracownik zobowiązany jest przechowywać udostępnione dokumenty papierowe przez okres niezbędny do wykonania określonego zadania podczas pracy zdalnej (zasada ograniczenia przetwarzania). Po tym czasie zobowiązany jest niezwłocznie zwrócić je pracodawcy.
4. Podczas przenoszenia dokumentów pracownik zobowiązany jest do odpowiedniego ich zabezpieczenia i przenoszenia dokumentów w taki sposób, aby były niewidoczne dla osób trzecich, na przykład w zabezpieczonej teczce.
5. Pracownik zobowiązany jest do bezpiecznego niszczenia dokumentów papierowych, na przykład za pomocą niszczarki do dokumentów. Jeżeli pracownik nie posiada niszczarki dokumentów, powinien dokumenty zabezpieczyć, a po zakończeniu pracy zdalnej niezwłocznie zniszczyć je w siedzibie pracodawcy.
6. Zabrania się pracownikowi wyrzucania papierowych dokumentów służbowych do domowego kosza na śmieci.

§ 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 administratora danych.

2. W przypadku powzięcia informacji o naruszeniu ochrony danych osobowych Administrator danych prowadzi postępowanie wyjaśniające w toku, którego:
 - 1) ustala zakres i przyczyny naruszenia ochrony danych osobowych oraz jego ewentualne skutki;
 - 2) informuje i konsultuje tok postępowania z Inspektorem Ochrony Danych;
 - 3) podejmuje działania prewencyjne zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.
3. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorcemu – Urząd Ochrony Danych Osobowych oraz w pewnych przypadkach powiadamia osoby, których dane dotyczą.
4. Jeżeli przyczyną naruszenia zasad ochrony danych osobowych było zaniedbanie ze strony pracownika, administrator może wyciągnąć konsekwencje dyscyplinarne wynikające z regulaminu pracy.
5. Zabrania się świadomego lub nieumyślnego wywoływania naruszeń przez osoby upoważnione do przetwarzania danych.