



ZWIĄZEK NAUCZYCIELSTWA POLSKIEGO

ROK ZAŁOŻENIA 1905

ZARZĄD GŁÓWNY

00-389 Warszawa, ul. Smulikowskiego 6/8
tel. (22) 318 91 00, 318 92 17, fax (22) 318 92 19
www.znp.edu.pl e-mail: znp@znp.edu.pl

Praca zdalna nauczycieli

w kontekście 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 (RODO).

wersja pełna

W związku z nagłym powstaniem obowiązku pracy zdalnej nauczycieli (podobnie jak milionów innych pracowników) w wyniku polecenia wydanego przez pracodawcę na podstawie art. 3 ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych z dnia 2 marca 2020 r. (Dz.U. z 2020 r. poz. 374), należy zauważyć, że:

1. Polecenie wykonywania pracy zdalnej nie oznacza, że nie podlega ona innym przepisom, w szczególności Kodeksu pracy i 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) (dalej: “**RODO**”).
2. Art. 32 ust. 1 i 2 RODO nakazuje dostosowanie technicznych i organizacyjnych środków bezpieczeństwa do rodzaju przetwarzania i związanego z tym ryzyka, czyli gdy rośnie ryzyko, poziom stosowanych środków bezpieczeństwa powinien być wyższy.
3. Do ustalenia obowiązków administratora danych osobowych (organu prowadzącego jednostkę oświatową) oraz warunków powierzenia nauczycielom przetwarzania

danych w związku z nauczaniem zdalnym zastosowanie mają m. in. art. 4 pkt 7 i 8, art. 24, 25, 28 i 29 RODO oraz motywy 74 i 78 RODO.

4. Zmiany funkcjonowania placówek oświatowych w związku z zagrożeniem COVID-19 określa rozporządzenie MEN z 20 marca 2020 r. (dalej **“Rozporządzenie MEN”**) w sprawie szczególnych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz. U. 2020, poz. 493, ze zmianami z 25 marca 2020 r. Dz. U. 2020 poz. 530 i 10 kwietnia 2020 r. Dz. U. 2020 poz. 657):
 - § 1 Rozporządzenia MEN reguluje obowiązki dyrektora szkoły w zakresie organizacji nauczania zdalnego,
 - § 2 Rozporządzenia MEN określa zalecane materiały, które mogą być wykorzystane w nauczaniu zdalnym,
 - § 8 i 9 Rozporządzenia MEN określa udostępnienie Zintegrowanej Platformy Edukacyjnej,
 - § 6 ust. 3 i 4 Rozporządzenia MEN reguluje użyczenie nauczycielom i uczniom sprzętu niezbędnego do realizacji nauczania zdalnego.
5. Za określenie warunków bezpiecznego przetwarzania danych osobowych i ich zapewnienie odpowiada administrator danych i nie może on na nikogo (w szczególności na pracowników) przerzucić tej odpowiedzialności.
6. W obecnej sytuacji pandemii koronawirusa występują warunki szczególne. Zapewnienie warunków pełnego bezpieczeństwa przetwarzania danych przy nauczaniu zdalnym w wielu przypadkach będzie niewykonalne. Jednakże to do administratora należy dokonanie analizy sytuacji, zidentyfikowanie zagrożeń dla bezpieczeństwa przetwarzania danych i praw osób, których dane są przetwarzane, możliwych do zastosowania środków ochrony oraz określenie zalecanych oraz dopuszczalnych warunków, w jakich nauczyciele (i inni pracownicy) mają wykonywać pracę zdalną. Taka analiza powinna stanowić podstawę do podejmowania decyzji i przekazywania ich pracownikom.
7. Administrator danych powinien opracować odpowiednie instrukcje, dostosowane do możliwych do wykorzystania środków przetwarzania danych; odpowiednie, dostosowane do tych warunków materiały informacyjne i zapoznać z nimi osoby, którym poleca wykonywanie pracy zdalnej. Instrukcje powinny przewidywać różne warianty wykonywania pracy zdalnej, zależnie od możliwości technicznych i organizacyjnych pracodawcy i pracownika oraz dostępnych łącz internetowych.

8. Pracownicy powinni stosować się do zasad przetwarzania danych obowiązujących u pracodawcy w zakresie, w jakim zostali przeszkoleni i dopuszczeni do przetwarzania danych, uwzględniając szczególne warunki przetwarzania będące wynikiem pandemii.
9. Pracownicy nie mogą przy tym ponosić negatywnych dla siebie skutków, gdy ze względu na brak możliwości spełnienia przez nich warunków bezpiecznego przetwarzania, wystąpią zagrożenia lub incydenty ochrony danych osobowych, jeśli się do tego nie przyczynili, ani nie mogą być nakłaniani do podpisywania oświadczeń niejasnych i nakładających na nich niedookreślone lub niemożliwe do spełnienia obowiązki.
10. Administrator danych przed poleceniem pracownikom wykonywania przetwarzania danych osobowych, w warunkach pracy zdalnej, powinien dokonać inwentaryzacji zasobów, jakie mogą być oddane do ich dyspozycji lub są w ich posiadaniu i mogą być do zleconego przetwarzania użyte, w szczególności:
 - a) dostępnego sprzętu komputerowego,
 - b) dostępnych łącz internetowych,
 - c) dostępnych aplikacji możliwych do zastosowania w pracy zdalnej,
 - d) umiejętności pracowników w zakresie pracy zdalnej i nauczania przy użyciu technik informatycznych, oraz możliwości uzyskania wsparcia informatycznego.
11. W zakresie sprzętu komputerowego pracodawca, zależnie od możliwości, powinien:
 - a) zapewnić pracownikom sprzęt służbowy odpowiednio wyposażony i zabezpieczony, lub
 - b) powierzyć do wykonywania pracę na sprzęcie będącym własnością, lub w wyłącznej dyspozycji pracownika, jeśli pracownik dysponuje takimi możliwościami i może być zapewniony odpowiedni poziom bezpieczeństwa przetwarzania danych, lub
 - c) zdecydować o możliwości wykonania, formie i zasadach pracy zdalnej pracownika, który współdzieli sprzęt prywatny z innymi osobami, lub nie dysponuje takim sprzętem,
 - d) udzielić wsparcia w zakresie konfiguracji i zabezpieczenia sprzętu wykorzystywanego do pracy zdalnej.
12. W zakresie łącz internetowych pracodawca, zależnie od możliwości, powinien:
 - a) zezwolić pracownikowi na wykorzystanie łącza prywatnego o właściwych parametrach i zabezpieczeniach (np. łącza stałe renomowanych dostawców i właściwie skonfigurowany router z firewallem),

- b) zaopatrzyć pracownika w służbowe łącze internetowe (np. mobilne) zapewniające odpowiednie bezpieczeństwo przesyłu danych i minimalną konieczną do wyznaczonych zadań jakość,
 - c) jeśli pracownik ma dostęp jedynie do łącz o niskiej jakości i niepewnym bezpieczeństwie, w szczególności łącz ogólnodostępnych, otwartych, niezabezpieczonych, pracodawca powinien zdecydować, czy takie łącze może być wykorzystywane, na jakich zasadach i zapewnić odpowiednie wsparcie w celu zapewnienia bezpiecznej transmisji danych (np. utworzenie VPN), lub
 - d) zdecydować o innej formie pracy zdalnej pracownika,
 - e) udzielić wsparcia w zakresie konfiguracji łącza, routera, utworzenia VPN itp., w celu zapewnienia bezpieczeństwa transmisji.
13. W zakresie dostępu do danych osobowych przetwarzanych na polecenie pracodawcy przez pracownika, pracodawca powinien:
- a) wyspecyfikować zbiory danych, rodzaj danych, grupy osób, których dane będą przetwarzane przez pracownika, zakres przetwarzania,
 - b) określić zasoby, do których pracownik ma mieć dostęp (serwery, bazy, katalogi, aplikacje itp.),
 - c) określić, na jakim sprzęcie dane będą przetwarzane przez pracownika,
 - d) określić drogę jaką będzie dokonywana transmisja (jakie łącza pracownika, VPN, kanały transmisji itp.),
 - e) określić jakie zabezpieczenia możliwe do zastosowania będą wymagane.
14. Łączenie z infrastrukturą firmową.
- a) Najwłaściwszą dla bezpieczeństwa danych formą pracy zdalnej jest praca na aplikacjach firmowych zainstalowanych na serwerze firmowym lub w chmurze, z wykorzystaniem komputera, jako pulpitu zdalnego, i połączenia tunelowego;
 - b) Mniej bezpieczne jest przetwarzanie w aplikacjach zainstalowanych na komputerze, lecz zapisywanie i udostępnianie plików na dysku sieciowym np. udostępnionym w aplikacji chmurowej;
 - c) Najmniej wskazane i najmniej bezpieczne jest zapisywanie danych na dysku lokalnym komputera i nośnikach zewnętrznych oraz przysyłanie plików przez Internet.
15. W zakresie przeszkolenia i poinformowania w sprawach ochrony danych osobowych pracodawca powinien:

- a) zweryfikować, czy pracownicy odbyli właściwe szkolenie w zakresie ochrony danych oraz podpisali oświadczenia o odbyciu przeszkolenia i zobowiązaniu się do ich stosowania przy przetwarzaniu danych osobowych;
- b) jeżeli przeszkolenie nie obejmowało ochrony danych osobowych przy pracy zdalnej, uzupełnić szkolenie w tym zakresie, np. z pomocą webinarów, szkolenia on-line, dostarczenia materiałów szkoleniowych;
- c) przeszkolić lub dostarczyć materiały informacyjne dotyczące szczegółów pracy zdalnej, w szczególności dostosowane do specjalnych okoliczności związanych z pandemią i na bieżąco je aktualizować, oraz
- d) uzyskać od pracownika potwierdzenie zapoznania się z tymi zasadami i zobowiązanie do ich stosowania (np. drogą mailową);
- e) na bieżąco śledzić proces przetwarzania, pojawiające się zagrożenia i informować o nich pracujących zdalnie.

16. W zakresie wydawania polecenia przetwarzania danych pracodawca powinien:

- a) zweryfikować zakres poleceń (instrukcji) przetwarzania danych wydanych pracownikowi,
- b) określić zasady, na jakich ma być wykonywana praca zdalna związana z przetwarzaniem danych osobowych z uwzględnieniem specyficznych warunków, w jakich pracownik będzie dokonywał przetwarzania danych osobowych,
- c) uzyskać od pracownika potwierdzenie, że warunki dokonywania przetwarzania przy pracy zdalnej określone przez pracodawcę mogą być spełnione,
- d) wydać nowe lub dodatkowe polecenie (instrukcje) związane ze zmienionymi warunkami przetwarzania,
- e) odebrać potwierdzenie otrzymania polecenia (instrukcji) przetwarzania oraz zobowiązanie do stosowania się do obowiązujących zasad przetwarzania danych w warunkach pracy zdalnej,
- f) jeśli to konieczne, wydać nowe upoważnienie do przetwarzania danych.

17. W zakresie zapewnienia ochrony danych osobowych administrator powinien:

- a) Dokonać przeglądu Polityki ochrony danych osobowych i wprowadzić niezbędne aktualizacje i uzupełnienia, jeśli ze względu na pracę zdalną w warunkach zagrożenia pandemią koronawirusa, są w tej części nieaktualne. W szczególności należy wprowadzić zmiany dotyczące dokumentowania czynności w warunkach izolacji pracowników spowodowanej obowiązującymi zarządzeniami władz

publicznych, zwłaszcza dotyczące stosowanie doręczeń i poświadczeń drogą elektroniczną;

- b) Na bieżąco śledzić proces przetwarzania, identyfikować pojawiające się nieprawidłowości i zagrożenia oraz przeciwdziałać im,
 - c) Zapewnić pracownikom wykonującym pracę zdalną niezbędne wsparcie techniczne i merytoryczne (np. porady on-line);
 - d) Na bieżąco aktualizować dokumentację związaną z przetwarzaniem (Rejestr czynności przetwarzania, wykaz zbiorów, ewidencję upoważnionych do przetwarzania, ewidencję nośników danych itd.);
 - e) Prowadzić ewidencję przetwarzających przy pracy zdalnej, zapewniającą zasób informacji koniecznych do zapewnienia bezpiecznego przetwarzania (osoby, sprzęt, łącza, aplikacje);
 - f) Po zakończeniu pracy zdalnej przez pracownika należy w zależności od sytuacji: odebrać sprzęt służbowy, wyłączyć dostęp do niepotrzebnych zasobów, aplikacji i baz danych, zobowiązać do usunięcia niepotrzebnych danych z komputera lub innego urządzenia własnego, czy nośnika danych i odebrać oświadczenie o usunięciu danych z wszelkich prywatnych nośników danych.
18. Pracownicy, z uwzględnieniem dostępności środków, powinni stosować się możliwie ściśle do zaleceń i instrukcji pracodawcy, zwracać przy wykonywaniu pracy zdalnej szczególną uwagę na bezpieczeństwo przetwarzania, w szczególności:
- a) Przed przystąpieniem do pracy zdalnej pracownik powinien być przeszkolony (lub otrzymać niezbędne informacje) w zakresie zleconej pracy zdalnej, czynności jakie ma wykonywać, środków jakie ma stosować, zasad bezpieczeństwa, które jest obowiązany stosować;
 - b) prywatne urządzenie, jeśli ma być użyte do pracy zdalnej, powinno mieć legalne i możliwie aktualne oprogramowanie (nie pirackie i nie pochodzące z nielegalnych źródeł, zwłaszcza internetowych). Powinien być zainstalowany i aktualizowany program antywirusowy. Nie można używać komputera, który jest używany do odwiedzania niebezpiecznych serwisów internetowych (nielegalne gry, nielegalne lub niepewnego pochodzenia programy, erotyczne itp.);
 - c) Najlepiej, gdy z komputera służącego do pracy zdalnej nie korzystają inni domownicy. Jeśli to niemożliwe, należy przy konieczności zapisywania plików na dysku komputera stworzyć odrębny folder, dostęp do którego będzie miała tylko osoba pracująca zdalnie z tymi danymi (zahasłowany lub zaszyfrowany);

- d) Przy przerwach w pracy oraz po zakończeniu pracy zdalnej z aplikacjami, należy się z tych aplikacji lub z komputera wylogowywać. Pozostawianie bez nadzoru niezabezpieczonego komputera podczas pracy zdalnej jest niedopuszczalne;
- e) Najlepiej korzystać z pewnych, stałych łącz internetowych (światłowodowe, kablowe), pochodzących od renomowanych dostawców. Szczególną uwagę na bezpieczeństwo należy zwracać przy korzystaniu z usług lokalnych dostawców Internetu radiowego;
- f) Sieć wewnętrzna powinna być właściwie skonfigurowana, domyślne hasła administratora routera zmienione, wskazane jest używanie routera z firewallem;
- g) Wewnętrzna sieć wifi musi być zamknięta i zabezpieczona, zaś hasła do sieci silne i nieujawniane innym osobom (np. sąsiadom);
- h) Korzystanie z publicznych sieci wifi jest niebezpieczne i poza wyjątkowymi sytuacjami powinno być zabronione. Zagrożeniem może być zarówno administrator takiej sieci, jak i łatwość podszycia się hakerów pod sieć publiczną. Grozi to przechwyceniem danych oraz instalacją programów szpiegujących;
- i) Należy unikać przesyłania plików z danymi osobowymi lub poufnymi, jako załączników do maili. Lepszym rozwiązaniem jest udostępnianie ich w aplikacjach chmurowych. Jeśli jednak konieczne jest wysłanie pliku mailem, wysyłany plik powinien być zaszyfrowany (np. zip lub rar z hasłem), zaś hasło do pliku musi być przekazane innym środkiem komunikacji, np. SMS (nie w innym mailu);
- j) Należy zgłaszać pracodawcy (lub wyznaczonemu przez niego Inspektorowi Ochrony Danych Osobowych) wszelkie zaobserwowane zagrożenia dla bezpieczeństwa danych, nietypowe lub podejrzanе zachowanie aplikacji itp. jak również sytuacje, gdy pracownik nie jest w stanie wypełnić nałożonych na niego obowiązków w zakresie ochrony danych i ich przetwarzania;
- k) Po zakończeniu okresu pracy zdalnej należy na wszystkich używanych nośnikach danych (w tym chmurowych i przenośnych) dokonać przeglądu zapisanych plików zawierających dane używane do celów służbowych i je trwale usunąć.

Krzysztof Stradomski

Inspektor Ochrony Danych

Związku Nauczycielstwa Polskiego

we współpracy z Kancelarią Adwokacką Wachowski