# ZARZĄDZENIE WEWNĘTRZNE NR 7/2020

# DYREKTORA ZSP W SŁOTWINIE

# z dnia 03.04.2020 r.

## w sprawie: wprowadzenia procedury dotyczącej warunków ochrony danych osobowych w trakcie pracy/nauki zdalnej

Na podstawie art. 24 ust. 1Rozporządzenia 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 - RODO) o raz ustawę z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. 2020 poz. 374 z późn. zm.) zarządzam, co następuje:

**§ 1.** Wprowadza się do stosowania procedurę dotyczącą ochrony danych osobowych w trakcie pracy / nauki zdalnej.

**§ 2.** Warunki ochrony danych osobowych w trakcie pracy / nauki zdalnej

1. Zobowiązuje się osoby wykonujące czynności zdalnie do zabezpieczania dostępu do sprzętu oraz posiadanych danych i informacji (w tym także znajdujących się na nośnikach papierowych) przed osobami postronnymi (w tym wspólnie z nim zamieszkującymi) oraz przed zniszczeniem **zgodnie z załącznikiem nr 1.**
2. Wykonywanie pracy w formie zdalnej nie zwalnia z obowiązku przestrzegania przepisów o ochronie danych osobowych.
3. Urządzenia (prywatne i służbowe) wykorzystywane do pracy / nauki zdalnej oraz organizacja muszą być zabezpieczone – przykładowy wykaz zabezpieczeń stanowi **załącznik nr 2**.
4. Na ogólnie dostępnych portalach lub stronach internetowych nauczyciel może jedynie publikować materiały edukacyjne, natomiast nie może przetwarzać danych osobowych uczniów lub rodziców.

**§ 3.** Pozyskanie danych osobowych i przekaz informacji

1. Placówka może wymagać od ucznia lub reprezentującego go rodzica (opiekuna prawnego) podania danych do założenia konta w systemie zdalnego nauczania, tylko w zakresie niezbędnym do tego, aby to konto założyć na podstawie art. 35 ustawy Prawa oświatowego w związku z art. 6 ust. 1 lit e RODO. Nie wolno gromadzić danych nadmiarowych bądź służących do realizacji innych celów.
2. Nauczyciel może przetwarzać dane osobowe uczniów i ich rodziców tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.
3. Rodzic (opiekun prawny) ma prawo wiedzieć, jak szkoła jako administrator będzie przetwarzała dane osobowe jego dziecka w trakcie nauki zdalnej oraz jakie w związku z tym przysługują mu prawa. Informacje należy przekazać drogą elektroniczną z wykorzystaniem poczty elektronicznej lub dzienników elektronicznych.
4. O sposobie realizacji nauki zdalnej należy powiadomić w prosty sposób, tak aby była zrozumiała dla wszystkich, do których skierowany jest komunikat. Jeżeli w celu realizacji nauki zdalnej będzie korzystać z nowych narzędzi lub usług świadczonych przez podmioty zewnętrzne, to należy poinformować o tym Rodziców oraz w jakim zakresie będą przetwarzane dane osobowe.

**§ 4.** Rozwiązania teleinformatyczne wykorzystane do pracy zdalnej

1. Wybór właściwego narzędzia do pracy / nauki zdalnej należy do Dyrektora, który podejmuje decyzje w porozumieniu z nauczycielem, przy uwzględnieniu wszystkich aspektów związanych z możliwościami Placówki, a przede wszystkim, biorąc pod uwagę możliwości techniczne i organizacyjne rodziców i uczniów.
2. Komunikację z uczniami i rodzicami w podstawowym zakresie prowadzi się poprzez już wdrożone w placówce rozwiązania teleinformatyczne, np. dzienniki elektroniczne, z którymi placówka ma podpisaną umowę powierzenia przetwarzania danych. Można również korzystać z innych usług dostawców zewnętrznych po ustaleniu zasad przetwarzania danych osobowych.
3. Po wyborze aplikacji lub innych narzędzi wykorzystywanych do zdalnej edukacji bądź komunikacji z uczniami należy sprawdzić zasady świadczenia usługi i zasady przetwarzania danych przez usługodawcę (politykę prywatności, umowy powierzenia przetwarzania danych, klauzule informacyjne) i przekazać do konsultacji Inspektorowi Ochrony Danych.
4. Do prowadzenia zajęć i komunikacji można wykorzystać również:
5. pocztę elektroniczną (służbową lub prywatną), z której należy korzystać w sposób bezpieczny, przede wszystkim podczas wysyłania korespondencji zbiorczej powinno się korzystać z opcji „UDW”, dzięki której odbiorcy wiadomości nie będą widzieć wzajemnie swoich adresów e-mail.
6. aplikacje i inne narzędzie do nauki zdalnej oraz do przeprowadzania telekonferencji
7. komunikatory internetowe kiedy komunikacja nie dotyczy przekazywania informacji zawierających dane osobowe
8. Po wyborze aplikacji lub innych narzędzi wykorzystywanych do zdalnej edukacji bądź komunikacji z uczniami należy sprawdzić i przekazać zasady świadczenia usługi i zasady przetwarzania danych przez usługodawcę (politykę prywatności, umowy powierzenia przetwarzania danych, klauzule informacyjne) do konsultacji Inspektorowi Ochrony Danych.

**§ 5.** Zarządzenie wchodzi w życie z dniem 03.04.2020 r.

**Załącznik nr 1** Oświadczenie o poufności i stosowaniu zabezpieczeń

|  |  |  |
| --- | --- | --- |
| ...........................................  imię i nazwisko (pismo drukowane) |  |  |

**OŚWIADCZENIE**

W związku z możliwością wykonywania pracy zdalnej niniejszym zobowiązuję się do zachowania w poufności i nieujawniania oraz nieudostępniania w jakikolwiek sposób, formie lub zakresie informacji lub danych mających charakter poufny („Informacje Poufne”), uzyskanych w trakcie lub w związku z wykonywaniem Umowy, w szczególności w zakresie przetwarzanych danych osobowych oraz sposobów ich zabezpieczenia, a także niepodejmowania działań lub zaniechań mogących skutkować:

1. ujawnieniem informacji poufnych takich jak:
2. dane osobowe zgodnie z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j.: Dz. U. z 2018 r., poz. 1000 ze zm.) 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 - RODO)
3. bazy danych zgodnie z ustawą z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. Nr 128, poz. 1402);
4. inne uzyskane przy wykonywaniu Umowy, których ujawnienie mogłoby na szkodę
5. sposoby obsługi i ochrony informacji poufnych stosowanych
6. uzyskaniem dostępu do informacji, o których mowa w pkt 1, przez osoby nieuprawnione,
7. wykorzystaniem informacji, o których mowa w pkt 1, w celach sprzecznych z prawem,
8. nieuprawnioną modyfikacją, utratą lub zniszczeniem informacji, o których mowa w pkt 1,
9. naruszeniem zabezpieczeń przetwarzania danych, telekomunikacyjnych oraz ochrony fizycznej, zakłóceniami w ich pracy lub nieuprawnionym uzyskaniem informacji o sposobie ich działania.

Powyższe zobowiązanie przyjmuję na siebie dobrowolnie i bezterminowo.

Jednocześnie zobowiązuję się do niezwłocznego informowania o wystąpieniu któregokolwiek z naruszeń, o których mowa w pkt 1-5.

Oświadczam, że zostałem/łam poinformowany/na o odpowiedzialności karnej i cywilnej, w tym wynikającej z ustawy o ochronie danych osobowych, za niedotrzymanie przeze mnie wskazanych wyżej zobowiązań.

|  |  |
| --- | --- |
|  |  |
|  | .......................................................  data i czytelne imię i nazwisko osoby składającej oświadczenie |

**Załącznik nr 2** „20 zasad bezpieczeństwa lekcji on-line”

1. Na bieżąco aktualizuj systemy operacyjne.
2. Systematycznie aktualizuj programy antywirusowe.
3. Regularnie skanuj stacje robocze programami antywirusowymi.
4. Pobieraj oprogramowanie wyłącznie ze stron producentów.
5. Nie otwieraj załączników z nieznanych źródeł dostarczanych poprzez korespondencję elektroniczną.
6. Nie zapamiętuj haseł w aplikacjach webowych.
7. Nie zapisuj haseł na kartkach.
8. Nie używaj tych samych haseł w różnych systemach informatycznych.
9. Zabezpieczaj serwery plików czy inne zasoby sieciowe.
10. Zabezpieczaj sieci bezprzewodowe.
11. Dostosuj złożoność haseł odpowiednio do zagrożeń.
12. Unikaj wchodzenia na nieznane czy przypadkowe strony internetowe.
13. Nie loguj się do systemów informatycznych w przypadkowych miejscach z niezaufanych urządzeń lub publicznych niezabezpieczonych sieci Wi-Fi.
14. Wykonuj regularne kopie zapasowe.
15. Korzystaj ze sprawdzonego oprogramowania do szyfrowania e-maili lub nośników danych.
16. Szyfruj dane przesyłane pocztą elektroniczną.
17. Szyfruj dyski twarde w komputerach przenośnych.
18. Przy pracy zdalnej korzystaj z szyfrowanego połączenia VPN.
19. Odchodząc od komputera, blokuj stację komputerową.
20. Nie umieszczaj w komputerze przypadkowo znalezionych nośników USB.