



**SZKOŁA PODSTAWOWA
IM. KARDYNAŁA STEFANA WYSZYŃSKIEGO W NASUTOWIE**

Nasutów 209A, 21-025 Niemce

tel./fax: (81) 756 - 64 - 75

e-mail: nasutowszkola@interia.pl, www.nasutowszkola.edupage.org

NIP 713-24-99-738; Regon: 001151735

*Załącznik nr do ZARZĄDZENIA NR 16/2020/2021
DYREKTORA SZKOŁY PODSTAWOWEJ IM. KARDYNAŁA STEFANA
WYSZYŃSKIEGO W NASUTOWIE z dnia 16 października 2020 r. w
sprawie wprowadzenia do stosowania „Regulamin pracy zdalnej
przy przetwarzaniu danych osobowych w Szkole Podstawowej im.
Kardynała Stefana Wyszyńskiego w Nasutowie będącej
administratorem danych osobowych”*

**Regulamin pracy zdalnej przy
przetwarzaniu danych osobowych
w Szkole Podstawowej
im. Kardynała Stefana Wyszyńskiego
w Nasutowie
będącej administratorem danych
osobowych**

Nasutów, 16 października 2020 rok

„Regulamin pracy zdalnej przy przetwarzaniu danych osobowych w Szkole Podstawowej im. Kardynała Stefana Wyszyńskiego w Nasutowie będącej administratorem danych osobowych”

§ 1. Osoby objęte regulaminem

1. Niniejszy regulamin pracy zdalnej przy przetwarzaniu danych osobowych (zwany dalej regulaminem) dotyczy wszystkich pracowników administratora danych osobowych (ADO) oraz innych osób wykonujących na podstawie jakiegokolwiek umowy cywilnoprawnej zadania na rzecz ADO w miejscu ich stałego wykonywania wyznaczonego przez ADO (dalej: pracownicy).
2. Osoby wskazane w ust. 1 powinny niezależnie od niniejszego regulaminu przestrzegać innych procedur ochrony danych osobowych obowiązujących u ADO, w tym także polityki bezpieczeństwa.

§ 2. Rola inspektora ochrony danych (lub innej osoby wyznaczonej przez ADO)

1. Inspektor ochrony danych (IOD) ma prawo do organizowania i przeprowadzania szkoleń oraz wydawania pracownikom wskazówek dotyczących stosowania niniejszego regulaminu.
2. IOD ma prawo przekazywać pracownikom wytyczne doprecyzowujące stosowanie niniejszego regulaminu. Powyższe wytyczne może on opracowywać we współpracy z Dyrektorem Departamentu Informatyki.
3. Każdy pracownik może kierować do IOD pytania dotyczące ochrony danych osobowych podczas pracy zdalnej.

§ 3. Upoważnienie do przetwarzania danych osobowych

1. Każdy pracownik może przetwarzać dane osobowe dopiero na wyraźne polecenie ADO.
2. ADO może wydawać i zmieniać pracownikom upoważnienie do przetwarzania danych osobowych.
3. W upoważnieniu, o którym mowa w ust. 2 ADO, określa zwłaszcza:
 - 1) cele przetwarzania danych osobowych;
 - 2) czynności przetwarzania danych osobowych;
 - 3) nazwę systemu, w którym te dane są przetwarzane;
 - 4) zakres uprawnień związanych z dostępem do danego systemu oraz
 - 5) okres obowiązywania upoważnienia.
4. Upoważnienie, o którym mowa w ust. 2, może być wydane wyłącznie w celu zastępstwa i obowiązywać wyłącznie w różnych okresach nieobecności osoby pierwotnie upoważnionej.

5. (Departament Informatyki) oraz IOD dokonają przeglądu wszystkich dotychczas udzielonych upoważnień do dnia 30 października 2020 roku i prześlą dyrektorowi szkoły wzory upoważnień, które wymagają aktualizacji pod kątem pracy zdalnej.
6. Każdy pracownik, który w związku z przejściem na pracę zdalną zaobserwuje konieczność rozszerzenia nadanego mu upoważnienia, powinien niezwłocznie zgłosić ten fakt do dyrektora szkoły

§ 4. Postępowanie z powierzoną infrastrukturą

1. Wszelkie dokumenty, oprogramowanie oraz sprzęt powierzony pracownikowi w celu zdalnego wypełniania swych obowiązków (dalej: infrastruktura) należy traktować zgodnie z zapisami niniejszego paragrafu.
2. Powierzoną infrastrukturę pracownik może wykorzystywać wyłącznie w celu wypełniania swoich obowiązków pracowniczych. Pracownikowi nie wolno w szczególności instalować bez zgody pracodawcy żadnego oprogramowania ani aplikacji.
3. Pracownik zobowiązany jest do niezwłocznego zgłaszania do Departamentu Informatyki (DI) wszelkich problemów związanych z eksploatacją powierzonej infrastruktury informatycznej.
4. Dyrektor DI ma prawo dokonywać zmian w powierzonej pracownikowi infrastrukturze w celu zabezpieczenia jej oraz danych osobowych przetwarzanych za jej pomocą.
5. Pracownik ma obowiązek niezwłocznie wykonywać polecenia Dyrektora DI w zakresie działań niezbędnych do zabezpieczenia powierzonej infrastruktury informatycznej, w szczególności takich jak dokonywanie niezbędnych aktualizacji lub instalacja dodatkowego oprogramowania.
6. Pracownik ma obowiązek dbać o bezpieczeństwo powierzonej infrastruktury, a w szczególności:
 - 1) przechowywać powierzony sprzęt tak, aby używając go lub przewożąc, nie dopuścić do jego zgubienia ani zniszczenia;
 - 2) zabezpieczać infrastrukturę tak, aby osoby postronne, w tym osoby bliskie pracownika, nie miały dostępu do danych osobowych, które pracownik przetwarza w toku pracy zdalnej, w szczególności poprzez schowanie powierzonej infrastruktury w bezpiecznym miejscu;
 - 3) zabezpieczać infrastrukturę przed działaniem czynników naturalnych, takich jak zbyt wysoka lub zbyt niska temperatura czy też wilgoć;
 - 4) ustalić hasło zabezpieczające dostęp do komputerów i urządzeń przenośnych, składające się co najmniej z 8 liter, w tym przynajmniej jednej dużej, i 2 znaków specjalnych;
 - 5) aktualizować wszystkie hasła przynajmniej raz w miesiącu;

- 6) zapewnić powierzonemu sprzętowi możliwość automatycznej blokady wymagającej ponownego wpisania hasła i pojawiającej się po 5 minutach bezczynności;
- 7) po zakończeniu zdalnych połączeń sprawdzać, czy nastąpiło rozłączenie, oraz wyłączać kamerę w razie jej wykorzystywania;
- 8) przysyłać dokumenty papierowe wyłącznie w zabezpieczonych, nieprześwitujących kopertach.

§ 5.Praca z pocztą elektroniczną

1. Podczas komunikacji związanej ze świadczeniem pracy zdalnie każdy pracownik zobowiązany jest wykorzystywać wyłącznie swój służbowy adres e-mail.
2. W razie problemów technicznych związanych z wykorzystaniem służbowego adresu e-mail pracownik powinien niezwłocznie zgłosić ten problem na zasadach opisanych w § 4 ust. 3, a z adresu e-mail innego niż służbowy korzystać tylko w nagłych wypadkach, po uprzednim zabezpieczeniu treści oraz załączników zgodnie ze wskazówkami Dyrektora DI.
3. W przypadku wysyłania plików zawierających dane osobowe (*np. dotyczące stanu zdrowia*) plik taki powinien zostać uprzednio zaszyfrowany za pomocą hasła składającego się co najmniej z 8 liter, w tym przynajmniej jednej dużej, i 2 znaków specjalnych.
4. Jeżeli jakiegokolwiek zawarte w treści wiadomości e-mail informacje zostały zabezpieczone hasłem, takiego hasła nie można wysyłać w tej samej wiadomości.
5. Pracownik powinien zwrócić szczególną uwagę na bezpieczeństwo przetwarzanych w ramach korespondencji elektronicznej danych osobowych, a w szczególności:
 - 1) dokładnie sprawdzać automatyczne sugestie przy nazwie adresata;
 - 2) unikać otwierania podejrzanych wiadomości od nieznanymi adresatów, w tym klikania w zawarte w nich linki;
 - 3) unikać otwierania podejrzanych załączników zawartych w wiadomościach e-mail;
 - 4) zgłaszać niezwłocznie wiadomości pochodzące z adresów podejrzanie podobnych do adresów, których używa na co dzień;

§ 6.Zasady przeprowadzania wideokonferencji z osobami z zewnątrz

1. Podczas komunikacji w ramach wideokonferencji pracownicy powinni zachować zasady bezpieczeństwa, a w szczególności:
 - 1) zadbać o to, aby wszelkie przetwarzane dane osobowe pozostały niewidoczne dla osób, z którymi rozmawiamy;
 - 2) po zakończeniu zdalnych połączeń sprawdzać, czy nastąpiło rozłączenie, oraz wyłączać kamerę w razie jej wykorzystania;

- 3) dopuszczać do wideokonferencji wyłącznie osoby znające ustalone wcześniej hasło;
2. Podczas komunikacji w ramach wideokonferencji należy uprzednio poinformować każdą osobę o:
 - 1) fakcie nagrywania rozmowy i możliwości niewyrażenia na to zgody poprzez zakończenie połączenia;
 - 2) treści obowiązku informacyjnego wynikającego z art. 13 RODO, która znajduje się pod adresem www.nasutowszkola.edupage.org którą można odczytać z pliku znajdującego się na stronie internetowej szkoły

cyt.:

Zgodnie z art. 13 Ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) informuję, iż:

- 1) administratorem Pani/Pana danych osobowych jest Dyrektor Szkoły Podstawowej im Kardynała Stefana Wyszyńskiego w Nasutowie, Nasutów 209A (poczta: Niemce), tel: (81) 756 64 75, mail: nasutowszkola@interia.pl;*
- 2) kontakt z Inspektorem Ochrony Danych ### iod@ecrklex.pl*
- 3) Pani/Pana dane osobowe przetwarzane będą w celu realizacji ustawowych zadań placówki oświatowej - na podstawie art. 6 ust. 1 lit. c ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. oraz na podstawie art. 9 ust.1 lit. g ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.;*
- 4) odbiorcami Pani/Pana danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa;*
- 5) Pani/Pana dane osobowe przechowywane będą w czasie określonym przepisami prawa, zgodnie z instrukcją kancelaryjną;*
- 6) posiada Pani/Pan prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania lub ograniczenia przetwarzania;*
- 7) ma Pani/Pan prawo wniesienia skargi do organu nadzorczego;*
- 8) podanie danych osobowych w zakresie wymaganym ustawodawstwem: Kodeks postępowania administracyjnego, ustawa ### Prawo oświatowe jest obligatoryjne.*

3. W przypadku jakichkolwiek pytań dotyczących ochrony danych osobowych, pojawiających się w trakcie wideokonferencji, na które pracownik nie może odpowiedzieć, należy daną osobę skierować do (IOD).
4. W przypadku braku zgody, o której mowa w ust. 2 pkt a, należy rozmowę zakończyć, a jej zapis trwale usunąć/przekazać do trwałego usunięcia Dyrektorowi DI.

§ 7. Postępowanie w przypadku naruszeń ochrony danych osobowych

1. Podczas pracy zdalnej należy mieć na uwadze fakt ewentualnego naruszenia ochrony danych osobowych.
2. Realizując obowiązek opisany w ust. 1, pracownik powinien zwrócić szczególną uwagę na:
 - 1) utratę dostępu do powierzonej infrastruktury, w której przetwarzane są dane osobowe;
 - 2) fakt zagubienia, kradzieży lub zniszczenia sprzętu i dokumentów, które zostały uprzednio powierzone pracownikowi;

- 3) wszelkie doniesienia medialne dotyczące zagrożenia danych osobowych przetwarzanych przez ADO;
3. W przypadku zaobserwowania naruszeń, o których mowa w ust. 1, należy niezwłocznie o tym fakcie powiadomić (*IOD oraz dodatkowo Dyrektora DI, w przypadku gdy naruszenie dotyczy infrastruktury informatycznej*).
4. W przypadku wystąpienia naruszenia, o którym mowa w ust. 1, należy współpracować z *IOD oraz Dyrektorem DI*, wykonując ich polecenia. W razie konfliktu w zakresie tych poleceń decydujące zdanie ma *IOD*.
5. Jeżeli pracownikowi, przed wystąpieniem naruszenia ochrony danych osobowych, zostały przekazane szczegółowe instrukcje dotyczące odzyskiwania lub usuwania danych osobowych, których naruszenie pracownik stwierdził, może on przystąpić do ich odzyskiwania lub zdalnego usuwania, jeżeli wykonanie tych czynności musi zostać podjęte niezwłocznie, a kontakt z IOD jest utrudniony.

§ 8. Postanowienia dodatkowe

1. Wszystkie dokumenty elektroniczne, na których pracownik wykonuje pracę zdalną, powinny zostać co najmniej raz na 3 dni przesłane do lokalizacji fim@nasutow.com znajdującej się na dysku Google G-Suite.
2. Pliki można przysyłać po uprzednim opatrzeniu ich hasłem, które należy następnie wysłać w osobnej wiadomości e-mail.

§ 9. Obowiązki regulaminu

1. Niniejszy regulamin wchodzi w życie z dniem odpisania
2. Regulamin może podlegać zmianom wynikającym z wdrożenia wytycznych, o których mowa w § 2 ust. 2, toteż każdy pracownik ma obowiązek regularnego zapoznawania się z jego aktualną treścią.
3. Za zamieszczanie oraz informowanie o aktualnej treści regulaminu odpowiedzialna jest administrator strony internetowej szkoły i dziennika elektronicznego LIBRUS – pani Aneta Kotowska i Elżbieta Fim