

INSTRUKCJA OCHRONY DANYCH OSOBOWYCH W SZKOLE PODSTAWOWEJ NR 50 WE WROCŁAWIU

Cel Instrukcji: wdrożenie w Szkole Podstawowej nr 50 we Wrocławiu najważniejszych reguł ochrony danych osobowych, zgodnie z Ogólnym Rozporządzeniem o Ochronie Danych (RODO).

Przedmiot Instrukcji: poinstruowanie pracowników Szkoła Podstawowa nr 50 we Wrocławiu w jaki sposób powinni działać, aby przestrzegać unijnych, krajowych i wewnętrznych regulacji w obszarze ochrony danych osobowych.

Adresaci Instrukcji: pracownicy Szkoły Podstawowej nr 50 we Wrocławiu (w tym nauczyciele i pracownicy administracyjni), którzy w ramach swoich obowiązków służbowych, przetwarzają dane osobowe – w tym uczniów, innych pracowników, wykonawców, dostawców lub innych osób (np. najemcy). Adresatami niniejszej Instrukcji są również członkowie Rady Rodziców, którzy w ramach swojej działalności mają dostęp do danych osobowych przetwarzanych przez Szkołę.

Zagadnienia poruszane w Instrukcji:

SPIS TREŚCI

A.	ZACHOWAJ BEZPIECZEŃSTWO DANYCH OSOBOWYCH	2
B.	ZAPEWNIJ DZIAŁANIE ZGODNE Z RODO	5
C.	WYDAWANIE I ODBIÓR SPRZĘTU SŁUŻBOWEGO	6
D.	JAK DZIAŁAĆ NA WYPADEK INCYDENTU BEZPIECZEŃSTWA.....	7
E.	WNIOSKI OSÓB UPRAWNIONYCH	8

A. ZACHOWAJ BEZPIECZEŃSTWO DANYCH OSOBOWYCH

Jednym z Twoich podstawowych obowiązków jest zapewnienie bezpieczeństwa danym osobowym, które znajdują się na nośnikach papierowych lub informatycznych. W obszarze bezpieczeństwa masz obowiązek stosować się do poniższych zasad:

1. Na koniec dnia uprzątnij biurko. Włóż wszystkie dokumenty nad którymi aktualnie pracujesz do szuflady biurka / do szafki i zamknij je na klucz. Pod Twoją nieobecność w pokoju mogą przebywać inne osoby (np. osoby sprzątające, pracownicy ochrony) i Twoim obowiązkiem służbowym jest zapewnić, aby osoby te nie miały dostępu do dokumentów zawierających dane osobowe.
2. Odchodząc od stanowiska pracy (nawet na chwilę) pamiętaj o wygaszeniu ekranu swojego monitora (jest to skrót klawiszowy  + L). Dzięki temu pod Twoją nieobecność żadna osoba nie podejrzy danych wyświetlonych na Twoim monitorze, ani nie będzie w stanie, korzystając z Twojego komputera, dokonać żadnych czynności w systemie, które byłyby przypisane Tobie.
3. Jeżeli zabierasz ze sobą do domu lub w podróż służbowe urządzenia i/lub dokumenty papierowe, miej je przy sobie do czasu umieszczenia w bezpiecznym i zamkniętym pomieszczeniu (np. mieszkanie, dom, pokój hotelowy). W szczególności nie zostawiaj niczego na noc w samochodzie. Nie zostawiaj niczego bez opieki w przedziale pociągu.
4. Ustalaj bezpieczne i niepowtarzalne hasła do komputera i systemów informatycznych. To takie hasła, które mają co najmniej 8 znaków, w tym cyfry lub znaki specjalne. Swoje hasło możesz zapisać w bezpiecznym miejscu (np. w telefonie zabezpieczonym PINem). Zabronione jest jednak zapisywanie hasła na kartce obok stanowiska pracy (np. przy monitorze, pod klawiaturą).
5. Nie oddawaj osobie, która nie ma upoważnienia do przetwarzania tych samych danych co Ty, kluczy do Twojego pokoju, do Twoich szafek i biurka, w których przechowujesz dokumenty.

6. Stosuj hasło lub PIN w swoim telefonie komórkowym lub innym urządzeniu przenośnym, jeżeli wykorzystujesz je w pracy do przetwarzania danych.
7. Nie podawaj nikomu swojego hasła do komputera lub do systemów bazodanowych, do telefonu lub do innego urządzenia przenośnego. Jeżeli z jakichkolwiek przyczyn jakakolwiek inna osoba uzyskała dostęp do Twojego hasła, po ustaniu tej przyczyny niezwłocznie zapewnij zmianę hasła. Jeżeli nie wiesz jako to zrobić, zwróć się o pomoc do informatyka zatrudnianego przez placówkę.
8. Jeżeli otrzymałeś/otrzymałaś urządzenie służbowe to nie loguj się do systemów Szkoły z komputera domowego, telefon prywatnego albo urządzenia innych osób. Takie urządzenia mogą zawierać szkodliwe oprogramowanie, które może narazić cały system na podatność na ryzyko w obszarze ochrony danych osobowych.
9. Jeżeli wysyłasz e-mailem dane osobowe na zewnątrz – na inny adres niż adres służbowy pracownika Naszej placówki - upewnij się, czy odbiorca stosuje protokół szyfrowania korespondencji e-mail. Jeżeli tego nie wiesz, konieczne umieść dane osobowe w pliku i zabezpiecz dostęp do pliku hasłem. Hasło do pliku prześlij do odbiorcy innym środkiem komunikacji niż e-mail (np. SMS, komunikator).
10. Nie otwieraj załączników przesłanych przez niezaufanego nadawcę, co do którego masz jakiegokolwiek wątpliwości (informacje z nieznanego źródła, albo z nieznanego adresu e-mail dot. wystawionych faktur, zaległych lub należnych płatności itp., zawierających załączniki z rozszerzeniem *.rar lub *.zip). Zweryfikuj dokładnie adres e-mail, z którego nadano korespondencję, spróbuj zorientować się czego może dotyczyć temat. Pamiętaj jednak, że do czasu upewnienia się, że korespondencja pochodzi od zaufanego nadawcy **zabronione jest otwieranie załącznika**. Jeżeli po dokonaniu podstawowej weryfikacji cały czas masz wątpliwości zadzwoń pod wskazany w stopce numer telefonu i dopytaj się czego dotyczy temat. Jeżeli wątpliwości nie da się rozstrzygnąć, nie otwieraj załącznika do wiadomości e-mail i pozostaw wiadomość bez odpowiedzi.
11. Pracując na urządzeniu służbowym nie korzystaj ze stron i serwisów internetowych obciążonych ryzykiem dla ochrony danych (portale z pirackim oprogramowaniem, pirackimi filmami, strony pornograficzne itp.).

12. Nie instaluj oprogramowania, ani aplikacji (w tym na swoim telefonie służbowym), które pochodzą z niezauważanych źródeł. Instalując samodzielnie jakiegokolwiek oprogramowanie/aplikację na urządzeniu służbowym zawsze korzystaj z zaufanego źródła, którym będzie strona internetowa wydawcy takiego programu/aplikacji albo zaufany dystrybutor (np. Sklep Play firmy Google).

B. ZAPEWNIJ DZIAŁANIE ZGODNE Z RODO

13. Jeżeli brałeś udział w rekrutacji pracownika i masz na swoim komputerze CV kandydatów, to pamiętaj, aby po zakończonej rekrutacji bezwzględnie usunąć te CV ze swojego dysku oraz ze swojej skrzynki e-mail. Po zakończonej rekrutacji można przetwarzać dalej CV tylko tych kandydatów, którzy wyrazili odrębną zgodę na przetwarzanie CV również po okresie rekrutacji.
14. Jeżeli jakaś osoba bezpośrednio na Twój adres e-mail prześle swoje CV – poza prowadzoną przez Szkołę rekrutacją – pamiętaj, aby potwierdzić takiej osobie otrzymanie jej wiadomości. Odpowiadając nawet krótkim „Dziękuję za aplikację” spełniasz obowiązek informacyjny wobec osoby zainteresowanej zatrudnieniem w Naszej Szkole, a to dzięki stosowanej przez Szkołę stopce informacyjnej obecnej w podpisie.
15. Przesyłając wiadomość e-mail do wielu adresatów nie będących pracownikami Szkoły (np. korespondencja zbiorcza do rodziców) zamieść ich adresy w ukrytej kopii. W ten sposób nie dojdzie do nieautoryzowanego ujawnienia adresów e-mail osobom nieuprawnionym.
16. Jeżeli jakiś zewnętrzny podmiot prosi Cię o podanie danych ucznia, rodziców, pracowników Szkoły – upewnij się, że na pewno możesz podać te dane. Sprawdź:
 - a. kto dokładnie prosi Cię o podanie danych – jaka organizacja, zweryfikuj adres e-mail
 - b. w jakim celu masz podać te dane – czy na pewno ten cel jest właściwy
 - c. jeżeli pytającym jest organ państwowy – zastanów się, czy ma podstawę prawną żądać takich informacji.

Jeżeli masz wątpliwości, czy na pewno możesz udostępnić określone dane osobowe skontaktuj się mailowo z Inspektorem Ochrony Danych pod adresem inspektor@coreconsulting.pl

C. WYDAWANIE I ODBIÓR SPRZĘTU SŁUŻBOWEGO

Przez sprzęt służbowy należy rozumieć wszelkie **nośniki danych**, czyli przykładowo (choć nie wyłącznie) **pendrive'y, zewnętrzne dyski, komputery stacjonarne, laptopy, tablety, telefony**, które zostały przygotowane przez Szkołę.

Wydawanie sprzętu służbowego pracownikowi

Przed wydaniem sprzętu służbowego przedstawiciel Szkoły odpowiedzialny za wydanie sprzętu powinien:

1. upewnić się, że pracownik, który otrzyma sprzęt nie będzie miał dostępu do jakichkolwiek danych po poprzednim pracowniku, który z niego korzystał, chyba że taki dostęp jest niezbędny do realizacji obowiązków służbowych tego pracownika;
2. zapewnić, aby na sprzęcie zostało ustanowione
 - a. hasło dostępu do odblokowania telefonu (z wyłączeniem odczytu linii papilarnych) – w przypadku telefonów komórkowych
 - b. hasło dostępu do konta na komputerze – w przypadku komputerów,
 - c. hasło dostępu do folderów lub plików – w przypadku nośników danych takich jak pendrive, zewnętrzny dysk, płyty CD.

Szkoła zobowiązana jest prowadzić rejestr określający – jaki komputer (o jakiej nazwie i numerze seryjnym) został wydany jakiemu pracownikowi, tak by móc przyporządkować wydawany sprzęt do konkretnej osoby.

Przyjmowanie sprzętu służbowego do utylizacji lub do odprzedaży

Jeżeli do informatyka lub innego pracownika administracji trafia jakikolwiek sprzęt służbowy w celu jego utylizacji lub odprzedaży (nawet temu samemu pracownikowi, który wcześniej z tego sprzętu korzystał), należy zapewnić trwałe i nieodwracalne usunięcia danych zawartych na tym urządzeniu, w tym kontakty, SMS-y, historię połączeń, pobrane pliki (w tym *cookies*), historię przeglądania, na dysku twardym lub karcie SD itp.

D. JAK DZIAŁAĆ NA WYPADEK INCYDENTU BEZPIECZEŃSTWA

Incydent – sytuacja lub zdarzenie, które wiąże się z co najmniej jednym z następujących skutków:

- a) bezpowrotna utrata danych osobowych (np. zniszczenie dysku, który nie ma kopii zapasowej)
- b) wyciek danych osobowych (uzyskanie dostępu do danych osobowych przez osobę nieuprawnioną)
- c) naruszenie integralności danych (doszło do nieautoryzowanych zmian w bazach danych, które np. skutkują brakiem możliwości stwierdzenia prawdziwości danych).

W przypadku podejrzenia wystąpienia incydentu przyjmuje się następujące reguły działania:

Krok 1 – pracownik, który stwierdzi ryzyko incydentu, niezwłocznie zabezpiecza dane przed dalszym wyciekiem/zniszczeniem przy jednoczesnym zachowaniu danych dot. **zdarzenia** (tj. należy zabezpieczyć dane przed dalszym dostępem osób nieuprawnionych, a jednocześnie należy zachować informacje o tym jakie dane wyciekły, w celu umożliwienia działania w kolejnych krokach; przykładowo w przypadku włamania na serwer Szkoły i wykradzenia danych, odłączamy serwer od Internetu ale nie kasujemy danych zawartych na serwerze – będą potrzebne do zidentyfikowania jaka była skala naruszenia i jakie dane zostały narażone)

Krok 2 – pracownik, który stwierdził ryzyko incydentu, po wykonaniu działań z kroku 1 niezwłocznie informuje przełożonego oraz inspektora ochrony danych osobowych (inspektor@coreconsulting.pl) o zdarzeniu.

Krok 3 – Inspektor Ochrony Danych we współpracy z Dyrekcją Szkoły oraz osobą odpowiedzialną za systemy IT (o ile incydent wiąże się z obszarem IT) dokonują wtórnej weryfikacji bezpieczeństwa danych osobowych.

Krok 4 – w przypadku incydentu większej wagi zostaje powołana wewnętrzna Komisja w celu zbadania okoliczności sprawy i określenie jej przebiegu, przyczyn naruszenia, potencjalnych konsekwencji naruszenia.

Krok 5 – następuje podjęcie decyzji o konieczności zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych oraz osób, których dane dotyczą o wystąpieniu naruszenia.

***Krok 6** – w razie konieczności Inspektor Ochrony Danych Osobowych zawiadamia Prezesa Urzędu Ochrony Danych Osobowych o incydencie (jeżeli są spełnione warunki z art. 33 RODO; wzór zgłoszenia stanowi **Załącznik nr 1** do Instrukcji).

Krok 7 – opracowanie pełnego Raportu ze zdarzenia; wyciągnięcie określonych wniosków w zakresie koniecznych zmian proceduralnych, zabezpieczeń fizycznych lub technicznych; konsekwencji personalnych (jeżeli dotyczy); wpisanie incydentu do rejestru naruszeń

UWAGA: zawiadomienie Prezesa Urzędu Ochrony Danych Osobowych o naruszeniach, które wiążą się z ryzykiem naruszenia praw lub wolności osób, których dane dotyczą powinno być dokonane niezwłocznie, nie później jednak niż w terminie **72 godzin** po stwierdzeniu naruszenia. Nie są to „godziny robocze”, więc działania w tym obszarze powinny być podejmowane bez zbędnej zwłoki.

E. WNIOSKI OSÓB UPRAWNIONYCH

1. Jeżeli wpłynie do Ciebie wniosek o:

- a. udostępnienie danych osobowych, lub
- b. sprostowanie danych, lub
- c. przeniesienie danych, lub
- d. ograniczenie przetwarzania danych, lub
- e. sprzeciw wobec przetwarzania danych osobowych, lub
- f. wniosek dot. prawa do bycia zapomnianym,

wniosek taki w wersji elektronicznej prześlij **niezwłocznie** bezpośrednio do Inspektora Ochrony Danych (inspektor@coreconsulting.pl).

2. Inspektor zobowiązany jest zweryfikować, czy nie ma wątpliwości co do tożsamości osoby składającej wniosek (tj. czy dane podane we wniosku zgadzają się z danymi posiadanymi przez placówkę w swojej dokumentacji lub w systemach):

- a. jeżeli wniosek wpłynie mailem – IODO weryfikuje wspólnie z przedstawicielami placówki, czy dla maila, z którego wysłany jest wniosek przypisana jest osoba fizyczna z tymi samymi danymi, które są ujęte w treści wniosku;
- b. jeżeli wniosek wpłynął pisemnie – złożony osobiście /przesyłką poleconą / kurierem – IODO odpowiada na wniosek na adres e-mail przypisany w dokumentacji lub w systemach informatycznych do danej osoby, a jeżeli takiego adresu e-mail Szkoła nie posiada, wówczas IODO odpowiada na adres korespondencyjny tej osoby zgodnie z informacjami w dokumentacji lub w systemach placówki;
- c. w przypadku wniosku złożonego telefonicznie – IODO weryfikuje, czy numer z którego dzwoniła osoba, jest numerem, który Szkoła ma już przypisany wcześniej do danej osoby.

Jeżeli IODO ma jakiegokolwiek wątpliwości, co do tożsamości wnioskodawcy zapewnia potwierdzenie treści wniosku z wnioskodawcą innym kanałem komunikacji.

3. Inspektor we współpracy z pracownikami Szkoły zapewnia wypełnienie formularza udostępnienia danych, który stanowi **Załącznik nr 2** do niniejszej Instrukcji.
4. Inspektor lub na jego polecenie pracownik Szkoły, który przyjął wniosek, zobowiązany jest przesłać do osoby fizycznej zgłaszającej wniosek dokument odpowiedzi.