# REGULAMIN PRZETWARZANIA DANYCH OSOBOWYCH W SZKOLE PODSTAWOWEJ W ZAMIENIU

Załącznik nr 1
do Zarządzenia Nr 11
z dnia 01.09.2021r.

**Wstęp.**

Szczegółowe procedury i instrukcje dotyczące zasad przetwarzania danych osobowych zawarte są w Polityce Bezpieczeństwa Informacji i Instrukcji Zarządzania Systemem Informatycznym, które zostały wdrożone w Szkle Podstawowej w Zamieniu. Niniejszy regulamin stanowi kompensację zasad ochrony danych osobowych obowiązujący pracowników upoważnionych przez Administratora do przetwarzania danych osobowych.

**Dopuszczenie do przetwarzania danych osobowych.**

1. Przed rozpoczęciem przetwarzania danych osobowych każdy pracownik obowiązany jest zapoznać się z zasadami przetwarzania i ochrony danych osobowych zawartymi w niniejszym Regulaminie. Zapoznanie to zostaje potwierdzone podpisem.
2. Przetwarzanie danych osobowych, których Administratorem jest Szkoła Podstawowa w Zamieniu jest możliwe dopiero po uzyskaniu upoważnienia wydanego przez Administratora.
3. Zabronione jest przetwarzanie danych osobowych w zakresie i czasie wykraczającym poza upoważnienie.

**zmiana sposobu przetwarzania danych osobowych**

1. Zmiana sposobu lub podjęcie nowej czynności przetwarzania danych wymaga wcześniejszego powiadomienia Inspektora Ochrony Danych. Informacja powinna zawierać:
   a) Jakich danych będzie dotyczyć zmiana;
   b) Czynności jakie będą wykonywane na danych osobowych;
   c) Rodzaj zabezpieczeń danych osobowych;
   d) Data zmiany;
   e) Wyszczególnienie osób mających mieć dostęp do danych.
2. Inspektor Ochrony Danych, ocenia proponowane zmiany pod względem legalności i ryzyka naruszenia praw i wolności osób, których dane dotyczą, a także dokonuje aktualizacji w prowadzonej dokumentacji przetwarzania.

**Bezpieczeństwo danych osobowych przetwarzanych w systemach papierowych.**

1. W miejscu przetwarzania danych osobowych, utrwalonych w formie papierowej, osoby upoważnione zobowiązane są do niepozostawiania materiałów zawierających dane osobowe w miejscach umożliwiających fizyczny dostęp do nich osobom nieuprawnionym. Po zakończeniu pracy oraz w przypadku opuszczenia stanowiska pracy, jeżeli dostęp do niego mają osoby nieposiadające upoważnienia do przetwarzania danych w zbiorze, w którym dane są przetwarzane, materiały zawierające dane osobowe winny być przechowywane w szafach zamykanych na klucz lub w pomieszczeniach do tego przystosowanych przez pracodawcę. Niedopuszczalne jest pozostawianie materiałów zawierających dane osobowe na biurku, regale, w niezamkniętej szafie.
2. Osoba upoważniona ma obowiązek dołożenia najwyższej staranności, by inne osoby nie miały wglądu do dokumentów zawierających dane osobowe lub informacje chronione znajdujących się na biurku lub w innych miejscach dostępnych dla osób trzecich.
3. Kopiowanie danych osobowych może odbywać się wyłącznie przez osobę w ramach posiadanego przez nią upoważnienia do przetwarzania danych osobowych, w związku z realizacją czynności służbowych. Kopie danych osobowych oraz błędnie wytworzone dokumenty, podlegają zniszczeniu niezwłocznie po realizacji celu, dla którego zostały wykonane.
4. Dokonywanie wydruków, skanowanie lub kopiowanie materiałów zawierających dane osobowe odbywa się wyłącznie w obecności pracownika przy urządzeniu. Niedozwolone jest pozostawianie urządzenia w trakcie drukowania/skanowania/kopiowania bez nadzoru, jeżeli materiały znajdujące się w urządzeniu zawierają dane osobowe.
5. Ochronie podlega każdy nośnik danych osobowych, niezależnie od tego, czy jest to oryginał lub kopia dokumentu, notatka lub zapiski wykonane odręcznie lub wydrukowane z postaci elektronicznej.
6. Każdy dokument papierowy zawierający dane osobowe sporządzony jako dokument roboczy należy najpóźniej na koniec dnia pracy zniszczyć lub zamknąć w miejscu uniemożliwiającym dostęp osób nieuprawnionych.
7. Wynoszenie dokumentów poza wyznaczoną strefę jest dozwolone tylko w szczególnych wypadkach i wymaga ich zabezpieczenia przed nieuprawnionym dostępem.
8. Pracownicy zobowiązani są do stosowania „polityki czystego biurka”, która polega na tym, że na biurku znajdują się jedynie dokumenty, nad którymi pracownik aktualnie pracuje, oraz nie pozostawiania żadnych dokumentów niezabezpieczonych na noc na biurku.
9. Pracownicy obowiązani są do zabezpieczenia dokumentów przed ich zagubieniem, utratą i kradzieżą, przypadkowym ujawnieniem osobom nieupoważnionym.
10. Dokumenty zawierające dane osobowe lub inne informacje podlegające ochronie należy niszczyć w niszczarkach. Dokumenty, zakwalifikowane do zniszczenia, niszczymy od razu. Zadrukowanych w ten sposób kart nie używamy ponownie np. na brudnopisy.

11. Pracownicy zobowiązani są do przestrzegania maksymalnych okresów przetwarzania danych osobowych. Zabronione jest przetwarzanie dokumentów po osiągnięciu celu, dla którego zostały zebrane.
12. Po zrealizowaniu celu na jaki dane zostały zebrane, odpowiedzialny za zbiór pracownik dokonuje jego zniszczenia, co zostaje potwierdzone protokołem.

**Zasady postępowania w przypadku udzielania informacji telefonicznie.**

1. Każdy pracownik odpowiadający na pytania telefonicznie powinien dochować szczególną ostrożność aby nie udzielić informacji osobie nieupoważnionej.
2. Przed udzieleniem informacji, należy sprawdzić tożsamość osoby dzwoniącej.
3. W razie wątpliwości lub niemożności ustalenia tożsamości, należy poprosić o przesłanie zapytania w formie papierowej.
4. W przypadku trudnych sytuacji lub wątpliwości należy poprosić o pomoc przełożonego.

**Zabezpieczenia pomieszczeń i stref przetwarzania danych osobowych**

1. W pomieszczeniach, w których przetwarzane są dane osobowe, przebywać mogą wyłącznie osoby upoważnione do przetwarzania danych osobowych. Klienci i inne osoby postronne mogą przebywać w strefie przetwarzania danych osobowych tylko w obecności pracownika.
2. Zabronione jest pozostawianie pomieszczeń, w których odbywa się przetwarzanie danych osobowych niezamkniętych, lub w których przebywają osoby postronne przez pracownika nawet na chwilę.
3. Każdy pracownik przed opuszczeniem pomieszczenia, w którym przetwarzane lub przechowywane są dane osobowe zobowiązany jest do zamknięcia go na klucz.
4. Każdy pracownik przed opuszczeniem pomieszczenia, w którym przetwarzane lub przechowywane są dane osobowe zobowiązany jest do zamknięcia okien.
5. Wszystkie pomieszczenia w których są przetwarzane dane osobowe na noc zamykane są na klucz. Ostatnia osoba wychodząca z budynku sprawdza czy pokoje i okna zostały zamknięte i zamyka budynek na klucz.

**Zasady używania sprzętu IT**

1. Za sprzęt IT uznawane są w szczególności: komputery, drukarki, tablety, serwery, routery, nośniki pamięci, dyski zewnętrzne.
2. Osoby upoważnione przetwarzając dane osobowe obowiązane są używać tylko i wyłącznie sprzętu przekazanego przez Administratora.
3. Pracownik obowiązany jest chronić sprzęt IT zgodnie z jego przeznaczeniem i zabezpieczać przed kradzieżą i uszkodzeniem.

4. Zniszczenie, kradzież lub utratę sprzętu pracownik obowiązany jest natychmiast zgłosić przełożonemu.
5. Zabronione jest używanie urządzeń oraz oprogramowania niezatwierdzonych przez Administratora Systemów Informatycznych.
6. Nośniki pamięci mogą być wynoszone tylko za zezwoleniem przełożonego.
7. Nośniki pamięci zawierające dane osobowe mogą być wynoszone poza strefę przetwarzania danych osobowych po wcześniejszym ich zaszyfrowaniu.
8. W przypadku uszkodzenia lub zużycia nośnika pamięci lub sprzętu komputerowego pracownik przekazuje go do Administratora Systemów Informatycznych w celu bezpiecznego zniszczenia go.
9. Zapisywanie danych osobowych na elektronicznych mobilnych nośnikach danych, np. pendrive, dysk zewnętrzny jest możliwe wyłącznie po spełnieniu następujących warunków:
    a) dane osobowe mogą być zapisywane na mobilnym nośniku danych wyłącznie na krótkotrwały czas;
    b) nośnik musi pozostawać do wyłącznej dyspozycji pracownika i być wykorzystywany wyłącznie do celów służbowych;
    c) nośniki wykorzystywane do zapisywania na nich danych osobowych muszą być zabezpieczone kryptograficznie lub pliki zawierające dane osobowe muszą być zabezpieczone hasłem;
    d) po zaprzestaniu korzystania z nośnika, na którym były lub są zapisane dane osobowe, nośnik ten musi zostać zniszczony fizycznie lub poddany działaniu profesjonalnego narzędzia do trwałego usuwania danych w sposób uniemożliwiający ich odtworzenie lub odzyskanie w całości lub w części;

**Zasady korzystania z oprogramowania**

1. Pracownicy zobowiązani są do korzystania wyłącznie z oprogramowania zainstalowanego przez Administratora Systemów Informatycznych.
2. Zabroniona jest zmiana konfiguracji systemów ustawionych przez Administratora Systemów Informatycznych.
3. Oprogramowanie typu MS Office służy jedynie do edycji tekstu i przygotowania dokumentu do wydruku. Pliki zawierające dane osobowe zapisane w tym oprogramowaniu powinny być niezwłocznie usuwane lub zanonimizowane (tj. pozbawione danych osobowych) zaraz po wydrukowaniu.
4. Pracownicy obowiązani są do regularnego skanowania urządzeń programem antywirusowym.
5. Zabronione jest wyłączanie ochrony antywirusowej.
6. W przypadku stwierdzenia zainfekowania sprzętu, należy niezwłocznie powiadomić Administratora Systemów Informatycznych.

**Zasady korzystania z dziennika elektronicznego**

1. Z dziennika elektronicznego mogą korzystać wyłącznie osoby, którym został przydzielony dostęp przez Administratora.
2. Zabronione jest umożliwianie dostępu do dziennika elektronicznego osobom nieposiadającym uprawnień.
3. Zabronione jest umożliwianie dostępu do komputera innym osobom po zalogowaniu się do dziennika elektronicznego z użyciem własnych danych uwierzytelniających: loginu oraz hasła.
4. Zabronione jest udostępnianie własnego hasła do dziennika elektronicznego innym osobom.
5. Logowanie oraz przetwarzanie danych w dzienniku elektronicznym ma odbywać się z zachowaniem poufności danych uwierzytelniających (login oraz hasło dostępu do systemu należy wpisywać w sposób uniemożliwiający przypadkowy dostęp osób nieupoważnionych).
6. Zabronione jest zapisywanie danych osobowych z dziennika elektronicznego na jakichkolwiek nośnikach danych.

**Zasady korzystania z poczty elektronicznej.**

1. Pracownicy mogą korzystać ze służbowej poczty elektronicznej tylko w celach związanych z wykonywaniem obowiązków służbowych.
2. Wysyłając wiadomości do wielu odbiorców użytkownik ma obowiązek korzystać z opcji UDW.
3. Przesyłanie plików stanowiących tajemnicę pracodawcy lub zawierających dane osobowe może tylko po wcześniejszym ich zaszyfrowaniu ewentualnie zabezpieczeniu hasłem. Hasło do pliku powinno być podane odbiorcy inną drogą np. telefoniczną.
4. Zakazuje się uczestnictwa w tzw. „łańcuszkach szczęścia”.
5. Użytkownicy nie powinni otwierać przesyłek od nieznanych sobie osób, których tytuł nie sugeruje związku z wypełnianymi przez nich obowiązkami służbowymi.
6. Użytkownicy nie powinni uruchamiać wykonywalnych załączników dołączonych do wiadomości przesyłanych pocztą elektroniczną.
7. Użytkownicy nie mają prawa korzystać z Systemu Poczty Elektronicznej w celu przeglądania lub rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
8. Zabronione jest używanie prywatnych skrzynek mailowych w celach służbowych.
9. Komunikacja mailowa z rodzicami powinna odbywać się za pośrednictwem systemu informatycznego wyznaczonego do tego celu przez Administratora -Vulcan.
10. Zabronione jest przekierowywanie poczty elektronicznej z domeny UNIQA przez inne serwery poczty elektronicznej, w szczególności przez darmowe konta poczty elektronicznej ogólnodostępne dla osób fizycznych nieprowadzących działalności gospodarczej.

11. Zabronione jest kopiowanie dokumentów i informacji zawierających dane osobowe przesyłanych pocztą elektroniczną na dysk twardy komputera, serwer lub inne nośniki danych niebędące własnością

**Stosowanie haseł.**

1. Pracownicy logując się do systemów przetwarzających dane osobowe obowiązani są stosować hasła o budowie: minimum 8 znaków (duże i małe litery cyfry lub znaki specjalne).
2. Hasłami nie mogą być powszechnie używane słowa, w szczególności imiona, daty, nr rejestracyjne, nr telefonów.
3. Pracownicy zobowiązani są do niezapisywania i nieujawniania haseł nawet po utracie ich ważności.

**Procedura rozpoczęcia i zakończenia pracy.**

1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe poprzez wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieuprawnione.
2. Użytkownik jest zobowiązany do powiadomienia Administratora Systemów Informatycznych o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
3. Użytkownik zobowiązany jest do używania wygaszaczy ekranu, których odblokowanie wymaga podania hasła.
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. uczniom, innym pracownikom) wgląd do dokumentów, nad którymi pracuje na biurku lub danych wyświetlanych na monitorach komputerowych.
5. Po zakończeniu pracy, pracownik zobowiązany jest:
   a) wylogować się z systemu informatycznego.
   b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, oraz kopie zapasowe, na których znajdują się dane osobowe.

**zasady przetwarzania danych osobowych poza strefą przetwarzania**

1. Na pracę z wykorzystaniem danych osobowych poza strefą przetwarzania musi wyrazić zgodę przełożony.
2. Dyski pamięci komputerów jak i przenośne nośniki pamięci typu pendrive, płyty CD, karty pamięci itp. przed wyniesieniem ze strefy przetwarzania powinny być zaszyfrowane.
3. Pracownik zobowiązany jest zabezpieczyć odpowiednio dane osobowe przed wglądem i podejrzeniem ich przez osoby nieupoważnione. Szczególną ostrożność należy wykazać korzystając z przenośnych komputerów w miejscach publicznych. Ustawienie ekranu komputera powinno uniemożliwiać podejrzenie jego zawartości przez osoby postronne a także przez kamery monitoringu.

4. Zabronione jest przesyłanie danych, korzystanie ze służbowej poczty elektronicznej lub służbowych systemów zawierających dane osobowe z wykorzystaniem publicznych sieci WiFi.
5. Pracownik powinien odpowiednio zabezpieczyć dane przed kradzieżą i zgubieniem. Zabronione jest pozostawianie komputerów, nośników pamięci i dokumentacji papierowej bez nadzoru.

**Postępowanie w przypadku stwierdzenia naruszenia danych osobowych.**

1. Za naruszenie ochrony danych osobowych uważa się w szczególności:
   a) Nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują.
   b) Naruszenie lub próby naruszenia integralności danych rozumiane, jako wszelkie modyfikacje, zniszczenie lub próby ich dokonania przez osoby nieuprawnione lub uprawnione działające w złej wierze lub jako błąd w działaniu osoby uprawnionej (np. zmianę zawartości danych, utratę całości lub części danych)
   c) Naruszenie lub próby naruszenia integralności systemu.
   d) Zmianę lub utratę danych zapisanych na kopiach zapasowych.
   e) Naruszenie lub próby naruszenia poufności danych lub ich części.
   f) Nieuprawniony dostęp (np. sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu).
   g) Udostępnienie osobom nieuprawnionych danych osobowych lub ich części.
   h) Zniszczenie, uszkodzenie lub wszelki próby ingerencji nieuprawnionej w system informatyczny zmierzający do zakłócenia jego działania bądź pozyskania w sposób niedozwolony danych.
   i) Inny stan pomieszczeń niż pozostawiony przez użytkownika po zakończeniu pracy.
   j) Dostęp pracownika do danych wykraczających poza wydane przez Administratora Danych Osobowych upoważnienie.
2. Każdy pracownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować natychmiast bezpośredniego przełożonego, który informuje Inspektora Ochrony Danych, a niedopełnienie tego obowiązku może powodować odpowiedzialność dyscyplinarną, cywilną lub możliwość zastosowania kar umownych;
3. Po wpłynięciu informacji o naruszeniu od pracownika Inspektor Ochrony Danych przeprowadza postępowanie wyjaśniające mające na celu ustalenie wszystkich okoliczności zdarzenia, zakresu i skali naruszenia i przedstawia ustalenia Administratorowi.
4. Każdy z pracowników ma obowiązek udzielić wyczerpujących wyjaśnień o okolicznościach naruszenia na polecenie Inspektora Ochrony Danych, w formie jaką Inspektor Ochrony Danych uzna z stosowną.
5. Analizę ryzyka naruszenia praw i wolności osoby lub osób, których dane naruszono Inspektor Ochrony Danych przedstawia Administratorowi.

6. Jeśli istnieje ryzyko naruszenia praw i wolności osób których dane naruszono w ciągu 72 godz. od wykrycia zdarzenia Administrator powiadamia organ nadzorczy.
7. Jeśli istnieje wysokie ryzyko naruszenia praw i wolności osób których dane naruszono, Administrator informuje również osoby, których dane naruszono.
8. Każde naruszenie wpisywane jest do rejestru naruszeń.

**Zachowanie tajemnicy danych osobowych.**

1. Każdy pracownik zobowiązany jest do nieujawniania danych osobowych o jakich dowiedział się w związku z wykonywaniem obowiązków służbowych.
2. Zabrania się ujawniania sposobów zabezpieczenia danych osobowych stosowanych przez Szkołę Podstawową w Zamieniu.
3. Zabrania się ujawniania danych osobowym osobom nieupoważnionym.
4. Zobowiązanie do zachowania w tajemnicy istnieje również po ustaniu zatrudnienia w Szkole Podstawowej w Zamieniu.

**Prawa osób, których dane dotyczą**

1. Osoby, których dane przetwarzane są przez Szkołę Podstawową w Zamieniu mają prawo do:
   a. Żądanie prawa dostępu do danych
   b. Żądanie sprostowania lub usunięcia danych
   c. Żądanie prawa do ograniczenia przetwarzania danych
   d. Żądanie przeniesienia danych
   e. Wniesienie sprzeciwu do przetwarzania danych osobowych lub cofnięcie zgody na przetwarzanie danych osobowych,
2. Po wpłynięciu żądania w formie pisemnej lub elektronicznej wyszczególnionego w pkt. 1, pracownik ma obowiązek potwierdzić przyjęcie takiego żądania zgodnie z instrukcją kancelaryjną.
3. W przypadku żądania wyrażonego telefonicznie, pracownik sporządza notatkę służbową wskazując dokładnie którego z praw wyszczególnionych w pkt. 1 domaga się osoba, oraz ustala tożsamość tej osoby i sposób kontaktu
4. Po przyjęciu żądania pracownik przekazuje je niezwłocznie do Inspektora Ochrony Danych.
5. Inspektor Ochrony Danych ustala, czy żądanie jest zasadne i identyfikuje osobę, której dane dotyczą.
6. Pracownicy mają obowiązek współpracować z Inspektorem Ochrony Danych w kwestii spełnienia żądania osoby wyszczególnionego w pkt. 1
7. Osobą uprawnioną do odpowiadania na żądania wyszczególnione w pkt. 1 jest Inspektor Ochrony Danych.

**Odpowiedzialność.**

1. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą, jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
2. W przypadku wystąpienia strat materialnych, spowodowanych nieprzestrzeganiem zasad niniejszego Regulaminu, postanowień umów powierzenia danych, Administrator może domagać się od osoby dokonującej naruszenia, pokrycia tych strat zgodnie z wskazaniami Kodeksu Cywilnego i Kodeksu Pracy.
3. Kara dyscyplinarna lub umowna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 10 maja 2018 roku o ochronie danych osobowych oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez Administratora Danych o zrekompensowanie poniesionych strat.
4. Regulamin wchodzi w życie z dniem podpisania.