Regulamin przetwarzania danych osobowych

W ZESPOLE SZKOLNO-PRZEDSZKOLNYM W ZAKRZOWIE

wersja 1 - ważna od 01.03.2022r.

Spis treści

PREAMBUŁA

I. Zasada generalna przetwarzania danych osobowych

1. Pracownik lub inna osoba pełniąca funkcje lub wykonująca pracę w jednostce oświatowej, jest zobowiązana/-y do zachowania w poufności informacji:
    - uzyskanych w związku z pełnioną funkcją lub wykonywaną pracą,
    - dotyczących danych dzieci, ich rodziców, pracowników jednostki oraz osób z nią współpracujących,
    - w szczególności dot. ich zdrowia, potrzeb rozwojowych i edukacyjnych, możliwości psychofizycznych, pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub światopoglądowych, seksualności, orientacji seksualnej.

POJĘCIA I ZASADY OGÓLNE

II. Podstawowe pojęcia

1. **Administrator Danych Osobowych (Administrator)** – Jednostka w imieniu której działa Dyrektor ustalający cele i sposoby przetwarzania danych osobowych w Jednostce.
2. **Administrator Systemu Informatycznego (ASI)** – należy przez to rozumieć wyznaczoną przez Administratora osobę realizującą zadania związane z utrzymaniem systemu teleinformatycznego, a w szczególności odpowiedzialną za utrzymywanie zabezpieczeń w tym systemie. W razie braku wyznaczenia ASI - jego zadania realizuje Administrator.
3. **Dane osobowe** – oznaczają informacje o zidentyfikowanej lub możliwej do identyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania **osoba fizyczna** to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
4. Jednostka – Zespół Szkolno-Przedszkolny w Zakrzowie
5. **Naruszenie ochrony danych osobowych** - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
6. **Przetwarzanie danych osobowych** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

III. Zakres podmiotowy (kogo obowiązuje Regulamin)

1. Regulamin obowiązuje:
    - **wszystkich pracowników** Jednostki niezależnie od formy umowy wiążącej ich z pracodawcą,

- **podmioty przetwarzające dane osobowe** na podstawie zawartych umów między Administratorem, a podmiotem przetwarzającym,
- **użytkowników systemów informatycznych** z dostępem do danych osobowych upoważnionych przez Administratora na piśmie,
- inne osoby, których Administrator upoważnił.

2. Każda z osób wymienionych w pkt. 1 jest zobowiązana do zapoznania się z niniejszym dokumentem i bezwzględnego przestrzegania zawartych w nim zasad.

IV. Obowiązki osoby przetwarzającej dane

Osoba przetwarzająca dane (w tym w pierwszej kolejności pracownik):

a) **powinna być świadoma**, że ma ochraniać powierzone jej w procesie pracy dane osobowe i przetwarzać je zgodnie z przepisami prawa i wewnętrznymi dokumentami;
b) **ma znać przepisy ochrony danych osobowych**, swoje obowiązki i **nie usprawiedliwia** jej brak ich znajomości w każdym momencie pracy na stanowisku, a szczególności podczas audytów, kontroli i wystąpienia incydentów bezpieczeństwa;
c) ma stały **dostęp** do wewnętrznych dokumentów w zakresie ochrony danych osobowych; w każdym momencie może zapoznać się z tymi przepisami zwracając się do Administratora;
d) ma **obowiązek** poddawania się szkoleniom z zakresu ochrony danych osobowych w terminach i zasadach określonych przez Administratora;
e) ma obowiązek **przestrzegania** procedur ochrony danych osobowych zawartych w niniejszym Regulaminie.

V. Legalność przetwarzania (upoważnienia, przekazywanie, zbieranie danych)

1. Pracownik może przetwarzać dane osobowe wyłącznie na podstawie **imiennego upoważnienia** do przetwarzania danych osobowych wydawanego przez Administratora lub jeśli jest przedsiębiorcą, to na podstawie zawartej umowy powierzenia przetwarzania danych osobowych.
2. W ww. upoważnieniu / umowie powierzenia wskazane jest jakie dane osobowe, w jakim zakresie i w jakim czasie można przetwarzać.
3. Jeśli pracownik przetwarza dane bez upoważnienia, umowy powierzenia lub w zakresie innym niż wskazany w upoważnieniu/umowie powierzenia to **narusza postanowienia polityki bezpieczeństwa i przepisy RODO**.
4. Jeśli w swoich zadaniach na stanowisku pracy pracownik ma przetwarzać dane określone w innym zakresie niż wskazanym w upoważnieniu / umowie powierzenia to musi bezzwłocznie **przed przystąpieniem** do wykonywania tych zadań zwrócić się do Administratora o poszerzenie zakresu upoważnienia / umowy powierzenia.
5. Dane osobowe, które pracownik przetwarza może przekazać innej osobie jeśli ma pewność, że:
   - osoba, której przekazuje dane jest osobą, której dane dotyczą (lub jest rodzicem / opiekunem dziecka) i ma do nich prawo, a pracownik/-ca jest **upoważniony/-a przez Administratora** do ich przekazywania; lub
   - osoba, której przekazuje dane ma upoważnienie Administratora do przetwarzania tych danych osobowych; lub

- osoba, której przekazuje dane reprezentuje przedsiębiorcę, który podpisał z Administratorem umowę powierzenia danych osobowych.

6. Pracownik może przekazywać dane osobowe innemu Administratorowi tylko będąc upoważnionym przez własnego Administratora do takich czynności i tylko w odpowiedzi na pisemny wniosek **zawierający podstawę prawną** legalności udostępnienia (należy sprawdzić tę podstawę prawną i udostępnić można tylko dane w zakresie opisanym w tej podstawie).
7. Zbierając dane osobowe należy pamiętać, aby zrealizować obowiązek informacyjny względem osoby, której dane dotyczą. O przygotowanie klauzuli informacyjnej należy zwrócić się do Administratora.
8. Zbieramy tylko dane niezbędne do realizacji zadań określonych przez prawo i w sposób zatwierdzony przez Administratora

VI. Nadrzędne zasady przetwarzania danych osobowych

Niezależnie od wykonywanych czynności przetwarzania danych pracownika obowiązuje:

1. **Zasada czystego biurka** – polega na **nie pozostawianiu** na biurku lub innych dostępnych miejscach w pomieszczeniu (w tym na drukarkach) danych osobowych na dowolnych nośnikach podczas nieobecności pracownika w pomieszczeniu, zwłaszcza poza godzinami pracy oraz podczas czasowego opuszczenia pomieszczenia. Z kolei podczas obecności na stanowisku polega ona na prowadzeniu procesu pracy związanego z przetwarzaniem danych osobowych w sposób uniemożliwiający wgląd w te dane przez osoby nieupoważnione.
2. **Zasada czystego ekranu** – polega na blokowaniu ekranu komputera, laptopa, tabletu, smartfona itp. po każdorazowym zaprzestaniu pracy na urządzeniu (w systemie operacyjnym Windows: klawisze WIN+L lub Ctrl+Alt+Delete i wybranie opcji „Zablokuj ten komputer").
3. **Zasada odwróconego ekranu** – polega na odwracaniu ekranu komputera, laptopa, telefonu, smartfona itp. chroniąc dane osobowe przed wglądem osób nieupoważnionych (stosuje się opcję wygaszacza ekranu – 10 min.).
4. **Zasada zamkniętej szafy** – polega na przechowywaniu dokumentów papierowych z danymi osobowymi, a także nośników z danymi osobowymi (przenośne pamięci, dyski, USB, kopie zapasowe, itp.) w szafach zamykanych na klucz oraz zabezpieczeniu tego klucza przed osobami nieupoważnionymi. Zasadę tę stosuje się niezależnie od formy zabezpieczenia pomieszczenia, w którym szafa się znajduje. Wprowadzenie wyjątku od tej zasady może być zastosowane tylko za zgodą Administratora, po zastosowaniu innych adekwatnych zabezpieczeń.

VII. Procedura przetwarzania danych podstawowych współpracowników

1. Pracownik powinien z rozwagą i ostrożnością przetwarzać dane osobowe zaliczane do danych podstawowych (imię i nazwisko pracownika jednostki, stanowisko służbowe).
2. Spisy pracowników oraz telefonów służbowych należy przechowywać w szufladach lub miejscach o ograniczonym dostępie dla osób trzecich.

SZCZEGÓŁOWE ZASADY PRZETWARZANIA DANYCH DLA WSZYSTKICH CZYNNOŚCI

VIII. Zasady udostępniania danych osobowych przez telefon

1. Co do zasady Administrator nie zezwala na przekazywanie danych osobowych drogą telefoniczną, poprzez SMS i MMS.
2. Wyjątkiem od tej zasady jest przekazanie informacji, których przekazanie:
   - leży w interesie osoby, której dane dotyczą (np. informacja dla dzwoniącego rodzica, do którego szpitala zostało zabrane jego dziecko po wypadku),
   - gdy podanie danych leży w interesie publicznym.
3. W przypadku opisanym w pkt. 2 należy mieć jednak pewność, że dane przekazywane są właściwej osobie. Dlatego w takich przypadkach należy poprosić rozmówcę o podanie dodatkowej/-ych informacji, która/-e pozwoli/-ą nam go zidentyfikować (na przykład pytamy o dane dziecka, które posiadamy by je potwierdzić, w co było ubrane). Próba identyfikacji nie może wpłynąć negatywnie na żywotny interes osoby, której dane dotyczą, a także na interes publiczny.
4. W powyżej opisany sposób nie należy udzielać informacji o osobach instytucjom, które zawsze powinny występować w tej sprawie w formie pisemnej.
5. Nie należy udzielać informacji instytucjom finansowym, w celu potwierdzenia wystawienia wcześniejszych zaświadczeń o zarobkach.
6. Nie należy udzielać informacji w sprawach pracowniczych krewnym, powinowatym lub współmałżonkowi, chyba że posiadamy w aktach osobowych nie budzące wątpliwości oświadczenie o zgodzie na takie udzielanie informacji.
7. Należy stosować ogólne przepisy prawa w tym zakresie.

IX. Zasady tworzenia i wykorzystywania haseł

Należy pamiętać o prawidłowości posługiwania się hasłami do aplikacji/systemów.

1. Hasło powinno składać się co najmniej z 8 znaków, zawierać małe i wielkie litery, cyfry i znak specjalny.
2. Hasło nie może być identyczne z imieniem, nazwiskiem, loginem lub identyfikatorem,
3. Należy je zmieniać się nie rzadziej niż co 30 dni, lub rzadziej, ale pod warunkiem mocniejszego hasła (tj. zawierającego co najmniej 12 znaków).
4. Hasło zmienia się przy pierwszym logowaniu.
5. Nie wolno go udostępniać innym osobom.
6. Należy niezwłocznie zgłosić jego utratę.
7. Należy utrzymać go w tajemnicy i nie zapisywać (nawet nieaktualnych wersji).
8. Nie wolno zapamiętywać go w przeglądarkach.
9. Należy zawsze zmieniać w przypadku podejrzenia ujawnienia.
10. W razie konieczności należy dostosować jego długość itp. do większych wymagań.

X. Zasady korzystania z Internetu służbowego,

1. Internet służbowy należy używać tylko w celach wykonywania swoich obowiązków.
2. Nie wolno ściągać nieznanych plików z niepewnego źródła.
3. Nie wolno instalować nielegalnych programów.
4. Pliki z nieznanych źródeł można ściągać po konsultacji z Administratorem/ASI.

5. Pracownik ponosi odpowiedzialność za straty w infrastrukturze IT spowodowanej ściąganiem nieznanych plików.
6. Nie wolno wchodzić na strony hackerskie, przestępcze, pornograficzne, gdyż może to grozić infekcją systemu szkodliwym oprogramowaniem.
7. Obowiązuje zakaz zapamiętywania haseł w przeglądarkach.
8. W przypadku korzystania z połączenia szyfrowanego należy zwracać uwagę na ikonę kłódki. Należy kliknąć w tę ikonę i sprawdzić, czy właściciel certyfikatu jest wiarygodny.
9. Należy zachować ostrożność w przypadku podejrzanego żądania logowania, podania PIN, logów lub haseł.

XI. Polityka korzystania z służbowej poczty e-mail

1. Pocztę e-mail można wykorzystywać tylko w celach służbowych.
2. Należy wykorzystywać mechanizmy kryptograficzne (hasło do pliku, podpis elektroniczny) w przypadku przesyłania danych osobowych poza jednostkę.
3. Hasło do pliku należy przesyłać innym kanałem komunikacji, obowiązuje w tym zakresie powyższa polityka haseł.
4. Należy sprawdzać dwukrotnie poprawność adresu e-mail, poprosić adresata o potwierdzenie otrzymania wiadomości.
5. Nie wolno otwierać załączonych plików bez weryfikacji nadawcy. Nie wolno wchodzić w hiperlinki w wiadomościach bez weryfikacji nadawcy.
6. Przy wysyłce maili do wielu adresatów należy korzystać z opcji: „Ukryte do wiadomości – UDW”.
7. Należy okresowo kasować stare wiadomości.
8. Nie wolno wysyłać poczty służbowej na prywatne e-maile.
9. Nie wolno korzystać z „łańcuszków szczęścia”, nie wolno dokonywać prywatnych zakupów z użyciem poczty służbowej.
10. Nie wolno wysyłać żadnych danych osobowych bez upoważniania Administratora.

XII. Polityka korzystania z systemu informatycznego

Zasady ogólne:

1. Przed rozpoczęciem pracy należy sprawdzić, czy stanowisko nie było wykorzystane przez nieuprawnioną osobę.
2. Należy Informować Administratora/ASI o problemach z logowaniem do systemu.
3. Należy stosować zasadę „czystego biurka” i „czystego ekranu”.
4. Kończąc pracę należy zapisać dane i wyłączyć aplikacje.
5. Kończąc pracę należy wylogować się z systemu, a następnie odłączyć urządzenie od zasilania.
6. Zawsze należy sprawdzić, czy w drukarce nie pozostały wydruki.
7. Nośniki danych należy zamykać w szafkach zamykanych na klucz.
8. Po skończonej pracy należy zabezpieczyć stanowisko pracy, sprzęt i nośniki z danymi osobowymi.
9. Należy tak ustawić ekran komputera, aby chronić dane osobowe przed wglądem osób nieupoważnionych (należy zastosować opcję wygaszacza ekranu – 10 min.).

10. Należy sprawdzać system na obecność wirusów przy użyciu licencjonowanego programu antywirusowego.
11. Nie wolno dokonywać samodzielnych napraw systemu informatycznego. Usterki należy zgłaszać Administratorowi/ASI.

Zasady szczegółowe:

1. **Rozpoczęcie pracy w systemie** odbywa się poprzez:
   a. przygotowanie stanowiska pracy,
   b. włączenie stacji roboczej,
   c. wprowadzenie swojego identyfikatora i hasła.
2. Przed rozpoczęciem pracy na danym stanowisku komputerowym użytkownik zobowiązany jest do jego zweryfikowania w celu sprawdzenia, czy nie zostało ono naruszone lub wykorzystane przez osobę nie będącą jego użytkownikiem. W przypadku pojawienia się trudności w autoryzacji (logowaniu), pomimo prawidłowo podanej nazwy użytkownika i hasła, użytkownik zobowiązany jest skontaktować się z ASI. Jeżeli proces autoryzacji przebiegł prawidłowo, użytkownik może przystąpić do pracy.
3. **Zawieszenie pracy w systemie** - w przypadku konieczności czasowego opuszczenia stanowiska pracy użytkownik jest zobowiązany zastosować zasady czystego biurka oraz czystego ekranu, blokując komputer poprzez wciśnięcie kombinacji klawiszy WIN+L lub Ctrl + Alt + Delete i wybranie opcji „Zablokuj ten komputer".
4. **Kończąc pracę**, użytkownik zobowiązany jest do:
   a. zapisania danych w aplikacji i zamknięcia aplikacji,
   b. wylogowania się z systemu i poczekania na jego wyłączenie, a następnie odłączenie urządzenia od zasilania,
   c. sprawdzenia czy w drukarce nie pozostały wydruki,
   d. umieszczenia w zamykanych na klucz szafach informatycznych nośników danych oraz dokumentów zawierających dane osobowe,
   e. zamknięcia okien, wyłączenia wszystkich urządzeń elektrycznych (w tym również komputerowych), zgaszenia światła w pomieszczeniach oraz zamknięcia drzwi opuszczanego pomieszczenia,
   f. Upewnienia się, czy po zakończeniu pracy nie pozostawił na jednostce ogólnej niezabezpieczonych danych osobowych (niezamknięta poczta elektroniczna, zapisane kopie danych, niewykasowane pliki z folderu „pobrane"),
   g. Szyfrowania pliki pozostawianych na stacjach ogólnodostępnych.
5. **Dostęp do Systemu (konto użytkownika)** lub stacji roboczych **ogólnodostępnych** jednostki może być wykorzystywane przez użytkownika wyłącznie do zadań związanych z pełnionym stanowiskiem lub realizacją umów. W szczególności nie może być ono wykorzystywane do rozpowszechniania treści i obrazów wulgarnych, obrażających osoby trzecie, naruszających czyjekolwiek dobra osobiste lub niezgodnych z prawem.
6. **Zabrania się użytkownikom** pracującym na zasobach informatycznych jednostki:
   a. udostępniania stacji roboczej osobom niezarejestrowanym w systemie, a jeśli nie ma systemu rejestracji - osobie nieupoważnionej,
   b. udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z ASI,
   c. instalowania samodzielnie, bez zgody ASI oprogramowania systemowego i aplikacji (programów),
   d. uruchamiania aplikacji (programów), które mogą zakłócić i destabilizować pracę Systemu, bądź naruszyć bezpieczeństwo danych w nim przetwarzanych,

e. pobierać z sieci, kopiować, przechowywać lub rozprowadzać oprogramowania, dane multimedialne (filmy, muzyka) oraz inne pliki, których używanie może powodować naruszenie praw do własności intelektualnej,
f. udostępniania osobom trzecim informacji na temat struktury Systemu, również po ustaniu okresu zatrudnienia lub po odebraniu dostępu do Systemu,
g. używania zasobów informatycznych do celów prywatnych, co w szczególności oznacza, że wszelkie dane przetwarzane na sprzęcie informatycznym jednostki nie oznaczone jako własność osób trzecich, są własnością jednostki – w tym także korespondencja elektroniczna.

7. Należy chronić **sprzęt komputerowy** przed kradzieżą, zniszczeniem lub niewłaściwym użytkowaniem oraz zagrożeniami ze strony otoczenia (kurz, promieniowanie słoneczne, ogień, woda itp.). Sprzęt komputerowy będący własnością jednostki nie może być wynoszony z siedziby jednostki, a w przypadku sprzętu stacjonarnego, przenoszony w inne miejsce jednostki bez wcześniejszej zgody ASI.
8. Utrata lub kradzież powierzonego Pracownikowi sprzętu powinna być niezwłocznie zgłaszana do Administratora.
9. Zabrania się używania jakichkolwiek prywatnych nośników danych (magnetycznych, optycznych oraz pamięci przenośnych) na stanowiskach komputerowych (w tym komputerach przenośnych) będących własnością jednostki bez zgody ASI.
10. Wszelkie osoby korzystające z Systemu są zobowiązane do przestrzegania prawa, zasad współżycia społecznego oraz zasad etyki. Zabrania się podejmowania działań, które naruszałyby dobra osobiste innych osób lub narażały te osoby na straty moralne lub materialne.
11. W przypadku udostępnienia przez Administratora komputera ogólnodostępnego **(bez konieczności logowania się na konto indywidualne użytkownika)** użytkownik:
    a. Upewnia się, czy Administrator zezwolił na danej stacjonarnej lub przenośnej jednostce przetwarzać dane osobowe,
    b. Upewnia się, czy po zakończeniu pracy nie pozostawił na jednostce niezabezpieczonych danych osobowych (niezamknięta poczta elektroniczna, zapisane kopie danych, niewykasowane pliki z folderu „pobrane”,
    c. Jeśli Administrator zezwolił, aby na ww. stacji roboczej możliwe był, czasowe przechowywanie plików z danymi osobowymi muszą być one umieszczone w folderach identyfikujących właściciela i bezwzględnie zaszyfrowane. Należy upewnić się jaka jest częstotliwość czyszczenia dysków wskazanych jednostek.

XIII. Zasady przetwarzania danych na sprzęcie służbowym poza jednostką

1. Przetwarzanie na służbowych przenośnych stacjach roboczych (w tym na telefonach) poza obszarem przetwarzania należy ograniczać do niezbędnego minimum.
2. Należy zapewnić mechanizmy szyfrowania danych w przypadku wskazanego przetwarzania.
3. Przed rozpoczęciem wskazanego przetwarzania należy zwrócić się do Administratora/ASI o zapewnienie zabezpieczenia kryptograficznego, ochrony antywirusowej.
4. W telefonach służbowych należy stosować PIN (przynajmniej czteroznakowy).
5. Nie wolno pozostawiać urządzenia bez blokady ekranu.
6. Należy zapewnić odpowiedni transport urządzenia uniemożliwiający kradzież oraz wgląd przez osoby nieupoważnione (praca w pociągu, autobusie, korytarzu itp.).

7. Należy ograniczać wykorzystywanie urządzeń do celów prywatnych i do podłączania prywatnych urządzeń bez pozwolenia Administratora/ASI.
8. Należy zabezpieczyć urządzenie przed negatywnymi warunkami otoczenia (słońce, wilgoć itp.).
9. Nie wolno udostępniać stacji osobom nieupoważnionym.
10. Należy niezwłocznie zgłaszać Administratorowi utratę urządzenia.

XIV. Zasady korzystania z przenośnych nośników informatycznych

1. Zakres danych zbieranych przez użytkownika może wynikać wyłącznie z zakresu realizowanych zadań.
2. **Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach danych oraz ich przesyłania pocztą elektroniczną bez uprzedniego zaszyfrowania.**
3. Na nośnikach, o których mowa w pkt. 2, dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych niezbędnych do realizacji bieżących danych.
4. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na wyznaczonym w tym celu stanowisku komputerowym oraz do oznakowania tego nośnika.
5. Nośniki magnetyczne raz użyte do przetwarzania danych osobowych nie mogą być wykorzystywane do innych celów mimo usunięcia danych.
6. Nośniki magnetyczne z zaszyfrowanymi jednostkowymi danymi osobowymi są na czas ich użyteczności przechowywane w zamkniętych na klucz szafach, a po wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki te są niszczone.
7. Korzystanie z przenośnych pamięci jest dozwolone w celu wykonania kopii zapasowej oraz udostepnienia danych na podstawie przepisów prawa lub umowy.
8. Należy chronić pamięć przed uszkodzeniem, zniszczeniem i kradzieżą.
9. Należy szyfrować dane na przenośnych pamięciach.
10. Nie wolno udostępniać danych osobom nieupoważnionym.
11. Należy niezwłocznie usuwać dane jeśli stają się nieużyteczne ze względu na cel przetwarzania.
12. Nie wolno pozostawiać przenośnych pamięci bez nadzoru w jednostce i poza nią.
13. Należy zapewnić kopię zapasową danych przetwarzanych na przenośnej pamięci, po ocenie zasadności jej wykonania, zwłaszcza jeśli utrata danych byłaby powodem naruszenia zasady dostępności (brak zapisu danych na trwałym nośniku),
14. Przenośne pamięci należy udostępnić w celach kontrolnych na każde polecenie Administratora, ASI i IOD, nawet jeśli dotyczy to nośnika prywatnego dopuszczonego do użytkowania przez Administratora,
15. Należy zwrócić sprzęt służbowy po zakończeniu pracy u Administratora.

XV. Polityka ochrony papierowej wersji dokumentacji jednostki

1. Wersja papierowa dokumentacji Jednostki (w szczególności dzienniki lekcyjne, arkusze ocen, opinie z poradni psychologiczno-pedagogicznej, klasówki, sprawdziany, listy uczniów tworzone doraźnie, dane o stanie zdrowia itp.) powinna być przechowywana w specjalnie do tego wyznaczonym miejscu – szafie zamykanej na klucz.

2. Pokój nauczycielski jest miejscem szczególnie chronionym, nie może w nim przebywać osoba postronna bez nadzoru przynajmniej jednej osoby posiadającej upoważnienie do przetwarzania danych osobowych.
3. Przenoszenie papierowej wersji dokumentacji jednostki zawierającej dane osobowe (w szczególności dzienników lekcyjnych) przez uczniów, bądź inne osoby, które nie są upoważnione do przetwarzania danych osobowych jest bezwzględnie zakazane. Obowiązkiem pracownika jest osobiste pobranie i odłożenie dokumentacji jednostki na wyznaczone miejsce. Dopuszczalne jest przekazanie dokumentacji przez inną osobę, o ile posiada ona upoważnienie do przetwarzania danych osobowych obejmujące zakres danych przetwarzanych w tej dokumentacji.
4. Wynoszenie dokumentów poza jednostkę jest co do zasady zakazane. Rodzaj dokumentacji papierowej, która może być wynoszona poza teren jednostki: listy uczniów (bez danych wrażliwych), sprawdziany, kartkówki (bez imion i nazwisk uczniów). Natomiast wynoszenie zeszytów uczniów poza jednostkę w szczególnych wypadkach dozwolone jest za zgodą Administratora.
5. Wynoszenie dokumentów zawierających dane osobowe pracowników (pobieranie akt pracowniczych bądź kopii dokumentów z sekretariatu) jest zakazane. Wyjątek od tej zasady może potwierdzić jednorazowo lub okresowo Administrator.
6. Dyrektor określa zasady poprawy sprawdzianów i prac domowych poza jednostką: sprawdziany i kartkówki mogą być sprawdzane poza jednostką, jeżeli są zakodowane (nie zawierają imienia i nazwiska ucznia).
7. Dokumentacja jednostki prowadzona jest na podstawie przepisów prawa (dzienniki, arkusze itp.).

XVI. Zasady korzystania z danych papierowych

1. Wszelkie pliki tworzone w edytorach tekstu, arkuszach kalkulacyjnych znajdujące się na nie zabezpieczonych urządzeniach (np. niezahasłowanych telefonach), albo urządzeniach prywatnych pracowników powinny być zabezpieczone hasłem i szyfrowane. Dotyczy to również przesyłaniu ww. plików przy użyciu e-maila.
2. Należy chronić wydruki przed dostępem osób nieupoważnionych (pozostawianie na drukarkach, przy ksero, korytarzach).
3. Nie wolno powtórnie wykorzystywać kartek z danymi osobowymi jednostronnie zadrukowanych.
4. Należy stosować zasadę „czystego biurka”.
5. Nie wolno wyrzucać niezniszczonych dokumentów na śmietnik lub pozostawiać niezabezpieczonymi na zewnątrz.
6. Dokumenty należy niszczyć w niszczarkach, lub korzystać z usług firm niszczących dokumenty.
7. Należy stosować zasady bezpiecznego wydruku zakładające, że:
   - niedozwolone jest drukowanie dokumentów zawierających dane osobowe na drukarce znajdującej się w miejscu ogólnodostępnym, chyba że użytkownik bezpośrednio obserwuje proces wydruku,
   - zabronione jest, aby osoba nieupoważniona do rodzaju przetwarzanych na tych dokumentach danych, odbierała gotowe wydruki z drukarki,
   - użytkownik ma obowiązek niezwłocznie po wykorzystaniu zniszczyć za pomocą niszczarki zbędne wydruki zawierające dane osobowe.

XVII. Zasady niszczenia nośników z danymi osobowymi

Zasady ogólne:

1. Trwałe niszczenie danych osobowych następuje wyłącznie na wniosek Administratora i w zgodzie z odrębnymi przepisami (w tym prawa archiwalnego).
2. Sposób zniszczenia danych osobowych musi być odpowiednio dobrany do rodzaju nośnika danych oraz ich kategorii.
3. Trwałe niszczenie głównych (podstawowych) zbiorów danych osobowych, a także ich kopii zapasowych powinno odbywać się komisyjnie, przy czym w komisji musi znajdować się Administrator (lub jego przedstawiciel).
4. Trwałe zniszczenie danych osobowych musi zostać potwierdzone spisaniem protokołu.
5. Za niezwłoczne usunięcie danych osobowych z nośników danych, które służyły do przeniesienia (przekazania) danych odpowiada ich użytkownik.
6. Za usunięcie zdjęć (filmów) z aparatów fotograficznych (kamer) nie nadających się do dalszego wykorzystania lub po upływie możliwości ich przetwarzania odpowiada użytkownik sprzętu. Podobne zasady obowiązują wobec zapisanych plików z wizerunkiem na innych nośnikach.
7. Każdy pracownika zna zasady archiwizowania dokumentów w jednostce, a Administrator zapewnia by zasady te były dostępne dla każdego pracownika.

Zasady usuwania danych w zależności od rodzaju nośnika:

1. Dokumentacja tradycyjna (wydruki, notatki, dokumenty itd.) – przy użyciu niszczarki.
2. Nośniki optyczne (płyty CD/DVD) – za pomocą niszczarek.
3. Nośniki elektroniczne (pendrive/karty pamięci/dyski twarde SSD) – korzystając z jednej z dwóch metod:
   - niszczenie programowe – polegające na wielokrotnym nadpisywaniu danych na nośniku, które uniemożliwiają odczytanie danych,
   - niszczenie sprzętowe – polegające na trwałym zniszczeniu nośnika za pomocą odpowiednich urządzeń.
4. Nośniki magnetyczne (dyskietki/dyski twarde HDD) – korzystając z jednej z trzech metod:
   - niszczenie programowe – polegające na wielokrotnym nadpisywaniu danych na nośniku, które uniemożliwiają odczytanie danych,
   - niszczenie sprzętowe – polegające na trwałym zniszczeniu nośnika za pomocą odpowiednich urządzeń,
   - demagnetyzacji nośników.
5. Zabrania się dokonywania samodzielnego niszczenia dokumentów i nośników w poza jednostką zwłaszcza w kotłowniach, ogniskach itp. Wszelkie dane osobowe przetwarzane poza jednostką należy zwrócić do jednostki, która nadzoruje ich zniszczenie.
6. Niszczenie poza jednostką może być wykonane tylko przez uprawnione podmioty, z którym administrator podpisał umowę powierzenia przetwarzania informacji.

XVIII. Zasady postępowania w przypadku naruszenia lub podejrzenia naruszenia ochrony

1. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych lub samego podejrzenia takiej sytuacji należy niezwłocznie powiadomić o tym fakcie Administratora (dotyczy danych osobowych gromadzonych w systemach informatycznych lub w formie tradycyjnej).
2. Należy zgłaszać wszelkie przypadki:

- usiłowania logowania się do systemu (sieci) przez osobę nieuprawnioną,
- usuwania, dodawania lub modyfikowania bez wiedzy i zgody użytkownika jego dokumentów,
- przebywania osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych i bez zgody administratora danych,
- pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe,
- udostępniania osobom nieuprawnionym stacji roboczej (w tym przenośnej), służącej do przetwarzania danych osobowych,
- niezabezpieczenia hasłem dostępu do urządzenia służącego do przetwarzania danych osobowych,
- przechowywania nośników informacji oraz wydruków z danymi osobowymi, nieprzeznaczonymi do udostępniania, w warunkach umożliwiających do nich dostęp osobom nieuprawnionym,
- zagubienia lub kradzieży nośnika danych osobowych, lub urządzenia na którym zapisane są dane osobowe,
- zagubienia lub kradzieży kart mikroprocesorowych,
- inne przypadki, które według oceny pracownika mogą stanowić incydent bezpieczeństwa.

3. Do czasu przybycia Administratora zgłaszający (zarówno w przypadku naruszenia, jak i w przypadku podejrzenia naruszenia ochrony danych osobowych):
   - powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności mogących spowodować zatarcie lub naruszenie śladów bądź innych dowodów,
   - zabezpiecza elementy systemu informatycznego lub dokumentacji, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym,
   - podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
4. Po przybyciu Administratora dokonuje on oceny sytuacji, a pracownik wraca na miejsce pracy dopiero po otrzymaniu od niego pozwolenia.
5. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej dyscypliny pracy, Administrator podejmuje stosowne działania wobec osób, które dopuściły się tego uchybienia.
6. Zgłoszenia należy dokonać niezwłocznie, gdyż Administrator w ciągu 72 godz. musi podjąć decyzję, czy zdarzenie należy zgłosić do organu nadzorczego i dokonać takiego zgłoszenia.

XIX. Kopie zapasowe

1. Kopie zapasowe tworzy się są na zewnętrznych dyskach, płytach CD lub pamięciach przenośnych z następującą częstotliwością: co najmniej jeden raz na miesiąc. Kopie roczne przechowywane są przez 5 lat.
2. Administrator przegląda okresowo kopie awaryjne i ocenia ich przydatność do odtworzenia zasobów systemu w przypadku jego awarii.
3. Stwierdzenie utraty przez kopie awaryjne waloru przydatności do celu, o którym mowa w ust. 1 upoważnia Administrator (ASI) do ich zniszczenia.

4. Niszczenie kopii zawierających dane, jak również wszelkich innych nośników zawierających zapis cyfrowy dokonuje się w sposób uniemożliwiający ich odzyskanie.
5. Kopie zapasowe przechowywane są w pomieszczeniach innych aniżeli pomieszczenia przeznaczone do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu. Kopie zapasowe przechowane są w zamykanych na klucz szafach w wyznaczonym obszarze przetwarzania. W miarę możliwości organizacyjnych kopie zapasowe przechowywane są w innym budynku.

XX. Zasady konserwacji sprzętu

1. Sprzęt służący do przetwarzania informacji należy konserwować zgodnie z zaleceniami dostawcy (w zakresie częstotliwości i zakresu).
2. Konserwacja zewnętrzna sprzętu obejmuje utrzymanie urządzeń w należytej czystości poprzez wykonywanie takich czynności jak: czyszczenie elementów zewnętrznych (klawiatur, myszy, monitorów itp.).
3. Naprawianie i konserwowanie wewnętrzne sprzętu należy zlecać do realizacji autoryzowanemu personelowi.
4. Na czas czynności konserwacyjnych przez personel zewnętrzny należy usunąć informacje z przekazanych urządzeń lub nadać tym osobom odpowiednie uprawnienia. Po czynnościach konserwacyjnych należy zweryfikować urządzenia czy sprzęt nie został zmanipulowany i nie realizuje szkodliwych funkcji.

XXI. Szyfrowanie plików Word/Excel (na przykładzie MS Office 2013)

1. Z górnego paska narzędzi wybieramy „Plik” (lewy górny róg).
2. Po otwarciu paska bocznego (Informacje) wybieramy „Chroń dokument”.
3. Po rozwinięciu menu wybieramy „Szyfruj przy użyciu hasła”.
4. Wprowadzamy dwa razy hasło.
5. Po zapisaniu pliku będzie się on otwierał wyłącznie po podaniu hasła.
6. Aby usunąć hasło należy wykonać czynności od 1-4, tylko zamiast nowego hasła należy pozostawić puste miejsce (nic nie wpisując). Po zapisaniu plik działa bez hasła.
7. W innych wersjach programu Office procedura może się nieznacznie różnić.

XXII. Szyfrowanie plików przy wykorzystaniu programu 7-Zip

1. Aby korzystać z możliwości szyfrowania przy wykorzystaniu 7-Zip należy zainstalować go na komputerze, pobierając z bezpiecznej strony internetowej.
2. Klikamy prawy przycisk myszy na pliku lub folderze.
3. Wybieramy 7-ZIP, a z rozwiniętego menu „Dodaj do archiwum”.
4. W otwartym oknie, w sekcji „szyfrowanie” należy wpisać hasło.
5. Zatwierdzamy.

XXIII. Zalecane praktyki w związku z realizacją zadań nauczania zdalnego i pracy zdalnej

1. Wyłącznie Administrator wyznacza zakres danych, które mogą być przetwarzane poza jednostką.

2. Wyłącznie Administrator wyznacza programy, aplikacje, sposoby komunikacji i komunikatory niezbędne do realizacji zadań.
3. Wyłącznie Administrator wyznacza rodzaje zasobów prywatnych, które mogą być wykorzystywane do przetwarzania danych jednostki w związku z realizacją pracy zdalnej i zdalnego nauczania.
4. Praktyki wskazane w przypadku przetwarzania danych na sprzęcie prywatnym:
   - Na bieżąco należy aktualizować systemy operacyjne.
   - Systematycznie należy aktualizować programy antywirusowe, antymalware i antyspyware.
   - Regularnie należy skanować stacje robocze programami antywirusowymi, antymalware i antyspyware.
   - Należy pobierać oprogramowanie wyłącznie ze stron producentów.
   - Nie należy otwierać załączników z nieznanych źródeł dostarczanych poprzez korespondencję elektroniczną.
   - Nie należy zapamiętywać haseł w aplikacjach web-owych.
   - Nie należy zapisywać haseł na kartkach.
   - Nie można używać tych samych haseł w różnych systemach informatycznych.
   - Należy zabezpieczać serwery plików czy inne zasoby sieciowe.
   - Należy zabezpieczać sieci bezprzewodowe – Access Point.
   - Należy dostosować złożoność haseł odpowiednio do zagrożeń.
   - Należy unikać wchodzenia na nieznane czy przypadkowe strony internetowe.
   - Nie należy logować się do systemów informatycznych w przypadkowych miejscach z niezaufanych urządzeń lub publicznych niezabezpieczonych sieci Wi-Fi.
   - Należy wykonywać regularne kopie zapasowe.
   - Należy korzystać ze sprawdzonego oprogramowania do szyfrowania e-maili lub nośników danych.
   - Należy szyfrować dane przesyłane pocztą elektroniczną.
   - Należy szyfrować dyski twarde w komputerach przenośnych.
   - Przy pracy zdalnej powinno korzystać się z szyfrowanego połączenia VPN.
   - Odchodząc od komputera należy blokować stację komputerową.
   - Nie należy umieszczać w komputerze przypadkowo znalezionych nośników USB. Może znajdować się na nich złośliwe oprogramowanie.

Źródło: https://www.uodo.gov.pl/pl/138/1473:

XXIV. Wideokonferencja

1. Przed rozpoczęciem wideokonferencji należy:
   - zapoznać się z programem i polityką prywatności narzędzia,
   - sprawdzić, czy obraz i dźwięk będą nagrywane,
   - sprawdzić, czy istnieje możliwość uczestnictwa z wyłączonym obrazem,
   - sprawdzić do jakich celów będą wykorzystane przetwarzane dane osobowe,
   - sprawdzić, o jakie uprawnienia ze strony programu będę poproszony (kontakty, lokalizacja itp.),
   - upewnić się, czy do mojego ekranu, pulpitu, zasobów nie mają dostępu osoby postronne,

- sprawdzić, czy aplikacja zapewnia niezbędne środki bezpieczeństwa, takimi jak szyfrowanie,
- należy korzystać z aplikacji webowych, a nie desktopowych,
- należy zabezpieczyć Wi-Fi silnym hasłem,
- należy zamknąć wszystkie okna, tak by inni nie mieli do nich dostępu,
- należy korzystać z kodów/PINów przy włączaniu się do telekonferencji,
- należy przeskanować program do telekonferencji systemem antywirusowym lub antymalware-owym.

2. W trakcie wideokonferencji należy:
   - ograniczyć podawanie danych osobowych (np. w miarę możliwości używać służbowego e-mail),
   - używać odrębnego hasła niż w innych usługach,
   - nie udostępniać linków do wideokonferencji w mediach społecznościowych,
   - włączyć, jeśli to możliwe, domyślną ochronę hasłem spotkania on-line,
   - zarządzać opcjami udostępniania ekranu,
   - korzystać w celu odbycia rozmów służbowych z VPN,
   - nie udostępniać dokumentów służbowych przy pomocy czatów,
   - jeśli jest taka możliwość wykorzystywać opcję zamazywania tła,
   - korzystać z opcji „poczekalnia" w celu kontroli osób dopuszczonych do spotkania,
   - podczas logowania należy mieć wyłączoną kamerę i mikrofon (włączamy jak będzie to potrzebne).
3. Po zakończeniu wideokonferencji należy:
   - wyłączyć mikrofon i kamerę,
   - wyłączyć aplikację,
   - upewnić się, czy aplikacja nie działa w tle.

XXV. Privacy by design

1. Każdy pracownik przestrzega i uwzględnia zasadę *privacy by design*.
2. Zasada *privacy by design* oznacza, że organizując nowe przedsięwzięcie (konkurs, zawody, wystawę) należy zorganizować je z uwzględnieniem bezpieczeństwa przetwarzania danych osobowych.
3. Obowiązek zaplanowania przedsięwzięcia leży na każdym pracowniku jeśli to on jest liderem projektu.
4. Do planowania wykorzystujemy formularz nr 4.
5. Formularz nr 4 musi być zatwierdzony przez Administratora.

ZASADY PRZETWARZANIA DANYCH W JEDNOSTCE OŚWIATOWEJ

XXVI. Rekrutacja do jednostki

1. Zasady rekrutacji do jednostki określają przepisy prawa i winny być przetwarzane w tym zakresie tylko dane osobowe wskazane w przepisach prawa i na zasadach tam wskazanych.
2. Zbieranie danych wykraczający poza ramy prawne wymaga konsultacji z IOD.
3. Za organizację procesu rekrutacji w zgodzie z RODO odpowiada Administrator, w tym celu wypełnia w każdym roku zał. nr 1.
4. W razie powołanie Komisji Rekrutacyjnej Administrator przekazuje zał. nr 1 Komisji Rekrutacyjnej. Przewodniczący planuje prace Komisji z uwzględnieniem zasad RODO przy wykorzystaniu załącznika nr 2, który zatwierdza Administrator.

XXVII. Organizacja pomocy psychologiczno – pedagogicznej

1. Zasady organizacji ppp określają przepisy prawa.
2. Podstawą przetwarzania danych osobowych w ramach ppp jest realizacja zadań w interesie publicznym. Nie może być nią zgoda.
3. Wszelkie zgody zbierane w ramach ppp nie są zgodami w rozumieniu RODO, ale zgodami formalnymi wynikającymi z prawa oświatowego (np. na objęcie dziecka ppp).
4. Należy zorganizować obieg dokumentów ppp, w tym zaplanować sposób przetwarzania danych poza jednostką (załącznik 3).
5. Nauczyciele zobowiązani są do respektowania zasad ustalonego obiegu dokumentów ppp (informacja w załączniku 5).

XXVIII. Zasady przetwarzania danych w dzienniku elektronicznym (jeśli dotyczy)

1. Wszystkie czynności w dzienniku elektronicznym winny być, co do zasady wykonywanie w jednostce.
2. Dyrektor jednostki może zezwolić na realizowanie pewnych czynności poza jednostką, przy zachowaniu zasad bezpiecznego użytkowania systemu dziennika elektronicznego (zasada czystego biurka, czystego ekranu, wylogowywanie z systemu po zakończeniu pracy) oraz bezpiecznych zasad pracy zdalnej.
3. Wykaz czynności dozwolonych w dzienniku elektronicznym poza jednostką wskazany jest w załączniku nr 5.

XXIX. Świadectwa szkolne

1. Świadectwa szkolne są dokumentami publicznymi zgodnie z ustawą z dnia 22 listopada 2018 r. o dokumentach publicznych.
2. Co do zasady nie można przetwarzać ich poza jednostką.
3. Zasady przechowywania ww. dokumentów (blankietów i dokumentów) określa art. 43 i 44 ww. ustawy.
4. Należy zapoznać się z wytycznym Administratora dotyczącymi przetwarzania dokumentów publicznych.

XXX. Nowe przedsięwzięcia związane z przetwarzaniem danych

1. Każda nowa czynność przetwarzania, nowy sposób realizowania już trwającej czynności przetwarzania, nowe specyficzne przedsięwzięcie w ramach czynności wymaga:
   - określenia podstaw prawnych przetwarzania,
   - określenia sposobów realizacji przedsięwzięcia (organizacja),
   - określenia zabezpieczeń,
   - wskazania ryzyk.
2. Każdy pracownik odpowiedzialny za projekt wypełnia załącznik nr 4 i przedstawia go do zatwierdzenia Administratorowi, który korzysta przy tym z doradztwa IOD-a.
3. Przykład nowych czynności przetwarzania: pojawiający się obowiązek przetwarzania danych w związku z pandemią, nowy projekt UE w jednostce itp.
4. Przykład zmiany sposobu przetwarzania danych: przejście z nauczania stacjonarnego na zdalne, wdrożenie dziennika elektronicznego, zmiana narzędzia do nauki zdalnej.
5. Przykład nowego przedsięwzięcia w ramach czynności: nowa wystawa, zawody, konkurs, wycieczka którego organizatorem jest jednostka (zwłaszcza te o zasięgu wychodzącym poza przetwarzanie danych dzieci/uczniów własnej Jednostki).
6. W sprawy wskazane w pkt. 3-5 obowiązkowo włączany jest IOD przynajmniej poprzez przesłanie do wglądu wypełnionego załącznika nr 4.

XXXI. Zasady korzystania z wizerunku w jednostce oświatowej (promocja)

Ponieważ wizerunek dziecka, rodzica, pracownika i każdej innej osoby może być przetwarzany tylko za jego zgodą należy pamiętać, że:

1. Do utrwalania wizerunku należy używać przede wszystkim sprzętu należącego do jednostki (aparat, kamera, zdjęcie w telefonie).
2. Aparaty fotograficzne, kamery należy zabezpieczać hasłem (o ile jest to możliwe) i przechowywać w zamkniętych szafach.
3. Zdjęcia wykonane telefonem powinny być niezwłocznie przegrane na nośnik elektroniczny jednostki i wykasowane z telefonu.
4. Utrwalanie wizerunku sprzętem prywatnym jest dozwolone za zgodą Administratora i pliki z jego utrwalenia powinny być niezwłocznie przegrane na nośnik jednostki i wykasowane ze sprzętu prywatnego.
5. Wizerunek utrwalony przez osobę trzecią (np. rodzica) na sprzęcie prywatnym dla celów osobistych właściciela może być przekazany do wykorzystania w jednostce i podlega ochronie od momentu zapisania pliku z jego utrwaleniem na nośniku jednostki.
6. Wizerunek może być przechowywany na przenośnych pamięciach tylko jako kopia zapasowa lub w celach wykonania czynności technicznych (przeniesienie danych).
7. Do korzystania z kamery / aparatu jednostki jest uprawniona tylko osoba upoważniona przez Administratora.
8. Umieszczanie zdjęć, filmów na stronie internetowej jednostki, w mediach społecznościowych, czy przekazywanie innym Administratorom (w tym mediom) może być dokonywane tylko przez osobę upoważnioną przez Administratora znającą zasady przetwarzania wizerunku w jednostce.
9. Osoba wymieniona powyżej w pkt. 8 zapewnia:
   - wykorzystanie wizerunku osób, które wyraziły na to zgodę, zarówno na kanwie prawa autorskiego (pierwsza zgoda na rozpowszechnianie wizerunku) oraz na kanwie RODO (druga zgoda na przetwarzanie danych osobowych),
   - spełnienie obowiązku informacyjnego wobec osób, których wizerunek jest wykorzystywany,

- wycofanie wizerunku osób, które cofnęły zgodę na jego przetwarzanie,
- nie umieszczanie zdjęć (filmów) osób, których utrwalony wizerunek można odczytać jako niekorzystny dla ich osoby (nienaturalna pozycja ciała, przymknięte oczy, dłubanie w nosie przez dziecko itp.).

10. Należy okresowo czyścić kartę pamięci aparatu fotograficznego (kamery) i nie przechowywać na nich zarejestrowanego wizerunku nie spełniającego wymogów dalszego wykorzystania w celach promocji jednostki.
11. Zasady z pkt. 10 dotyczą także wizerunku przechowywanego w plikach na innych nośnikach jednostki.
12. Przynajmniej raz w roku należy dokonać przeglądu wszystkich filmów (zdjęć) zarejestrowane w jednostce i usunąć niewykorzystywane filmy (zdjęcia) zwłaszcza dzieci, które już nie uczęszczają do jednostki i pracowników, którzy zakończyli zatrudnienie.
13. W przypadku wykorzystywania danych w celach promocyjnych należy stosować zasadę minimalizacji (mając 100 zdjęć z imprezy, można ją wypromować wybierając np. 10 najlepiej oddających charakter przedsięwzięcia, a nie „wciskać na siłę" wszystkie 100 zdjęć).

XXXII. Organizacja konkursów

1. Podstawą przetwarzania danych w konkursach wewnętrznych (tylko dla uczniów własnych) będzie zazwyczaj realizacja działań w interesie publicznym. W przypadku konkursów zewnętrznych (z udziałem uczestników zewnętrznych) dane przetwarzamy za zgodą.
2. Konkursy wewnętrzne stanowiące naturalną kontynuację realizacji funkcji edukacyjnej, opiekuńczej lub wychowawczej jednostki, a także w związku z upowszechnianiem czytelnictwa przez bibliotekę, nie angażujące nowych niezatwierdzonych przez Administratora technologii, nie wymagają planowania z wykorzystaniem załącznika nr 4 i konsultacji z IOD.
3. W pozostałych przypadkach (niewymienionych w pkt. 2) niezbędne jest planowanie przedsięwzięcia z użyciem formularza nr 4, pozyskaniem opinii IOD i zatwierdzenia Administratora.
4. Przy planowaniu konkursu zewnętrznego lub rozbudowanego konkursu wewnętrznego z nagrodami należy w załączniku nr 4, w opisie przedsięwzięcia wskazać:
   - czy działanie będzie konkursem, czy wybór zwycięzców oparty będzie o czynniki losowe,
   - określić zaangażowane podmioty,
   - określić zasady uczestnictwa i zakres zbieranych danych,
   - zasady zgłaszania uczestnictwa i sposoby jego dokonywania,
   - zasady oceny i sposób spisywania protokołu,
   - wartość nagród i obowiązki podatkowe,
   - sposób realizacji praw osób,
   - okres przechowywania dokumentów,
   - zasady wręczania nagród,
   - sposób wykorzystania prac, nagrań czy zdjęć po konkursie.
5. Udział w konkursach obcych należy konsultować z IOD ilekroć będą wątpliwości w sprawie przetwarzania danych osobowych. Zwłaszcza w sytuacja, gdy szkoła będzie przekazywać dane w imieniu uczestników. W takich przypadkach opiekun dba o wypełnienie obowiązków informacyjnych i zbieranie zgód od uczestników.

6. Do prawidłowego zorganizowania konkursu z nagrodami niezbędne jest stworzenie (prawo podatkowe):
   - Regulaminu,
   - Protokołu prac jury i wyłaniania zwycięzców.

XXXIII. Promocja jednostki

1. Administrator wyznacza katalog zamknięty bieżących narzędzi promocji jednostki (np. strona, internetowa, profil Facebook, gablota itp.) – załącznik nr 5.
2. Inne przedsięwzięcia promocyjne (np. wystawy) należy zaplanować zgodnie z zasadą *privacy by design* (załącznik nr 4).
3. Administrator określa okresy eksponowania danych w poszczególnych nośnikach promocji, tak by można by je podać w klauzulach informacyjnych.
4. W promocji staramy się stosować zasadę minimalizacji (np. ze 100 zdjęć z imprezy wybieramy 10, które adekwatnie pokażą jej przebieg, a nie wrzucamy wszystkie 100 zdjęć na stronę promocyjną).

XXXIV. Kronika jednostki

1. Administrator określa cel przetwarzania danych w kronice i wpisuje do rejestru czynności.
2. Jeśli jednym z celów prowadzenia kroniki jest: prowadzenie zapisów o aktualnej działalności jednostki na tle uwarunkowań gospodarczych, społecznych i ekonomicznych dla przyszłych pokoleń, to wtedy podstawą prawną przetwarzania jest działanie w interesie publicznym.
3. Wykorzystanie kroniki do celów promocji powinno odbywać się za zgodą osób, których dane dotyczą, a w szczególnych wypadkach w interesie publicznym po konsultacji z IOD i ocenie nowego przedsięwzięcia promocyjnego zgodnie z zasadą *privacy by design* (załącznik nr 4).
4. Dane z kroniki mogą być udostępnione osobie fizycznej tylko na jej pisemny wniosek, w którym wskaże interes prawny lub osobisty jednostki. O udostępnieniu danych, bądź odmowie udostępnienia decyduje Administrator po konsultacji z IOD.
5. Dane z kroniki są udostępniane innym wnioskodawcom niż osoby fizyczne na ogólnych zasadach udostępniania (pisemny wniosek z podaniem podstawy prawnej ubiegania się o dane).

XXXV. Zasady zarządzania kluczami

Sposób zarządzania kluczami do jednostki uregulowany jest w odrębnej procedurze.

XXXVI. Poufność personelu sprzątającego

1. Co do zasady personel sprzątający nie przetwarza żadnych danych osobowych, a jeśli wykonuje czynności związane z przetwarzaniem danych otrzymuje od Administratora upoważnienie.
2. Osoby wyłącznie sprzątające jednostkę nie są uprawnione do przetwarzania danych osobowych (w tym w szczególności ich przeglądania), a jedynie do przebywania w strefach przetwarzania tych danych.
3. W przypadku odnalezienia danych osobowych w jakiejkolwiek formie (pozostawionych / zgubionych dokumentów itp.), na terenie jednostki, wokół jednostki lub też w miejscu

wysypywania śmieci, osoba zobowiązania jest do zabezpieczenia tych danych i przekazania ich Administratorowi.

4. Sprzątanie jednostki poza godzinami jej funkcjonowania odbywa się przy zamkniętych drzwiach głównych / bocznych.
5. Osoba sprzątająca otwiera tylko pomieszczenie, które sprząta, pozostałe pozostają zamknięte.
6. Obowiązuje zakaz wpuszczania osób trzecich po godzinach pracy na teren jednostki.
7. Członków personelu sprzątającego obowiązuje zasada dyskrecji – nie wolno rozmawiać poza jednostką o sprawach dzieci, rodziców, nauczycieli i innych osób, zasłyszanych podczas wykonywania obowiązków, w szczególności zgodnie z zasadami preambuły.

XXXVII. Postępowanie dyscyplinarne

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z powyższymi zasadami może też być uznane przez Pracodawcę za naruszenie przepisów dot. ochrony danych osobowych i mogą być wyciągane konsekwencje karne wynikające z Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.