Polityka prywatności Katolickiej Szkoły Podstawowej w Trzciance w zakresie ochrony danych osobowych

1. W dążeniu do zapewnienia wysokiego poziomu ochrony przetwarzanych danych osobowych, w tym zabezpieczenia danych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych w Katolickiej Szkole Podstawowej w Trzciance określa się *Politykę prywatności Katolickiej Szkoły Podstawowej w Trzciance w zakresie ochrony danych osobowych*.
2. Dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania 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.
3. Środowiskiem przetwarzania danych jest placówka oświatowa, w imieniu której obowiązki administratora danych osobowych wykonuje dyrektor szkoły. Na nim spoczywa odpowiedzialność za przetwarzane dane, bez względu na to, kto faktycznie nimi administruje i kto je przetwarza. Podstawowym obowiązkiem administratora jest dbanie o to, aby przetwarzanie danych odbywało się zgodnie z *Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnym rozporządzeniem o ochronie danych)* i aby móc to wykazać.
4. Administratorem szkolnych danych wskazanych w zgodzie na przetwarzanie danych osobowych jest Katolicka Szkoła Podstawowa w Trzciance reprezentowana przez dyrektora szkoły z siedzibą przy ul. Spokojnej 2 w Trzciance (kod pocztowy: 64-980), tel. 67 216 22 56, adres e-mailowy: katolik.trzcianka@gmail.com.
5. Przetwarzanie danych osobowych może być realizowane po spełnieniu jednego z warunków określonych w art. 6 ogólnego rozporządzenia o ochronie danych.
6. Niniejsza polityka prywatności w zakresie ochrony danych osobowych obejmuje wszystkie procesy i czynności przetwarzania danych osobowych w szkole i odnosi się do zabezpieczenia danych osobowych przetwarzanych zarówno w formie papierowej, jak i przy wykorzystaniu systemów teleinformatycznych.
7. Przetwarzanie danych osobowych stanowi operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak ich 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.
8. Dyrektor Katolickiej Szkoły Podstawowej jako administrator zobowiązany jest do zabezpieczenia przetwarzanych danych osobowych poprzez podjęcie środków technicznych i organizacyjnych odpowiadających ryzyku naruszenia praw lub wolności osób fizycznych, z uwzględnieniem wiedzy technicznej, kosztów wdrożenia oraz charakteru, zakresu, kontekstu i celów przetwarzania.
9. Administrator danych:
    1) nie ma konieczności wyznaczenia inspektora ochrony danych w przypadku szkoły prowadzonej przez podmiot niepubliczny, zgodnie z art. 37 ogólnego rozporządzenia o ochronie danych i art. 9 ustawy o ochronie danych osobowych,
    2) ma wdrażać odpowiednie i skuteczne środki techniczne i organizacyjne:
        a) mają one zapewniać najwyższy znany i możliwy w chwili przetwarzania danych poziom ochrony,

b) nie może być to czynność jednorazowa, środki te są w razie potrzeby poddawane przeglądom i uaktualniane,
c) dokonuje tego, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia,
d) jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki te obejmują wdrożenie przez administratora odpowiedniej polityki ochrony danych,

3) prowadzi komunikację z podmiotem danych i przekazuje mu informacje w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny,
4) ułatwia podmiotom danych wykonywanie ich praw,
5) nieodpłatnie udziela podmiotom danych informacji, również na ich żądanie, czas na udzielenie informacji wynosi maksymalnie miesiąc,
6) weryfikuje tożsamość osób wnoszących żądania udzielenia informacji,
7) potwierdza, czy przetwarzane są dane osobowe dotyczące danej osoby fizycznej, a jeżeli to następuje, udziela informacji wskazanych ogólnym rozporządzeniem o ochronie danych,
8) ułatwia osobie, której dane dotyczą, wykonywanie jej praw z art. 15–22 ogólnego rozporządzenia o ochronie danych,
9) informuje osobę, której dane dotyczą, o działaniach, jakie podjął, w związku z jej żądaniami opartymi na art. 15–22 ogólnego rozporządzenia o ochronie danych,
10) uzasadnia odrzucenie żądania osoby, której dane dotyczą, i poucza ją o prawie skargi,
11) umożliwia dostęp do jej danych osobie, której one dotyczą,
12) dokonuje sprostowania i uzupełniania danych,
13) usuwa dane,
14) ogranicza przetwarzanie danych,
15) powiadamia o sprostowaniu lub usunięciu danych osobowych bądź o ograniczeniu ich przetwarzania,
16) dokonuje przenoszenia danych.

10. Do obowiązków administratora danych należą:
    1) poddawanie przeglądom i uaktualnianie stosowanych technicznych i organizacyjnych środków ochrony danych osobowych,
    2) wdrożenie przez administratora danych odpowiednich polityk ochrony,
    3) stosowanie przez administratora danych zatwierdzonych kodeksów postępowania lub zatwierdzonego mechanizmu certyfikacji,
    4) wydawanie upoważnień do przetwarzania danych osobowych,
    5) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
    6) ewidencjonowanie oświadczeń osób upoważnionych o zaznajomieniu się z zasadami zachowania bezpieczeństwa danych,
    7) określanie potrzeb w zakresie stosowanych w szkole zabezpieczeń, zatwierdzanie rozwiązań i nadzorowanie prawidłowości ich wdrożenia,
    8) podnoszenie świadomości i kwalifikacji osób przetwarzających dane osobowe w szkole.
11. Administrator danych — dyrektor szkoły, może wyznaczyć pracownika administracyjnego, który będzie dbał o dokumentację związaną z danymi i będzie podlegał dyrektorowi szkoły.
12. Osobom udostępniającym dane osobowe szkole przysługuje prawo dostępu do treści danych oraz ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także prawo sprzeciwu, zażądania zaprzestania przetwarzania i przenoszenia danych, jak również prawo do cofnięcia zgody w dowolnym momencie oraz prawo do wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych.
13. Dane udostępnione przez osoby nie będą podlegały profilowaniu. Jest ono dopuszczalne tylko w wyniku obowiązku profilowania podyktowanego prawem zewnętrznym.
14. Administrator danych nie ma zamiaru przekazywać danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

15. Dane osobowe będą przechowywane przez okres określony prawem zewnętrznym.
16. W przypadku Katolickiej Szkoły Podstawowej w Trzciance wymienia się następujące zbiory danych osobowych:
    1) dokumentacja nauczania prowadzona przez sekretariat szkolny — dane pracownicze, dane dzieci i ich rodziców, dane kontrahentów, dane finansowo-księgowe, rejestr korespondencji, dane osób ubiegających się o pracę,
    2) dokumentacja nauczania prowadzona przez wychowawców klas,
    3) dokumentacja nauczania prowadzona przez nauczycieli,
    4) dokumentacja prowadzona w gabinecie profilaktyki zdrowotnej przez pielęgniarkę szkolną,
    5) dokumentacja nauczania prowadzona przez dostawcę dziennika elektronicznego Uonet+ firmę Vulcan Sp. z o.o., ul. Wołowska 6, 51-116 Wrocław, tel. 71 757 29 29, pod adresem strony internetowej https://uonetplus.vulcan.net.pl/powiatczarnkowskotrzcianecki,
    6) zbiór danych dotyczących życia szkoły prowadzony w witrynie szkolnej obecnej pod adresem internetowym http://www.katolik.trzcianka.com.pl,
    7) zbiór danych dotyczących życia szkoły prowadzony na szkolnym koncie Facebooka obecnym pod adresem internetowym https://www.facebook.com/katolik.trzcianka/?ref=hl,
    8) zbiór danych nauczycieli i pozostałych pracowników szkoły prowadzony przez pracownika służby BHP,
    9) zbiór danych dokumentacji nauczania odnoszący się do uczniów i nauczycieli tworzony w ramach Systemu Informacji Oświatowej,
    10) zbiór danych dokumentacji nauczania odnoszący się do uczniów i nauczycieli tworzony przez wydział oświaty jednostki samorządu terytorialnego,
    11) zbiór danych dokumentacji nauczania odnoszący się do uczniów i nauczycieli tworzony przez Ministerstwo Edukacji Narodowej,
    12) zbiór danych dokumentacji nauczania odnoszący się do uczniów i nauczycieli tworzony przez Kuratorium Oświaty w Poznaniu,
    13) zbiory danych odnoszące się do uczniów i nauczycieli tworzony przez operatorów wycieczkowych w ramach organizacji wyjazdów szkolnych (np. wycieczki szkolne, zielone szkoły),
    14) zbiory danych odnoszące się do uczniów i nauczycieli tworzony przez ubezpieczycieli,
    15) zbiory danych odnoszące się do uczniów i nauczycieli tworzony przez zewnętrzne podmioty szkoleniowe,
    16) zbiór danych odnoszący się do uczniów i nauczycieli tworzony przez wizyjny monitoring szkolny realizowany w celach bezpieczeństwa.
17. Pracownik upoważniony do przetwarzania danych osobowych:
    1) chroni prawo do prywatności osób fizycznych powierzających szkole swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w polityce prywatności Katolickiej Szkoły Podstawowej w Trzciance w zakresie ochrony danych osobowych,
    2) zapoznaje się zasadami określonymi w polityce prywatności i składa oświadczenie o znajomości tych przepisów, zgodnie z przyjętym wzorem oświadczenia o zachowaniu poufności i zapoznaniu się z przepisami o ochronie danych osobowych,
    3) zostaje upoważniony przez administratora danych osobowych — dyrektora szkoły, do przetwarzania danych osobowych w Katolickiej Szkole Podstawowej zgromadzonych w formie tradycyjnej oraz w systemach informatycznych w celach związanych z wykonywaniem obowiązków na stanowisku pracownika szkoły, zgodnie z przyjętym wzorem upoważnienia do przetwarzania danych osobowych,
    4) za przetwarzanie danych osobowych niezgodnie z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te

dane dotyczą, ponosi odpowiedzialność karną, wynikająca z przepisów ustawy o ochronie danych osobowych lub pracowniczą na zasadach określonych w kodeksie pracy.

18. W szkole pracownik przetwarza dane osobowe za pomocą przyjętych systemów informatycznych, w związku z czym przestrzega się następujące wytyczne:
    1) Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych w szkole.
    2) Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników odpowiada administrator danych — dyrektor szkoły.
    3) Usuwanie kont stosowane jest wyłącznie w uzasadnionych przypadkach, standardowo, przy ustaniu potrzeby utrzymywania konta danego użytkownika ulega ono dezaktywacji w celu zachowania historii jego aktywności.
    4) Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu stosunku pracy, co jest równoznaczne z cofnięciem uprawnień do przetwarzania danych osobowych.
    5) Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień. Zmiana hasła jest wymuszona automatycznie przez system.
    6) System informatyczny służący do przetwarzania danych osobowych posiada mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych przez daną uprawnioną osobę.
    7) W celu wykonywania pracy w systemie informatycznym użytkownik loguje się do systemu przetwarzania danych za pomocą identyfikatora i hasła.
    8) W sytuacji tymczasowego zaprzestania pracy na skutek nieobecności przy stanowisku komputerowym należy uniemożliwić osobom postronnym korzystanie z systemu informatycznego poprzez wylogowanie się z sytemu.
    9) W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor w sposób uniemożliwiający wgląd w wyświetlaną treść.
    10) Użytkownik wyrejestrowuje się z systemu informatycznego przed wyłączeniem stacji komputerowej poprzez zamknięcie programu przetwarzającego dane.
    11) Pracownik korzystający z systemu informatycznego zobowiązany jest do powiadomienia administratora danych osobowych w razie:
        a) podejrzenia naruszenia bezpieczeństwa systemu,
        b) braku możliwości zalogowania się użytkownika na jego konto,
        c) stwierdzenia fizycznej ingerencji w przetwarzana dane,
        d) stwierdzenia użytkowania narzędzia programowego lub sprzętowego niezgodnie z ich przeznaczeniem.
    12) Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane wyłącznie przez pracowników szkoły lub przez upoważnionych przedstawicieli wykonawców. Prace te powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych. Przed rozpoczęciem tych prac przez osoby niebędące pracownikami szkoły należy dokonać potwierdzenia tożsamości tychże osób.
    13) Wszelkie wydruki z systemów informatycznych zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach i po upływie ich przydatności są niszczone przy użyciu niszczarek w sposób uniemożliwiający ich odczytanie.
    14) Niszczenie zapisów na nośnikach danych powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
    15) Uszkodzone nośniki danych przed ich wyrzuceniem należy fizycznie zniszczyć w niszczarce.

19. Pomieszczenia, w których przetwarzane są dane osobowe, pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. Opuszczenie pomieszczenia musi być poprzedzone przeniesieniem danych osobowych do odpowiednio zabezpieczonego miejsca. Przy planowanej dłuższej nieobecności pracownika pomieszczenie winno być zamknięte na klucz.
20. Klucze do szaf, w których przechowywane są dane osobowe, mają jedynie pracownicy upoważnieni do przetwarzania danych osobowych, w zakresie zgodnym z kategorią danych.
21. Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w szkole powinno odbywać się po uzyskaniu upoważnienia lub skonsultowane z administratorem danych, w przypadku pracowników upoważnionych do przetwarzania tych danych — na podstawie ogólnie obowiązujących przepisów.
22. Dane są przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość").
23. Dane są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu").
24. Gromadzenie danych odbywa się adekwatnie, stosownie oraz w sposób ograniczony do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych").
25. Dane są prawidłowe i w razie potrzeby uaktualniane. Podejmuje się wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość").
26. Dane są przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania").
27. Dane są przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").
28. Administrator danych jest odpowiedzialny za przestrzeganie przepisów dotyczących zasad przetwarzania danych musi być w stanie wykazać ich przestrzeganie („rozliczalność").
29. Przetwarzanie danych zwykłych posiada podstawę prawną.
30. Przetwarzanie szczególnych kategorii danych osobowych posiada podstawę prawną.
31. Jeżeli dane przetwarzane są na podstawie zgody administrator danych jest w stanie wykazać, że osoba której dane dotyczą wyraziła zgodę na przetwarzanie danych.
32. Jeżeli dane przetwarzane są na podstawie zgody, a zgoda jest wyrażana w pisemnym oświadczeniu, przedstawia się ją w sposób pozwalający wyraźnie odróżnić ją od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
33. Jeżeli dane przetwarzane są na podstawie zgody, wyrażona zgoda jest łatwa do wycofania.
34. Jeżeli dane przetwarzane są na podstawie zgody, osoba, która zgodę ma wyrazić, jest informowana o prawie jej wycofania w każdej chwili przed jej wyrażeniem.
35. Jeżeli dane przetwarzane są na podstawie zgody, od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.
36. W przypadku osób niepełnoletnich zgodę na przetwarzanie danych wyraża lub aprobuje osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody.
37. Administrator danych, uwzględniając dostępną technologię, podejmuje rozsądne starania, by zweryfikować, czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła zgodę lub ją zaaprobowała.

38. Informacje podawane w obowiązku informacyjnym oraz komunikacja w sprawach art. 15–22 ogólnego rozporządzenia o danych osobowych udzielane są w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie. Informacji udziela się na piśmie, w tym w stosownych przypadkach elektronicznie lub w inny sposób (np. ustnie).
39. Administrator ułatwia osobie, której dane dotyczą, uzyskanie wszelkich informacji w przedmiocie przetwarzanych danych.
40. Administrator bez zbędnej zwłoki, a w każdym razie w terminie miesiąca od otrzymania żądania, udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15-22 ogólnego rozporządzenia o danych osobowych.
41. Jeżeli występuje przedłużenie terminu do spełnienia żądań osoby, której dane dotyczą w ramach art. 15-22 ogólnego rozporządzenia o danych osobowych, występuje to z uwagi na skomplikowany charakter żądania lub liczbę żądań, czas udzielenia informacji jest jednak nie dłuższy niż dalsze dwa miesiące.
42. Obowiązek informacyjny oraz wykonywanie praw przysługujących osobie, której dane dotyczą w ramach art. 15-22 ogólnego rozporządzenia o danych osobowych, odbywa się bez pobierania opłat.
43. Odmówienie podjęcia działań w związku z żądaniem na podstawie art. 15–22 ogólnego rozporządzenia o danych osobowych lub pobieranie rozsądnej opłaty następuje, jeżeli żądania osoby są nadmierne lub ewidentnie nieuzasadnione w szczególności ze względu na swój ustawiczny charakter.
44. Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby składającej żądanie w zakresie art. 15-22 ogólnego rozporządzenia o danych osobowych, żąda dodatkowych informacji niezbędnych do potwierdzenia tożsamości.
45. W ramach weryfikacji dopełnienia obowiązku informacyjnego w przypadku gromadzenia danych od osoby, której dane dotyczą, oraz z innych źródeł, przyjmuje się następujące wymogi podlegające zasadzie rozliczalności zgodnie z ogólnym rozporządzeniem o danych osobowych:
    1) określenie własnej tożsamości i danych kontaktowych oraz, gdy ma to zastosowanie, określenie tożsamości i danych kontaktowych swojego przedstawiciela,
    2) gdy ma to zastosowanie — dane kontaktowe inspektora ochrony danych,
    3) cele przetwarzania danych osobowych oraz podstawa prawna przetwarzania,
    4) określenie prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią,
    5) określenie informacji o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
    6) gdy ma to zastosowanie — informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych,
    7) wskazanie okresu, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, określenie kryteriów ustalania tego okresu,
    8) rozpowszechnianie przez administratora informacji o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
    9) określenie, jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) — informacji o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
    10) podawanie informacji o prawie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych,

11) podawanie informacji, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
12) określenie kwestii tego, że jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji.

46. W szkole są realizowane prawa dotyczące ochrony danych:
    1) prawo dostępu do danych przysługującego osobie, której dane dotyczą, w tym wydawanie kopii danych,
    2) prawo do usunięcia danych (prawo do bycia zapomnianym) i w zgodzie z prawem zewnętrznym,
    3) prawo do ograniczenia przetwarzania danych,
    4) obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania,
    5) prawo do przenoszenia danych,
    6) możliwość wniesienia sprzeciwu przez osobę, której dane dotyczą — z przyczyn związanych z jej szczególną sytuacją — wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e ogólnego rozporządzenia o danych osobowych (wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej) lub f (prawnie usprawiedliwiony cel administratora danych lub strony trzeciej), w tym profilowania na podstawie tych przepisów,
    7) poinformowanie osoby, której dane dotyczą, najpóźniej przy okazji pierwszego kontaktu, w sposób jasny i odrębny od wszelkich innych informacji o możliwości wniesienia sprzeciwu,
    8) niepodejmowanie decyzji względem osoby, której dane dotyczą, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, o ile jest to dopuszczalne, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa,
    9) jeżeli profilowanie jest dopuszczalne, administrator danych wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji,
    10) niepoddawanie profilowaniu danych szczególnej kategorii, chyba że osoba, której dane dotyczą wyraziła zgodę lub przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.
47. W szkole uwzględnia się ochronę danych w fazie projektowania oraz domyślną ochronę danych z uwzględnieniem następujących wytycznych:
    1) uwzględnianie ochrony danych w fazie projektowania,
    2) domyślna ochrona danych (np. pseudonimizacja),
    3) korzystanie przez administratora danych z usług podmiotów przetwarzających zapewniających wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych w celu spełniania wymogów co do przetwarzania zgodnie z ogólnym rozporządzeniem o danych osobowych oraz realizowanie ochrony praw osób, których dane dotyczą,
    4) niekorzystanie przez podmiot przetwarzający z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora.
48. W szkole w trakcie zawierania umów dotyczących przetwarzania i przechowywania danych osobowych dba się o następujące elementy umowy o powierzeniu przetwarzania i przechowywania danych:
    1) przedmiot i czas trwania przetwarzania i przechowywania,

2) charakter i cel przetwarzania,
3) rodzaj danych osobowych oraz kategorie osób, których dane dotyczą,
4) obowiązki i prawa administratora danych,
5) wskazanie, że przetwarzanie danych odbywa się wyłącznie na udokumentowane polecenie administratora,
6) zapewnienie, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
7) realizowanie środków bezpieczeństwa danych, zgodnie z art. 32 ogólnego rozporządzenia o danych osobowych,
8) zobowiązanie podmiotu przetwarzającego do przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego,
9) pomoc administratorowi danych poprzez odpowiednie środki techniczne i organizacyjne w celu wywiązania się z obowiązku odpowiadania na żądania osoby, której dane dotyczą,
10) pomoc administratorowi danych w wywiązaniu się z obowiązku zapewnienia bezpieczeństwa danych, zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu, zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, oceny skutków przetwarzania, uprzednich konsultacji, zgodnie z art. 32–36 ogólnego rozporządzenia o ochronie danych osobowych,
11) zobowiązanie do usunięcia lub zwrotu administratorowi danych wszelkich danych osobowe oraz usunięcie wszelkich ich istniejących kopii, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych,
12) zobowiązanie do udostępnienia administratorowi danych wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w artykule 28 ogólnego rozporządzenia o danych osobowych oraz umożliwienie administratorowi danych lub audytorowi upoważnionemu przez administratora danych przeprowadzanie audytów, w tym inspekcji, i przyczynianie się do nich.

49. Przy określaniu minimalnych wymogów, które powinien spełnić podmiot przetwarzający dane, należy brać pod uwagę charakter, skalę i zakres przetwarzania oraz, jeśli to konieczne, uwzględniać wyniki szacowania ryzyka przeprowadzone w szkole w tym zakresie.
50. Powierzenie przetwarzania danych osobowych odbywa się na podstawie pisemnej umowy lub porozumienia, które wyraźnie określają charakter i cel przetwarzania, przedmiot i czas trwania przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, oraz obowiązki i prawa administratora i podmiotu przetwarzającego.
51. Dokumentacja, na podstawie której następuje powierzenie danych, musi mieć formę pisemną Dopuszcza się prowadzenie tej dokumentacji w formie elektronicznej.
52. Dokumentacja, na podstawie której następuje powierzenie danych, musi gwarantować Administratorowi realizację zadań wynikających z zapisów art. 28 ogólnego rozporządzenia o ochronie danych, w tym w szczególności:
    1) możliwość egzekwowania wskazanych w dokumentacji obowiązków podmiotu przetwarzającego,
    2) możliwość przeprowadzanie kontroli/audytów w zakresie realizacji umowy powierzenia,
    3) możliwości weryfikacji, czy powierzone dane nie zostały przekazane innemu podmiotowi przez przetwarzającego bez zgody („podpowierzenie danych”).
53. Przetwarzanie odbywa się z upoważnienia administratora lub podmiotu przetwarzającego, co oznacza, że podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii Europejskiej lub prawo państwa członkowskiego.

54. Rejestrowanie czynności przetwarzania prowadzona w formie pisemnej, w tym elektronicznej, rejestru czynności przetwarzania danych osobowych nie dotyczy podmiotu zatrudniającego mniej niż 250 osób, zgodnie z art. 30 ust. 5 ogólnego rozporządzenia o danych osobowych.
55. Administrator lub podmiot przetwarzający (ewentualnie przedstawiciel) współpracuje z organem nadzorczym w ramach wykonywania przez niego swoich zadań, tj. z Prezesem Urzędu Ochrony Danych Osobowych.
56. Dbając o bezpieczeństwo danych osobowych, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku uwzględniając stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cel przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. Uwzględnienie w szczególności ryzyka wiążącego się z przetwarzaniem (szacowanie ryzyka), w szczególności wynikające z:
    1) przypadkowego lub niezgodnego z prawem zniszczenia,
    2) utraty, modyfikacji, nieuprawnionego ujawnienia,
    3) nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
57. W trakcie procesu zarządzania ryzykiem przeprowadzana jest identyfikacja zagrożeń bezpieczeństwa danych osobowych oraz określane są podatności i skutki wystąpienia tych zagrożeń oraz kategoryzacja danych i czynności przetwarzania pod kątem ryzyka, które przedstawiają.
58. W ramach procesu zarządzania ryzykiem przeprowadzana jest:
    1) analiza ryzyka dla czynności przetwarzania danych lub ich kategorii,
    2) ocena skutków dla ochrony danych objętych wysokim ryzykiem naruszenia praw i wolności osób.
59. Uzyskane, w ramach procesu analizy ryzyka, wyniki są podstawą do dalszego postępowania ze zidentyfikowanymi ryzykami w kontekście wdrożenia rozwiązań technicznych i organizacyjnych, które pozwolą ochronić dane osobowe przed utratą ich podstawowych atrybutów (poufności, integralności, dostępności, rozliczalności) oraz pozwolą zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania tych danych w szkole.
60. Ocena skutków czynności przetwarzania dla ochrony danych oraz ich wpływu na naruszenia praw lub wolności osób fizycznych obejmuje analizę i rozpatrywanie możliwych sytuacji i scenariuszy naruszenia ochrony danych osobowych przy uwzględnieniu charakteru, zakresu, kontekstu i celów przetwarzania, oraz różnego prawdopodobieństwa wystąpienia i wagi zagrożenia.
61. W ramach przeprowadzanej oceny ryzyka zagrożenia bezpieczeństwa danych należy brać pod uwagę wskazane przez Prezesa Urzędu Ochrony Danych Osobowych rodzaje procesów i czynności przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych.
62. Dbając o bezpieczeństwo danych osobowych, administrator i podmiot przetwarzający wdrażają:
    1) pseudonimizację i szyfrowanie danych osobowych,
    2) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
    3) zdolność do szybkiego przywracania dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
    4) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
63. Administrator i podmiot przetwarzający stosują zatwierdzony kodeks postępowania lub zatwierdzony mechanizm certyfikacji celem wykazania wdrożenia odpowiednich środków technicznych i organizacyjnych dla bezpieczeństwa danych osobowych.
64. Administrator oraz podmiot przetwarzający podjęli działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii Europejskiej lub prawo państwa członkowskiego.

65. W przypadku zgłaszania naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych dba się o następujące wytyczne:
    1) zgłaszanie naruszenia ochrony danych osobowych powodujące ryzyko naruszenia praw i wolności osób fizycznych przez administratora w terminie 72 godzin po stwierdzeniu naruszenia do organu nadzorczego,
    2) podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi,
    3) zgłoszenie zawiera wymagane elementy zgodne z art. 33 ust 1 a–d ogólnego rozporządzenia o danych osobowych,
    4) administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
66. W przypadku naruszenia ochrony danych osobowych zawiadamia się osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych:
    1) o naruszeniu ochrony danych osobowych powodującym wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu,
    2) zawiadomienie jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b, c i d ogólnego rozporządzenia o danych osobowych.
67. W przypadku przekazywania danych osobowych do państw trzecich, tj. państw, które nie należą do Europejskiego Obszaru Gospodarczego, są spoza Unii Europejskiej, w szczególności do takich, które nie zapewniają na swoim terytorium odpowiedniego poziomu ochrony danych osobowych, a przekazanie ich wiąże się z dużym ryzykiem naruszenia praw i wolności osób, których dane dotyczą, jak to dzieje się np. w ramach wymiany uczniów pomiędzy różnymi szkołami zagranicznymi, spełnia się następujące wytyczne zgodnie z art. 45, 46 i 49 ogólnego rozporządzenia o danych osobowych:
    1) przekazywanie danych osobowych do państwa trzeciego znajduje podstawę w decyzji Komisji Europejskiej,
    2) przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej następuje poprzez zapewnienie odpowiednich zabezpieczeń, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej,
    3) przekazywanie danych znajduje podstawę w decyzji wydanej przez organ nadzorujący ochronę danych osobowych, a która to dotychczas nie została zmieniona, zastąpiona, uchylona,
    4) jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej następuje na podstawie jednego z wyjątków.
68. Osoby przetwarzające dane osobowe zobowiązane są do stosowania postanowień zawartych w niniejszym dokumencie oraz pozostałej dokumentacji, która uszczegóławia wymagania i zasady ochrony danych osobowych.
69. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako naruszenie obowiązków służbowych.
70. Polityka prywatności w zakresie ochrony danych osobowych oraz pozostała dokumentacja, która uszczegóławia wymagania i zasady ochrony danych osobowych, może być udostępniania osobom trzecim, jeżeli nie zawiera w swojej treści i w załącznikach szczegółowych informacji o wdrożonych w szkole zabezpieczeniach danych osobowych oraz innych informacji prawnie chronionych.