**Zarządzenie nr 10/2022/2023**

**Dyrektora Szkoły Podstawowej nr 16 w Częstochowie z dnia 08 listopada 2022 r.**

**w sprawie wprowadzenia Procedury wyboru dostawcy przetwarzającego dane osobowe w Szkole Podstawowej nr 16 im. Bolesława Chrobrego w Częstochowie**

Na podstawie rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (ogólne rozporządzenie o ochronie danych) zarządzam, co następuje:

1. Wprowadza się do stosowania Procedurę wyboru dostawcy przetwarzającego dane osobowe w Szkole Podstawowej nr 16 im. Bolesława Chrobrego w Częstochowie.
2. Procedury stanowią załącznik do niniejszego zarządzenia.

1. Zarządzenie wchodzi w życie z dniem podpisania.

(-)Jolanta Dominiak

Dyrektor szkoły

Załącznik nr 1do Zarządzenia nr 10/2022/2023 dyrektora

Szkoły Podstawowej nr 16 im. Bolesława Chrobrego w Częstochowie

z dnia 08 listopada 2022r.

**Procedura wyboru dostawcy przetwarzającego dane osobowe**

**1. Definicje**

**1.1.** Administrator –Szkoła Podstawowa nr 16 im. Bolesława Chrobrego w Częstochowie reprezentowana przez dyrektora szkoły.

**1.3. Dostawca** – osoba fizyczna prowadząca działalność gospodarczą lub jednostka organizacyjna posiadająca osobowość prawną lub nieposiadająca osobowości prawnej, której na podstawie zawartej z Administratorem umowy dotyczącej korzystania przez Administratora z określonych usług mogą zostać powierzone do przetwarzania Dane osobowe.

**1.5. Podmiot Danych** – osoba, której dotyczą Dane osobowe przetwarzane przez Administratora.

**1.6. Procedura** – niniejsza Procedura wyboru Dostawcy – podmiotu przetwarzającego Dane osobowe na zlecenie Administratora.

**1.7. RODO** – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (ogólne rozporządzenie o ochronie danych).

**1.8. Umowa** – umowa powierzenia przetwarzania danych osobowych – umowa pomiędzy Administratorem a Dostawcą, w ramach wykonania której Dostawcy zostaje powierzone przetwarzanie Danych osobowych pochodzących od Administratora.

**2. Warunki dopuszczalności powierzenia Danych osobowych Dostawcy**

**2.1.** Warunkiem dopuszczalności powierzenia przetwarzania Danych osobowych jest zapewnienie przez Dostawcę gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, tak by przetwarzanie spełniało wymogi RODO i chroniło prawa Podmiotów Danych.

**2.2.** Administrator może powierzyć Dostawcy przetwarzanie Danych osobowych na podstawie Umowy w następujących przypadkach:

**2.2.1.** gdy Dostawca stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO;

**2.2.2.** gdy Dostawca posiada zatwierdzony mechanizm certyfikacji lub znak jakości w zakresie ochrony Danych osobowych, o których mowa w art. 42 RODO i które obejmują całość operacji przetwarzania Danych osobowych przez Dostawcę w ramach realizacji Umowy;

**2.2.3.** gdy spełnione są warunki określone w rozdziale 4 Procedury wyboru Dostawcy;

**2.2.4.** gdy Dostawca przeszedł pozytywną weryfikację zgodnie z rozdziałem 5 Procedury wyboru Dostawcy.

**2.3.** W szczególnie uzasadnionych przypadkach Administrator może zawrzeć Umowę z danym Dostawcą bez konieczności jego weryfikacji.

**3. Zawarcie Umowy z Dostawcą**

**3.1.** Administrator ustala, czy spełniony został choćby jeden z warunków określonych w pkt 2.2.1–2.2.3. W takim przypadku Administrator może zawrzeć z Dostawcą Umowę.

**3.2.** W razie gdy żaden z warunków określonych w pkt 2.2.1–2.2.3 nie jest spełniony, Administrator przystępuje do weryfikacji Dostawcy zgodnie z rozdziałem 5 Procedury wyboru Dostawcy.

**3.3.** Przed zawarciem Umowy Administrator może zasięgnąć opinii Inspektora Ochrony Danych (dalej IOD). IOD ma prawo wydania negatywnej opinii w przedmiocie zawarcia Umowy z Dostawcą w każdym przypadku, także gdy spełnione są przesłanki określone w punktach 2.2.1–2.2.3. Ostateczną decyzję w przedmiocie zawarcia Umowy z Dostawcą podejmuje Administrator.

**4. Minimalne wymagania dla Dostawcy**

**4.1.** Jeżeli nie zachodzą przypadki określone w pkt 2.2.1 lub 2.2.2, Administrator może zawrzeć Umowę z Dostawcą bez konieczności jego weryfikacji w sposób określony w rozdziale 5, jeżeli spełnione są łącznie wszystkie następujące warunki:

**4.1.1.** powierzenie nie zakłada profilowania Podmiotów danych przez Dostawcę na zlecenie Administratora oraz

**4.1.2.** powierzenie nie obejmuje zautomatyzowanego podejmowania decyzji wobec Podmiotów danych przez Administratora z wykorzystaniem usług Dostawcy; oraz

**4.1.3.** powierzenie nie zakłada systematycznego monitorowania (obserwacji) zachowań Podmiotów danych; oraz

**4.1.4.** powierzenie nie obejmuje szczególnych kategorii Danych osobowych i Danych osobowych dotyczących wyroków skazujących, ani naruszeń prawa, o których mowa w art. 9 i 10 RODO; oraz

**4.1.5.** powierzenie nie wiąże się z przetwarzaniem na dużą skalę Danych osobowych przez Dostawcę (przy ocenie tego kryterium należy wziąć pod uwagę liczbę Podmiotów danych, zakres powierzanych danych, czas trwania powierzenia oraz zakres geograficzny przetwarzania); oraz

**4.1.6.** powierzenie nie wiąże się z innowacyjnym wykorzystaniem nowych rozwiązań technologicznych (przy czym za innowacyjne wykorzystanie nowych technologii nie uważa się znanych już sposobów wykorzystania nowych technologii); oraz

**4.1.7.** w ramach powierzenia nie dochodzi do transferu Danych osobowych poza Europejski Obszar Gospodarczy (EOG).

**4.2.** Przed zawarciem Umowy z Dostawcą w przypadku, o którym mowa w niniejszym rozdziale, Administrator może zasięgnąć opinii IOD. IOD może zarekomendować w szczególności przeprowadzenie weryfikacji Dostawcy zgodnie z rozdziałem 5 Procedury wyboru Dostawcy.

**4.3.** Ostateczną decyzję w przedmiocie zawarcia Umowy z Dostawcą podejmuje Administrator.

**5. Weryfikacja Dostawcy**

**5.1.** W przypadku powzięcia decyzji w przedmiocie przeprowadzenia weryfikacji Dostawcy weryfikacja przeprowadzana jest poprzez przesłanie do Dostawcy Ankiety dla podmiotu przetwarzającego (procesora) stanowiącej załącznik nr 1 do niemniejszej procedury.

**5.1.1.** Dostawca uzupełnia odpowiedzi na pytania zawarte w Ankiecie;

**5.1.2.** Administrator na podstawie udzielonych odpowiedzi określa poziom zgodności w zakresie wymagań.

**5.2.** Dodatkowo weryfikacja przeprowadzana jest poprzez analizę wszystkich lub wybranych następujących informacji lub czynników:

**5.2.1.** informacje publikowane przez Dostawcę na stronie internetowej oraz inne informacje uzyskane bezpośrednio od Dostawcy, w tym informacje o tym, czy Dostawca dysponuje odpowiednią wiedzą fachową nt. ochrony Danych osobowych oraz środkami technicznymi i organizacyjnymi gwarantującymi bezpieczeństwo Danych osobowych;

**5.2.2.** posiadany przez Dostawcę certyfikat lub przedłożone oświadczenie dotyczące wdrożonego systemu zarządzania bezpieczeństwem informacji, zgodnego z wymaganiami normy ISO/IEC 27001 lub innymi adekwatnymi normami;

**5.2.4.** opinie i rekomendacje nt. współpracy z Dostawcą dostępne w Internecie lub uzyskane z innych możliwych źródeł w granicach obowiązującego prawa;

**5.2.5.** informacje nt. toczących się w stosunku do Dostawcy postępowań administracyjnych lub sądowych dotyczących ochrony Danych osobowych, ochrony informacji niejawnych lub tajemnic szczególnie chronionych.

**5.3.** Przed zawarciem Umowy z Dostawcą w przypadku, o którym mowa w niniejszym rozdziale, Administrator może zasięgnąć opinii IOD. Ostateczną decyzję w przedmiocie zawarcia Umowy z Dostawcą podejmuje Administrator na podstawie analizy całości zgromadzonego materiału.

**6. Uprawnienia IOD**

**6.1.** Przed zawarciem Umowy z Dostawcą Administrator informuje IOD o sposobie weryfikacji Dostawcy zgodnie z niniejszą procedurą oraz o wynikach takiej weryfikacji.

**6.2.** W każdym przypadku IOD:

**6.2.1.** ma prawo wyrażenia opinii w przedmiocie zawarcia Umowy z Dostawcą oraz metod weryfikacji. Opinia powinna być sporządzona na piśmie lub w formie e-maila. Opinia negatywna powinna być umotywowana;

**6.2.2.** ma prawo żądać dodatkowych informacji od Dostawcy, jeżeli w jego ocenie takie dodatkowe informacje są w danym przypadku niezbędne w celu dokonania oceny Dostawcy;

**6.2.3.** ma prawo zarekomendować przeprowadzenie audytu u Dostawcy lub zlecić podmiotowi zewnętrznemu przeprowadzenie takiego audytu, jeżeli w jego ocenie przeprowadzenie audytu w danym przypadku jest niezbędne w celu dokonania oceny Dostawcy.

**6.3.** Opinie IOD, wydawane na podstawie Procedury wyboru Dostawcy, nie mają charakteru wiążącego.

**7. Postanowienia końcowe**

7.1. Procedura obowiązuje od 08.11.2022 r.

Załącznik nr 1 do Procedury wyboru dostawcy przetwarzającego dane osobowe

|  |
| --- |
|  |
|
|  **Ankieta dla podmiotu przetwarzającego (procesora)** |
| **Lp.** | **Pytanie**  | **Odpowiedź** | **Poziom zgodności** | **Uwagi** |
| **1** | Czy zgodnie z art. 29 RODO osoby wykonujące operacje na danych osobowych otrzymały od podmiotu przetwarzającego upoważnienia do przetwarzania danych, w których został określony w szczególności zakres przetwarzanych przez te osoby danych?  |   | **Wybierz poziom zgodności** |   |
| **2** | Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania zawierający wszystkie informacje wskazane w art. 30 ust. 2 RODO? |   | **Wybierz poziom zgodności** |   |
| **3** | Czy podmiot przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych? |   | **Wybierz poziom zgodności** |   |
| **4** | Czy podmiot przetwarzający jest w stanie wykazać przestrzeganie danych zasad dotyczących przetwarzania osobowych m. in. poprzez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji ochrony danych osobowych? |   | **Wybierz poziom zgodności** |   |
| **5** | Czy podmiot przetwarzający zapewnia, aby nowozatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa?  |   | **Wybierz poziom zgodności** |   |
| **6** | Czy podmiot przetwarzający dba o bieżące doskonalenie wiedzy swoich pracowników poprzez cykliczne szkolenia oraz inne działania mające na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych?  |   | **Wybierz poziom zgodności** |   |
| **7** | Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych zostali zobowiązani do zachowania ich w tajemnicy? |   | **Wybierz poziom zgodności** |   |
| **8** | Czy podmiot przetwarzający stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 RODO? |   | **Wybierz poziom zgodności** |   |
| **9** | Czy w ciągu dwóch ostatnich lat podmiot przetwarzający poddawał zewnętrznej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych? |   | **Wybierz poziom zgodności** |   |
| **10** | Czy podmiot przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych/podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych? |   | **Wybierz poziom zgodności** |   |
| **11** | Czy zastosowano środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu? |   | **Wybierz poziom zgodności** |   |
| **12** | Czy zapewniono fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez organizację od tych, które należą do innych organizacji? |   | **Wybierz poziom zgodności** |   |
| **13** | Czy dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona), bądź dostęp ten jest szczegółowo nadzorowany? |   | **Wybierz poziom zgodności** |   |
| **14** | Czy każdy pracownik otrzymuje imienny identyfikator do systemów informatycznych? |   | **Wybierz poziom zgodności** |   |
| **15** | Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowe zmiany haseł oraz zmian w razie zaistniałej potrzeby? |   | **Wybierz poziom zgodności** |   |
| **16** | Czy pracownicy zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów poprzez blokadę ekranu lub w inny równoważny sposób? |   | **Wybierz poziom zgodności** |   |
| **17** | Czy pracownicy zostali zobowiązani do niezwłocznego odbierania z drukarek wydruków zawierajacych dane osobowe lub inne poufne informacje? Czy wskazana zasada jest przestrzegana przez pracowników?  |   | **Wybierz poziom zgodności** |   |
| **18** | Czy w organizacji jest stosowana polityka tzw. „czystego biurka”? |   | **Wybierz poziom zgodności** |   |
| **19** | Czy dane osobowe gromadzone w formie papierowej, po godzinach pracy organizacji, przechowywane są w zamykanych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych? |   | **Wybierz poziom zgodności** |   |
| **20** | Czy zapewniono oprogramowanie antywirusowe na wszystkich stacjach?  |   | **Wybierz poziom zgodności** |   |
| **21** | Czy oprogramowanie posiada licencję i jest na bieżąco aktualizowane? |   | **Wybierz poziom zgodności** |   |
| **22** | Czy stosuje się szyfrowanie dysków komputerów przenośnych? |   | **Wybierz poziom zgodności** |   |
| **23** | Czy urządzenia mobilne posiadają skonfigurowaną kontrolę dostępu? |   | **Wybierz poziom zgodności** |   |
| **24** | Czy wobec urządzeń mobilnych stosuje się techniki kryptograficzne? |   | **Wybierz poziom zgodności** |   |
| **25** | Czy na urządzeniach mobilnych zainstalowano oprogramowania antywirusowe? |   | **Wybierz poziom zgodności** |   |
| **26** | Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? |   | **Wybierz poziom zgodności** |   |
| **27** | Jaki przyjęto zakres oraz częstotliwość tworzenia kopii zapasowych? |   | **Wybierz poziom zgodności** |   |
| **28** | Gdzie są przechowywane kopie zapasowe? |   | **Wybierz poziom zgodności** |   |
| **29** | Czy organizacja posiada procedury odtwarzania systemu po awarii oraz ich testowania? |   | **Wybierz poziom zgodności** |   |
| **30** | Czy organizacja wdraża nowe rozwiązania zgodnie z zasadą "privacy by design"? |   | **Wybierz poziom zgodności** |   |
| **31** | Czy organizacja działa zgodnie z zasadą "privacy by default"? |   | **Wybierz poziom zgodności** |   |
| **32** | Czy organizacja prowadzi ocenę skutków dla ochrony danych? |   | **Wybierz poziom zgodności** |   |
| **33** | Czy organizacja gwarantuje realizację praw osób, których dane dotyczą tj. m.in. prawo do przenoszenia danych, prawo do ogranizaczenia przetwarzania, prawo do bycia zapomnianym? |   | **Wybierz poziom zgodności** |   |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  | **POZIOM ZGODNOŚCI** |  |  |  |
|  |  |  |  |  |
|  | * **ZGODNOŚĆ**
* **CZĘŚCIOWA ZGODNOŚĆ**
* **NIEZGODNOŚĆ**
 |  |  |  |