Uchwała nr 1412/19

Zarządu Głównego Społecznego Towarzystwa Oświatowego

z dnia 16 marca 2019 r.

w sprawie przyjęcia Polityki bezpieczeństwa danych osobowych Społecznego Towarzystwa Oświatowego.

Zarząd Główny Społecznego Towarzystwa Oświatowego, działając na podstawie art. 29 ust. 2 pkt 3 statutu Społecznego Towarzystwa Oświatowego w związku z art. 24 i 32 rozporządzenia 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, uchwala, co następuje:

§ 1.

1. Przyjmuje się Politykę bezpieczeństwa danych osobowych Społecznego Towarzystwa Oświatowego w brzmieniu stanowiącym załącznik do niniejszej uchwały.
2. Polityka bezpieczeństwa, o której mowa w ust. 1, nie ma zastosowania do samodzielnych kół terenowych Społecznego Towarzystwa Oświatowego oraz szkół i placówek przez nie prowadzonych.

§ 2

Uchwała wchodzi w życie z dniem uchwalenia.

tel. 22 826 78 64, 22 828 88 57
fax 22 826 78 03
e-mail:biuro@sto.org.pl

00-029 Warszawa, ul. Nowy Świat 39
NIP 525-16-42-603
REGON 001391959

KRS 0000012189
Dowiedz się więcej:
www.sto.org.pl

Polityka bezpieczeństwa danych osobowych Społecznego Towarzystwa Oświatowego

1. Wstęp

Polityka bezpieczeństwa danych osobowych jest elementem porządku i organizacji pracy w STO. Naruszenie jej postanowień może być podstawą do pociągnięcia do odpowiedzialności porządkowej, cywilnej lub karnej.

O ile nie zostanie to inaczej uregulowane, postanowienia polityki bezpieczeństwa danych osobowych oraz tworzonych na jej podstawie dokumentów wykonawczych są stosowane odpowiednio w celu ochrony innych przetwarzanych w STO informacji prawnie chronionych oraz innych informacji mających istotne znaczenie dla STO.

2. Zakres

Niniejsza polityka dotyczy przetwarzania danych osobowych przez członków władz STO, pracowników i współpracowników Biura STO. Tam gdzie mowa jest o pracownikach lub współpracownikach należy rozumieć również osoby wykonujące na rzecz STO usługi na podstawie umów cywilnoprawnych, wolontariuszy, praktykantów itp.

Niniejsza polityka dotyczy przetwarzania danych osobowych w formie papierowej oraz elektronicznej - na informatycznych nośnikach danych oraz w systemach informatycznych.

Niniejsza polityka dotyczy przetwarzania danych osobowych, których administratorem jest STO, jak również przetwarzania danych osobowych powierzonych STO.

Niniejsza polityka nie ma zastosowania do przetwarzania danych osobowych w Samodzielnych Kołach Terenowych.

3. Dokumentacja systemu ochrony danych osobowych

Politykę bezpieczeństwa danych osobowych zatwierdza Zarząd Główny STO.

Inne dokumenty określające zasady przetwarzania danych osobowych przez STO, skierowane do wszystkich członków władz STO i pracowników, może zatwierdzać Prezes STO.

Dokumenty skierowane wyłącznie do pracowników Biura STO oraz dokumenty dotyczące systemów informatycznych może zatwierdzać Dyrektor Biura STO.

Dokumentację systemu ochrony danych osobowych, w tym dokumentację systemów informatycznych służących przetwarzaniu danych osobowych w STO, opracowuje, utrzymuje, udostępnia i nadzoruje Dyrektor Biura STO.

4. Podstawowe zasady przetwarzania danych osobowych

4.1 Szacowanie ryzyka i wdrażanie zabezpieczeń

Dyrektor Biura STO prowadzi i aktualizuje szacowanie ryzyka. Metodę szacowania ryzyka opracowuje Inspektor Ochrony Danych. W szacowaniu ryzyka udział bierze Dyrektor Biura STO, Inspektor Ochrony Danych, Administrator Systemów Informatycznych oraz inne osoby, stosownie do potrzeb.

Wyniki szacowania ryzyka oraz plany postępowania z ryzykiem zatwierdzają łącznie Prezes STO i Skarbnik ZG STO.

W ramach szacowania ryzyka utrzymywany jest wykaz zabezpieczeń. Dla wdrożonych zabezpieczeń zalecane jest opracowanie procedur operacyjnych oraz przypisanie odpowiedzialności za ich funkcjonowanie i monitorowanie.

Szacowanie ryzyka jest aktualizowane co najmniej raz w roku oraz po każdej istotnej zmianie w sposobie przetwarzania danych osobowych oraz po każdym naruszeniu ochrony danych osobowych.

Dyrektor Biura STO wdraża plany postępowania z ryzykiem i wymagane zabezpieczenia.

Dyrektor Biura STO odpowiada za wdrożenie, bieżące zarządzanie i nadzór nad zabezpieczeniami fizycznymi i technicznymi .

Dyrektor Biura STO odpowiada za prawidłowy przebieg procesów przetwarzania danych osobowych, za wyjątkiem ich przetwarzania przez członków władz STO, którzy przyjmują osobistą odpowiedzialność za przetwarzane przez siebie dane osobowe.

Administrator Systemów Informatycznych odpowiada za wdrożenie, bieżące zarządzanie i nadzór nad zabezpieczeniami w systemach informatycznych.

4.2 Zasady zarządzania systemami informatycznymi

Administrator Systemów Informatycznych (ASI) utrzymuje wykaz eksploatowanych systemów informatycznych.

Dla poszczególnych systemów mogą być wyznaczeni przez Dyrektora Biura STO administratorzy tych systemów. Domyślnie administratorem każdego eksploatowanego systemu jest ASI.

Administratora Systemów Informatycznych oraz administratorów systemów wyznacza Dyrektor Biura STO.

Administrator systemu utrzymuje wykaz haseł administracyjnych niezbędnych do zarządzania systemem. Hasła administracyjne deponuje u dyrektora Biura STO po każdej ich zmianie.

Administrator systemu zarządza kontami i uprawnieniami użytkowników w systemie. Konta i uprawnienia nadaje, zmienia i odbiera na wniosek Dyrektora Biura STO lub Prezesa STO

przekazany pocztą elektroniczną. Administrator systemu utrzymuje ewidencję użytkowników systemu.

Przy nadawaniu uprawnień stosuje się zasadę minimalizacji uprawnień. Przy zakładaniu kont stosuje się zasadę imiennych kont.

Zasady bezpiecznego korzystania z systemów informatycznych są przedstawione w *Regulaminie bezpieczeństwa danych osobowych*.

Szczegółowe zasady zarządzania systemami informatycznymi mogą być określone w dokumentach wykonawczych: instrukcjach, procedurach lub wytycznych.

4.3 Zasady przetwarzania danych osobowych

4.3.1 Upoważnienia i uprawnienia

Członkowie władz STO (członkowie Zarządu Głównego, Głównej Komisji Rewizyjnej, Sądu Koleżeńskiego oraz Rzecznik Dyscyplinarny) są upoważnieni do przetwarzania danych osobowych we wszystkich zbiorach, w okresie pełnienia funkcji, z zachowaniem zasad wynikających z powszechnie obowiązujących przepisów oraz dokumentacji systemu ochrony danych osobowych w STO.

Dyrektor Biura STO jest upoważniony do przetwarzania danych osobowych we wszystkich zbiorach danych osobowych oraz do wydawania i odbioru w imieniu administratora danych upoważnień do przetwarzania danych osobowych.

Dyrektor Biura STO prowadzi ewidencję upoważnień. W ewidencji uwzględnia się osoby, których upoważnienie wynika z niniejszej polityki.

O każdej zmianie tj. wydaniu, odebraniu lub zmianie zakresu upoważnienia Dyrektor Biura STO informuje pocztą elektroniczną członków Zarządu Głównego, pozostałych pracowników oraz Administratora Systemów Informatycznych, Inspektora Ochrony Danych i – o ile to konieczne – innych administratorów systemów.

Administratorzy systemów niezwłocznie wprowadzają zmiany w nadanych uprawnieniach wynikające z nadania, odbioru lub zmiany zakresu upoważnienia.

4.3.2 Rejestrowanie czynności przetwarzania

Inspektor Ochrony Danych prowadzi *Rejestr czynności przetwarzania* oraz *Rejestr kategorii czynności przetwarzania*.

Wszelkie nowe czynności przetwarzania danych osobowych oraz wszelkie zmiany w już prowadzonych czynnościach przetwarzania danych osobowych muszą być uzgodnione z Dyrektorem Biura STO oraz z Inspektorem Ochrony Danych.

Inspektor Ochrony Danych prowadzi również inne rejestry i wykazy niezbędne do spełnienia zasady rozliczalności lub nadzoruje ich prowadzenie przez inne, wyznaczone przez Dyrektora Biura STO osoby.

4.3.3 Polecenie przetwarzania

Pracownicy posiadający upoważnienie mogą przetwarzać dane osobowe tylko w zakresie tego upoważnienia oraz tylko na podstawie wydane polecenia przetwarzania.

Poleceniem przetwarzania jest m.in. umieszczenie pracownika (lub jego komórki organizacyjnej, stanowiska lub funkcji) w rejestrze czynności przetwarzania (rejestrze kategorii czynności przetwarzania) lub wpisanie czynności przetwarzania danych do zakresu obowiązków lub każde inne polecenie wydane przez administratora danych lub przełożonego, do wykonania którego niezbędne jest przetwarzanie danych osobowych.

4.3.4 Zbieranie danych i klauzule informacyjne

Wszelkie nowe czynności zbierania danych osobowych oraz wszelkie zmiany w już prowadzonych czynnościach zbierania danych osobowych muszą być uzgodnione z Dyrektorem Biura STO oraz z Inspektorem Ochrony Danych.

Przy projektowaniu tych czynności należy wziąć pod uwagę zasady określone w RODO (m.in. zasadę legalności, minimalizacji danych, ograniczenia czasu przechowywania, domyślnej ochrony, rozliczalności).

Należy również rozważyć i – o ile to praktyczne - udokumentować co najmniej sposób implementacji procedur obsługi żądań realizacji praw osób, których dane dotyczą oraz sposób implementacji procedur usuwania danych.

Wszelkie zmiany w stosowanych klauzulach informacyjnych zatwierdza Dyrektor Biura STO po konsultacji z Inspektorem Ochrony Danych. Wzorcowe oraz aktualnie obowiązujące klauzule udostępnia Dyrektor Biura STO.

Przed pozyskaniem nowych danych osobowych bezpośrednio od osoby, której dotyczą, pracownik pozyskujący te dane zobowiązany jest zapoznać tę osobę z właściwą klauzulą informacyjną lub umożliwić zapoznanie się z tą klauzulą.

W przypadku gdy dane są pozyskiwane ze źródła innego niż osoba, której dotyczą, konieczne jest powiadomienie tej osoby o przetwarzaniu jej danych zgodnie z art. 14 RODO – jeżeli sposób powiadomienia nie jest określony w *Rejestrze czynności przetwarzania* lub *Rejestrze kategorii czynności* przetwarzania wówczas należy skontaktować się niezwłocznie z Inspektorem Ochrony Danych w celu ustalenia szczegółów postępowania.

4.3.5 Powierzanie przetwarzania danych osobowych

Umowy powierzenia przetwarzania danych osobowych muszą być skonsultowane z Inspektorem Ochrony Danych lub muszą być oparte na wzorcowych umowach przygotowanych przez Inspektora Ochrony Danych.

Za zidentyfikowanie potrzeby zawarcia umowy powierzenia oraz doprowadzenie do jej zawarcia odpowiedzialny jest Dyrektor Biura STO.

Nadzór nad wykonaniem umów powierzenia przetwarzania danych prowadzi Inspektor Ochrony Danych.

4.3.6 Obsługa żądań realizacji uprawnień

Wszystkie otrzymane żądania realizacji uprawnień określonych w RODO w art. 15-21 muszą być przekazane Inspektorowi Ochrony Danych, chyba że sposób ich realizacji jest określony w obowiązujących w STO dokumentach a tożsamość osoby wnoszącej żądanie nie budzi wątpliwości.

Inspektor Ochrony Danych przedstawia Dyrektorowi Biura STO proponowany sposób realizacji żądania. Dyrektor Biura STO zatwierdza i wdraża postępowanie służące realizacji żądania, o ile jest ono zasadne. Inspektor Ochrony Danych może prowadzić korespondencję z osobą, która złożyła żądanie.

Inspektor Ochrony Danych prowadzi rejestr otrzymanych żądań realizacji uprawnień.

4.3.7 Obsługa udostępnień

Udostępnienia podmiotom wskazanym w *Rejestrze czynności przetwarzania* lub *Rejestrze kategorii czynności przetwarzania* mogą być zrealizowane pod warunkiem ich odnotowania w sposób określony w odpowiednim *Rejestrze*. Wszystkie inne udostępnienia wymagają zgody Dyrektora Biura STO oraz powiadomienia Inspektora Ochrony Danych.

Wszelkie przekazania poza EOG wymagają zgody Dyrektora Biura STO oraz powiadomienia IOD.

4.3.8 Obsługa naruszeń ochrony danych osobowych

Każda stwierdzona sytuacja lub zdarzenie, którego skutkiem jest lub może być naruszenie ochrony danych osobowych musi być niezwłocznie zgłoszone Dyrektorowi Biura STO oraz Inspektorowi Ochrony Danych, który dokonuje oceny ryzyka naruszenia praw i wolności osób fizycznych.

Dyrektor Biura STO, w razie potrzeby po konsultacji z Inspektorem Ochrony Danych i Administratorem Systemów Informatycznych, klasyfikuje zgłoszoną sytuację lub zdarzenie jako incydent i podejmuje działania służące wyjaśnieniu przyczyn i skutków incydentu oraz ograniczające jego skutki i eliminujące przyczyny (działania naprawcze, korygujące i zapobiegawcze).

Jeżeli incydent dotyczy danych osobowych Inspektor Ochrony Danych dokonuje oceny czy doszło do naruszenia ochrony danych osobowych i jakie jest ryzyko naruszenia praw lub wolności osób fizycznych a następnie przedkłada Dyrektorowi Biura STO i Prezesowi STO stanowisko dot. zgłoszenia incydentu organowi nadzorczemu lub powiadomienia osób, dotkniętych incydentem oraz przygotowuje, we współpracy z Dyrektorem Biura STO, wymagane w zgłoszeniu lub powiadomieniu informacje.

Inspektor Ochrony Danych prowadzi dokumentację naruszeń ochrony danych osobowych.

Administrator Systemów Informatycznych prowadzi dokumentację incydentów dot. systemów informatycznych.

Po wyjaśnieniu przyczyn incydenty w razie potrzeby aktualizowane jest szacowanie ryzyka.

4.4 Szkolenia i audyty

Przed dopuszczeniem do pracy lub wykonywania obowiązków członkowie władz oraz pracownicy i współpracownicy STO zobowiązani są zapoznać się z dokumentacją systemu ochrony danych osobowych i zobowiązać do jej przestrzegania.

Szkolenia z zasad ochrony danych osobowych prowadzi co najmniej raz na 2 lata Inspektor Ochrony Danych Osobowych.

Dyrektor Biura STO prowadzi bieżący nadzór nad prawidłowym przebiegiem procesów przetwarzania danych osobowych i funkcjonowaniem zabezpieczeń fizycznych i technicznych. Administrator Systemów Informatycznych oraz każdy administrator systemu prowadzą bieżący nadzór nad bezpieczeństwem systemów informatycznych.

Inspektor Ochrony Danych monitoruje przestrzeganie zasad przetwarzania i ochrony danych osobowych oraz przeprowadza audyty.