POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W I LICEUM OGÓLNOKSZTAŁCĄCYM IM. ADAMA ASNYKA W KALISZU

Polityka bezpieczeństwa to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz I LO. Jest ona częścią dokumentacji danych osobowych, z której wstępem należy się zapoznać przed przeczytaniem niniejszego dokumentu.

Dokument ten odnosi się całościowo do problemu zabezpieczenia danych osobowych w I LO tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych. Wskazuje działania, jakie należy wykonać oraz ustanawia zasady i reguły postępowania, które należy stosować, aby właściwie zabezpieczyć dane osobowe.

1. OŚWIADCZENIE O INTENCJACH KIEROWNICTWA

W celu realizacji postanowień dokumentacji ochrony danych osobowych Dyrektor I LO dołoży wszelkich starań i zapewni:

- niezbędne środki finansowe, prawidłowe wyposażenie i zabezpieczenie stanowisk i narzędzi pracy;
- odpowiedni poziom procedur, konieczne szkolenia pracowników, uświadamianie w dziedzinie bezpieczeństwa informacji;
- odpowiednie zabezpieczenia pomieszczeń i systemu informatycznego.

Zasady i standardy określone w dokumentacji muszą być stosowane przez wszystkich pracowników I LO (również osoby nie mające bezpośredniego dostępu do danych jak np. osoby pilnujące porządku, sprzątające), dlatego każdy pracownik zobligowany jest do zapoznania się z dokumentacją i bezwzględne przestrzeganie zasad w niej zawartych.

Mając świadomość, iż żadne zabezpieczenie techniczne nie gwarantuje 100%-towej szczelności systemu konieczne jest, aby każdy pracownik był pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z błędów ludzkich.

W przypadku naruszenia bezpieczeństwa informacji stosuje się procedury postępowania stworzone dla takiej sytuacji, a pracownicy ponoszą odpowiedzialność dyscyplinarną i prawną wynikającą z przepisów prawa, Kodeksu Cywilnego oraz Kodeksu Pracy.

2. ANALIZY, REJESTRY I EWIDENCJE PROWADZONE PRZEZ ADO

W celu odpowiedniego zabezpieczenia i rozliczalności ochrony danych osobowych prowadzi się w formie papierowej lub elektronicznej:

- rejestr czynności przetwarzania danych osobowych oraz analizę ryzyka;
- rejestr naruszeń ochrony danych osobowych;
- ewidencję osób upoważnionych do przetwarzania danych osobowych;
- ewidencję zapoznania się z niniejszą dokumentacją;
- ewidencję dostępów do systemów informatycznych;
- ewidencję podmiotów przetwarzających powierzone dane osobowe.

ADO może wyznaczyć osobę odpowiedzialną za prowadzenie poszczególnych rejestrów i ewidencji.

ADO na bieżąco analizuje ocenę skutków dla ochrony danych, ocenę ryzyka naruszenia praw i wolności osoby fizycznej oraz zabezpieczenia związane z ochroną danych osobowych zbiorów tradycyjnych i systemów informatycznych.

3. OKREŚLENIE ŚRODKÓW ORGANIZACYJNYCH

W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, wprowadza się następujące środki organizacyjne:

- urządzenia w systemie informatycznym I LO są połączone do sieci publicznej, w związku z tym ADO stosuje środki bezpieczeństwa na poziomie wysokim;
- przetwarzanie danych osobowych może odbywać się wyłącznie w ramach wykonywania zadań służbowych;
- zakres uprawnień do przetwarzania danych osobowych wynika z zakresu zadań służbowych;
- do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie, natomiast osoby przebywające w pomieszczeniach gdzie przetwarzane są dane osobowe, powinny mieć na to zgodę; podpisane upoważnienie lub zgoda dołączane jest do akt osobowych; wzór upoważnienia i zgody stanowią załączniki nr 1 i 2 do niniejszej dokumentacji; wydanie nowego upoważnienia/zgody unieważnia automatycznie poprzednio wydane; ADO może wprowadzić zarządzeniem ważność upoważnień wydanych do czasu wprowadzenia aktualnej dokumentacji;
- każdy pracownik podpisuje oświadczenie o zobowiązaniu się do zachowania poufności; wzór oświadczenia stanowi załącznik nr 3 do niniejszej dokumentacji; ADO może wprowadzić zarządzeniem ważność oświadczeń podpisanych do czasu wprowadzenia aktualnej dokumentacji;
- prowadzona jest ewidencja osób upoważnionych do przetwarzania danych oraz mających zgodę na przybywanie w miejscu przetwarzania danych;
- prowadzona jest ewidencja zapoznania się osób upoważnionych z niniejszą dokumentacją;
- obszar przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych; klucze do pomieszczeń przechowywane i wydawane są zgodnie z instrukcją przechowywania i wydawania kluczy;
- przebywanie osób nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą ADO lub w obecności osoby upoważnionej do przetwarzania danych osobowych;
- przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach;
- pomieszczenia w których przetwarza się dane osobowe zamykane są na klucz;
- zabrania się gromadzenia lub tworzenia odrębnych zbiorów danych osobowych poza zbiorami zgodnie z prowadzonym rejestrem czynności przetwarzania - w szczególności w podręcznej dokumentacji;
- wszelkie podręczne wydruki lub zestawienia, w których występują dane osobowe powinny być zminimalizowane do niezbędnych informacji, a po użyciu trwale zniszczone lub zanonimizowane (usunięte dane osobowe jak np. pesel, adres);
- niepotrzebne dokumenty lub dokumenty po ustaniu ich przydatności zawierające dane osobowe powinny być niszczone w sposób uniemożliwiający ich odczytanie;
- monitory komputerów, na których przetwarzane są dane osobowe powinny być ustawione w sposób uniemożliwiający odczytanie tych danych osobom trzecim;
- wszelki dostęp do danych osobowych zapisanych elektronicznie oraz dostęp do systemów komputerowych powinien odbywać się poprzez logowanie z użyciem osobistych loginów i haseł;
- zbiory danych osobowych przechowywane elektronicznie powinny być zabezpieczone poprzez regularne wykonywanie kopii bezpieczeństwa;
- wszelkie dokumenty elektroniczne zawierające dane osobowe, które są wynoszone lub przesyłane poza obszar przetwarzania danych powinny być zabezpieczone hasłem odczytu lub zaszyfrowane;
- szczegółowe zasady postępowania ze zbiorami przetwarzanymi elektronicznie określa Instrukcja Zarządzania Systemem Informatycznym, która jest częścią dokumentacji;
- zasady korzystania z komputerów służbowych oraz z zasobów informatycznych, w tym sieci internet określa odrębny regulamin korzystania z zasobów informatycznych I LO;

4. OKREŚLENIE ŚRODKÓW TECHNICZNYCH

Środki techniczne niezbędne dla zapewnienia poufności, bezpieczeństwa, integralności, rozliczalności i niezawodności przetwarzanych danych:

- budynek I LO zabezpieczony jest alarmem oraz monitoringiem wizyjnym; całodobowy dozór ochrony pełni zewnętrzna firma ochroniarska;
- budynek wyposażony jest w wolnostojące gaśnice przeciwpożarowe, które powinny być w miejscach ogólnie dostępnych, w szczególności w miejscach w których przechowywane są dane osobowe;
- obszary przechowywania i przetwarzania danych zabezpiecza się przed fizycznym dostępem poprzez zamki w drzwiach, a także przestrzeganie procedur spraw porządkowych oraz postępowania z kluczami;s
- komputery na których przetwarza się dane osobowe zaopatrzone są w licencjonowane programy i okresowo sprawdzane pod kątem poprawności ich instalacji i aktualizacji;
- system informatyczny zabezpieczony jest poprzez nadanie haseł uprawnionym użytkownikom a także poprzez sporządzanie kopii bezpieczeństwa danych na nośnikach magnetycznych i optycznych oraz wydrukach komputerowych;
- zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego;
- wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbiorów danych osobowych;
- system informatyczny zabezpieczony jest oprogramowaniem antywirusowym zarządzanym centralnie, umożliwiającym w łatwy sposób diagnozowanie poprawności aktualizacji oraz występujących problemów;
- zastosowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe;
- komputery, które służą do przechowywania i przetwarzania danych osobowych, za wyjątkiem komputerów służących przede wszystkim do odczytu powinny być zabezpieczone w urządzenia podtrzymujące napięcie na wypadek braku zasilania;
- dostęp z sieci publicznej do sieci wewnętrznej zabezpieczony jest systemem typu firewall na głównym urządzeniu dostępowym z sieci publicznej w celu ochrony zagrożeń z zewnątrz, próby nieuprawnionego dostępu są logowane;
- dostęp z sieci do komputerów lokalnych zabezpieczony jest oprogramowaniem typu firewall;
- zbiory danych w postaci tradycyjnej umieszczane są w szafach zamykanych na klucz;
- zbiory danych w postaci tradycyjnej, zawierające dane osobowe mające istotne znaczenie dla ochrony danych osoby fizycznej umieszczane są w szafach metalowych lub sejfach;
- archiwalne bazy danych znajdują się w składnicy akt szkoły; klucze do składnicy akt posiadają uprawnieni pracownicy.

5. POLITYKA PRYWATNOŚCI NA STRONIE INTERNETOWEJ I LO

W celu zapewnienia bezpieczeństwa danych osobowych osób korzystających z serwisów internetowych I LO, stworzona została polityka prywatności.

Polityka prywatności jest zamieszczona na stronach www placówki.

6. ZASADY POSTĘPOWANIA PRZY PRZETWARZANIU DANYCH OSOBOWYCH

Każdy pracownik działający z upoważnienia administratora i mający dostęp do danych osobowych przetwarza je wyłącznie na polecenie administratora i w zakresie jaki został wskazany w upoważnieniu.

Osoby upoważnione zobowiązane są do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczeń. Obowiązek ten istnieje również po ustaniu stosunku pracy.

Każdy pracownik, który dokonuje czynności związane z przetwarzaniem danych osobowych zobligowany jest stosować się do niniejszej dokumentacji oraz ponosi odpowiedzialność za bezpieczeństwo przetwarzania danych osobowych.

Wynoszenie poza placówkę dokumentów zawierających dane osobowe w formie papierowej oraz cyfrowej jest surowo zabronione z wykluczeniem sytuacji związanych z wykonywaniem czynności służbowych oraz zastosowaniem odpowiednich zabezpieczeń.

Pracownik korzystający z systemu informatycznego zobowiązany jest do przestrzegania Instrukcji Zarządzania Systemem Informatycznym, która jest częścią niniejszej dokumentacji oraz wskazówek zawartych w instrukcji obsługi urządzeń, oprogramowania i nośników.

7. PROCEDURY PRZEKAZYWANIA DANYCH PODMIOTOM TRZECIM

Administrator Danych może przekazywać w szczególnych przypadkach przetwarzanie danych osobowych zewnętrznym podmiotom, instytucjom, organizacjom, placówkom tylko i wyłącznie w konkretnym i sprecyzowanym celu oraz na podstawie przepisów prawa, które umożliwia przetwarzanie danych osobowych w tym celu.

ADO może korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi przepisów prawa i chroniło prawa osób, których dane dotyczą.

Powierzenie danych musi być potwierdzone umową powierzenia, która zawiera cel przekazania, zakres danych, kategorię osób oraz czas planowanego przetwarzania danych przez podmiot przetwarzający.

ADO prowadzi rejestr podmiotów, którym powierzył przetwarzanie danych.

8. ZAPEWNIENIE DOKUMENTACJI I CIĄGŁOŚCI DOSKONALENIA ZABEZPIECZEŃ

Mając na uwadze złożoność problemu stosowania zabezpieczeń ADO dołoży wszelkich starań aby należycie wykonać zadania związane z ochroną danych osobowych.

Najważniejsze czynniki wpływające na złożoność problemu to:

- asymetria działań mających na celu zabezpieczenie systemu - polega ona tym, że aby skutecznie zabezpieczyć system należy usunąć wszystkie słabości, podczas gdy wystarczy znaleźć jedną, aby skutecznie system został zaatakowany;
- zależność od otoczenia - wpływ całego otoczenia systemu i środowiska informatycznego na bezpieczeństwo, w którym dany system/program przetwarzania danych funkcjonuje;
- ciągłość działania - wymóg permanentnego monitorowania i aktualizowania zastosowanych środków bezpieczeństwa. Jakakolwiek zmiana struktury systemu czy też dodanie nowych usług każdorazowo wymaga jego weryfikacji pod względem zagrożeń i ryzyka, na jakie

przetwarzane dane mogą być narażone i tym samym - weryfikacji zastosowanych środków bezpieczeństwa.

9. ZADANIA INSPEKTORA OCHRONY DANYCH

Zgodnie z przepisami prawa ADO powinien powołać Inspektora Ochrony Danych. Do głównych zadań IOD należy:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów prawa oraz wewnętrznych procedur;
- doradzanie i szkolenia pracowników w zakresie upowszechniania i doskonalenia wiedzy z zakresu ochrony danych osobowych;
- monitorowanie przestrzegania przepisów prawa oraz wewnętrznych procedur w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
- współpraca z organem nadzorczym;
- nadzorowanie opracowania i aktualizowania dokumentacji ochrony danych;
- pomoc w prowadzeniu rejestru czynności przetwarzania danych osobowych oraz innych rejestrów i ewidencji;
- monitorowanie działań i skuteczności zabezpieczeń wdrożonych w celu ochrony danych osobowych.

10. ZADANIA ADMINISTRATORA SYSTEMU INFORMATYCZEGO

ADO może powołać Administratora Systemu Informatycznego. W takim przypadku do jego głównych zadań należy m.in.:

- zarządzanie systemem infomatycznym przetwarzającym dane;
- opracowywanie wykazu użytkowanego oprogramowania, jego konserwacja oraz uaktualnianie;
- prowadzenie monitoringu przetwarzania danych osobowych;
- nadawanie uprawnień użytkowników i prowadzenie aktualnego rejestru;
- kontrola mechanizmów uwierzytelnienia użytkowników;
- kontrola wykonywania kopii bezpieczeństwa;
- kontrola systemu antywirusowego i firewall;
- informowanie Administratora danych o wszelkich próbach złamania zabezpieczeń, awariach programów czy niewłaściwego wykorzystania sprzętu.

W przypadku niepowołania Administratora Systemu Informatycznego, powyższe zadania odwołują się do Administratora Danych Osobowych.

11. POSTĘPOWANIE W PRZYPADKU NARUSZENIA ZASAD BEZPIECZEŃSTWA

Użytkownik zobowiązany jest do niezwłocznego powiadamiania bezpośredniego przełożonego, ASI, ADO lub IOD o wszelkich wykrytych lub podejrzewanych słabościach systemu, zagrożeniach z nimi związanych oraz o wszelkich innych incydentach, a w szczególności:

- stwierdzenia włamania i/lub kradzieży sprzętu lub nośników zawierających dane;

- stwierdzenia zaginięcia nośnika zawierającego dane (wydruku, kopii bezpieczeństwa, itp.);
- stwierdzenia lub podejrzenia nieuprawnionego dostępu do pomieszczeń, gdzie są przetwarzane dane lub do systemu informatycznego;
- stwierdzenia nieuzasadnionej modyfikacji, utraty danych lub niezgodności w danych (np. utraty plików na dysku komputera, braku lub nadmiaru danych);
- znalezienia poza pomieszczeniami przetwarzania wszelkich dokumentów, wydruków, dyskietek i innych nośników danych;
- przesłania danych lub informacji dotyczących danych lub polityki bezpieczeństwa do niewłaściwego miejsca lub adresata;
- wszelkich awarii systemu informatycznego (sprzętu lub oprogramowania);
- nietypowego działania systemu informatycznego, np. braku połączenia szyfrowanego przy uwierzytelnianiu się przez przeglądarkę internetową;
- nietypowych komunikatów wyświetlanych na ekranie monitora;
- obecności podejrzanych plików w poczcie elektronicznej;
- obecności podejrzanych urządzeń w pobliżu komputera, np. kamer, mikrofonów, urządzeń wpiętych w porty usb;
- wykrycia wirusa w systemie.

Po stwierdzeniu wystąpienia lub podejrzeniu wystąpienia incydentu naruszenia bezpieczeństwa informacji użytkownik powinien:

- niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców;
- rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia;
- zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę;
- powstrzymać się od wszelkich czynności w pomieszczeniu przetwarzania mogących zatrzeć ślady naruszenia bezpieczeństwa informacji;
- zastosować się do poleceń ADO, IOD lub ASI;
- zwrócić uwagę, aby nie porzucać, wyrzucać do śmieci, niszczyć lub sprawdzać zawartości znalezionych nośników danych;
- sporządzić notatkę o zdarzeniu i przekazać ją ASO lub IOD.

Użytkownik posiadający tylko informacje mogące mieć wpływ na bezpieczeństwo danych osobowych również zobowiązany jest niezwłocznie zgłosić ten fakt ADO lub IOD.

ADO wraz z IOD po zgłoszeniu naruszenia zasad bezpieczeństwa lub incydentu dokonuje:

- analizy sytuacji oraz konsekwencji naruszenia dóbr osobistych osób fizycznych, których dotyczy naruszenie;
- podejmuje odpowiednie kroki zabezpieczające dane osobowe oraz minimalizujące negatywne skutki naruszenia dóbr osobistych osób fizycznych, których dotyczy naruszenie;
- w przypadku poważnego naruszenia dokonuje oceny konieczności powiadomienia osób fizycznych których dane dotyczą oraz Prezesa Urzędu Ochrony Danych o fakcie i zakresie naruszenia przepisów;
- udokumentowuje zaistniały przypadek i sporządza raport.

Po sporządzeniu raportu IOD przygotowuje dokument procesów naprawczych, określa możliwości techniczne związane z ewentualnym odtworzeniem danych z kopii zapasowych, jak również zarządza w jakim terminie nastąpi wznowienie procesu przetwarzania danych.

Za incydentalne naruszenie przepisów o ochronie danych osobowych uznaje się pojedyncze zdarzenie lub serię niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań placówki i zagrażają bezpieczeństwu informacji, czyli:

- nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł itd.);
- niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
- nieodpowiednie zabezpieczenie sprzętu IT czy oprogramowania przed wyciekiem lub utratą danych osobowych.

Za wysokie naruszenie przepisów o ochronie danych osobowych uznaje się takie naruszenie, które ma związek z naruszeniem dóbr osobistych, które są pod ochroną prawa cywilnego, w szczególności: zdrowie, wolność, swoboda sumienia, dane personalne, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska oraz dotyczy wielu osób.