Zarządzenie nr 10
Rzecznika Praw Dziecka
z dnia 18 maja 2018 roku

w sprawie polityki bezpieczeństwa informacji
w Biurze Rzecznika Praw Dziecka

W związku z § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247) oraz w oparciu o § 8 Statutu Biura Rzecznika Praw Dziecka zarządza się, co następuje:

§ 1

Wprowadza się „Politykę bezpieczeństwa informacji w Biurze Rzecznika Praw Dziecka", stanowiącą Załącznik do zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

Grażyna Mazicka-Gołębiewska
RADCA PRAWNY

POLITYKA BEZPIECZEŃSTWA INFORMACJI

W BIURZE RZECZNIKA PRAW DZIECKA

Spis treści

1. Wstęp

Rzecznik Praw Dziecka stoi na straży praw dziecka, a w szczególności:

- prawa do życia i ochrony zdrowia,
- prawa do wychowania w rodzinie,
- prawa do godziwych warunków socjalnych.

Rzecznik Praw Dziecka wykonując swoje uprawnienia, kieruje się zasadami zawartymi w Konstytucji RP, Konwencji o Prawach Dziecka i ustawie o Rzeczniku Praw Dziecka, w tym zwłaszcza:

- zasadą dobra dziecka,
- wszystkie działania podejmowane są w najlepiej pojętym interesie dziecka,
- zasadą równości,
- troską o ochronę praw każdego dziecka,
- zasadą poszanowania odpowiedzialności, praw i obowiązków obojga rodziców za rozwój i wychowanie dziecka,
- prawa do nauki.

Realizacja misji Rzecznika Praw Dziecka i podejmowanych działań w wielu obszarach wymaga, między innymi, efektywnego dostępu do informacji oraz zapewnienia bezpieczeństwa zasobów informacyjnych.

Biuro Rzecznika Praw Dziecka (BRPD/Biuro) zapewnia wykonywanie ustawowo określonych zadań Rzecznika Praw Dziecka (RPD).

2. Słownik pojęć:

- **bezpieczeństwo informacji** - zachowanie poufności, integralności, dostępności. Dodatkowo można brać pod uwagę inne właściwości, takie jak: autentyczność, rozliczalność, niezaprzeczalność, niezawodność (na podstawie PN-ISO/IEC 27000:2014),
- **autentyczność** - właściwość polegająca na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie jak deklarowane (na podstawie PN-ISO/IEC 27000:2014),
- **dostępność** - właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu (na podstawie PN-ISO/IEC 27000:2014),
- **integralność** - właściwość polegająca na zapewnieniu dokładności i kompletności (na podstawie PN-ISO/IEC 27000:2014),
- **niezaprzeczalność** - zdolność do udowodnienia, że wystąpiły deklarowane zdarzenia lub działania oraz, że wywołał je dany podmiot (na podstawie PN-ISO/IEC 27000:2014),
- **niezawodność** - właściwość oznaczająca spójne, zamierzone zachowanie i skutki (na podstawie PN-ISO/IEC 27000:2014),
- **poufność** - właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom (na podstawie PN-ISO/IEC 27000:2014),

- **incydent związany z bezpieczeństwem informacji** - pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji (na podstawie PN-ISO/IEC 27000:2014),
- **ryzyko** - wpływ niepewności na cele (na podstawie PN-ISO/IEC 27000:2014),
- **aktyw/zasób** - wszystko to, co ma wartość dla organizacji w zakresie informacji (zarówno informacje, jak i środki techniczne oraz organizacyjne do ich przetwarzania).

3. Wymagania prawne dotyczące bezpieczeństwa informacji

Podstawą prawną dla Polityki bezpieczeństwa informacji w Biurze Rzecznika Praw Dziecka (dalej: Polityki) oraz dokumentów szczegółowych z niej wynikających są w szczególności:

- ustawa z dnia 6 stycznia 2000 r. o Rzeczniku Praw Dziecka (Dz. U. z 2017 r. poz. 922),
- ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412),
- ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922),
- ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2016 r. poz. 1764),
- ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570).

Do tworzenia i rozwijania Polityki są stosowane odpowiednie normy i standardy, w szczególności Polska Norma PN-ISO/IEC 27001.

Polityka będzie aktualizowana w przypadku zmiany powszechnie obowiązujących przepisów związanych z polityką bezpieczeństwa informacji.

4. Zagrożenia bezpieczeństwa informacji i systemów teleinformatycznych

Źródła zagrożeń bezpieczeństwa informacji i systemów informatycznych:

- siła wyższa,
- uchybienia organizacyjne,
- błędy ludzkie,
- działania rozmyślne.

5. Cel i zakres polityki bezpieczeństwa informacji

Celem strategicznym Polityki jest osiągnięcie akceptowanego poziomu bezpieczeństwa zasobów informacyjnych BRPD.

Zadaniem Polityki jest zmniejszenie ryzyka płynącego z zagrożeń do akceptowalnego poziomu, to znaczy:

- zapobieganie przypadkom naruszenia bezpieczeństwa zasobów informacyjnych w BRPD,
- zminimalizowanie możliwości takiego naruszenia bezpieczeństwa,
- umożliwienie wczesnego jego wykrycia,
- zminimalizowanie strat związanych z takim naruszeniem oraz sprawne usunięcie jego skutków.

Politykę są obowiązani stosować:

- wszyscy pracownicy Biura,
- stażyści, praktykanci i wolontariusze,
- pracownicy i przedstawiciele podmiotów zewnętrznych pośrednio lub bezpośrednio świadczących usługi dla Biura, którzy mają pośredni lub bezpośredni dostęp do zasobów informacyjnych BRPD.

Polityka ma zastosowanie do wszystkich informacji będących w dyspozycji BRPD, a które są:

- przechowywane w bazach danych,
- przechowywane na komputerach, przekazywane przez sieci wewnętrzne i publiczne,
- przechowywane na nośnikach elektronicznych,
- drukowane lub pisane odręcznie,
- prezentowane z wykorzystaniem mediów audiowizualnych,
- przekazywane ustnie podczas rozmów telefonicznych, spotkań,
- przesyłane faksem lub z użyciem innych środków komunikacji.

Z treścią Polityki, zapoznaje się wszystkich pracowników Biura i inne osoby mające dostęp do informacji przetwarzanych w Biurze (zgodnie z zasadą wiedzy koniecznej), przed przystąpieniem do przetwarzania danych/informacji.

Polityka może być przedstawiana do wiadomości podmiotom, z którymi BRPD jest związane umowami lub innym jednostkom współpracującym.

Niniejszy dokument jest dokumentem nadrzędnym nad pozostałymi politykami, instrukcjami, regulaminami i procedurami określającymi szczegółowo obszary bezpieczeństwa informacji w BRPD.

Dokumentacja polityki bezpieczeństwa powinna być przeglądana i weryfikowana:

- na polecenie Rzecznika Praw Dziecka lub Dyrektora Biura,
- w przypadku wejścia w życie nowych przepisów dotyczących bezpieczeństwa informacji,
- w przypadku wystąpienia poważnych incydentów związanych z bezpieczeństwem informacji,
- w celu realizacji zaleceń wynikających z przeprowadzonych audytów i kontroli,
- w przypadku poważnych modyfikacji systemu teleinformatycznego Biura,
- okresowo, nie rzadziej niż raz do roku.

6. Deklaracja Rzecznika Praw Dziecka

Polityka wyznacza kierunek działania pracowników Biura w celu zapewnienia systemowego nadzoru nad gromadzeniem, przetwarzaniem, przechowywaniem i udostępnianiem informacji, niezależnie od sposobu realizacji tych procesów.

Rzecznik Praw Dziecka zapewnia bezpieczeństwo zasobów oraz informacji zawartych w systemach informacyjnych Biura i poza nimi, w sposób opisany w zarządzeniach, postanowieniach, wytycznych i poleceniach, ponieważ mają one fundamentalne znaczenie dla realizacji misji i celów BRPD.

Polityka wyraża wolę Rzecznika Praw Dziecka w zakresie ochrony zasobów informacji w BRPD.

Rzecznik Praw Dziecka oraz Dyrektor Biura aktywnie wspierają procesy zmierzające do

zapewnienia bezpieczeństwa przetwarzania informacji poprzez wdrażanie, rozwój, uaktualnianie Polityki oraz regulacji z niej wynikających.

7. Klasyfikacja informacji

W oparciu o wymagania prawne w BRPD obowiązuje następująca klasyfikacja informacji:

1) informacje niejawne - w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych,
2) dane osobowe - w rozumieniu ustawy z dnia 6 stycznia 2000 r. o Rzeczniku Praw Dziecka oraz ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
3) informacje objęte tajemnicą przedsiębiorstwa uzyskane przez BRPD w związku z wykonywaniem zadań publicznych,
4) informacje wewnętrzne (jawne) nie wchodzące w zakres, o którym mowa w pkt 1-3,
5) informacje publiczne - w rozumieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej oraz ustawy z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2016 r. poz. 352, z późn. zm.).

Informacje niejawne

Informacje niejawne są przetwarzane i chronione zgodnie z przepisami ustawy o ochronie informacji niejawnych.

Dane osobowe

Dane osobowe są przetwarzane i chronione zgodnie z przepisami ustawy o ochronie danych osobowych.

Należy postępować zgodnie z:

- „Polityką bezpieczeństwa ochrony danych osobowych w BRPD",
- „Instrukcją zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w BRPD".

Informacje objęte tajemnicą przedsiębiorstwa uzyskane w związku z wykonywaniem zadań publicznych przetwarzane i chronione są zgodnie z ustawą o Rzeczniku Praw Dziecka oraz obowiązującymi przepisami prawa i zawartymi umowami.

Informacje wewnętrzne

Informacje dotyczące działalności BRPD przeznaczone wyłącznie do użytku wewnętrznego są przetwarzane i chronione zgodnie z „Instrukcją Kancelaryjną BRPD".

Informacje publiczne

Ochrona informacji publicznych realizuje wymagania ustawy o dostępie do informacji publicznej oraz ustawy o ponownym wykorzystywaniu informacji sektora publicznego.

Odpowiedzialność za bezpieczeństwo informacji w BRPD ponoszą wszyscy pracownicy. Odpowiedzialność za realizację bezpieczeństwa informacji musi być jasno określona, z przypisaniem osób odpowiedzialnych.

Każdy pracownik BRPD jest zapoznawany z zasadami bezpieczeństwa oraz z aktualnymi procedurami ochrony informacji w swojej komórce organizacyjnej oraz w BRPD.
Właściciel aktywu/zasobu odpowiada za bieżące nadzorowanie oraz zarządzanie aktywem.

8. Postępowanie z ryzykiem bezpieczeństwa

W ramach zarządzania bezpieczeństwem informacji w BRPD prowadzony jest systematyczny proces zarządzania ryzykiem, na który składa się:

- klasyfikacja zasobów,
- identyfikacja stopnia zagrożeń i ich następstw,
- określenie i wdrożenie działań zabezpieczających zasoby.

Dla obszarów wysokiego ryzyka prowadzone są działania zapobiegawcze. Obszary akceptowalnego ryzyka są monitorowane.

9. Utrzymanie odpowiedniego poziomu bezpieczeństwa informacji.

Ciągła aktualizacja Polityki i stosowanych zabezpieczeń oraz monitorowanie zagrożeń i zabezpieczeń powinno być niezbędną praktyką po wdrożeniu mechanizmów ochrony informacji. Nakłady ponoszone na zabezpieczenia muszą być poprzedzone analizą ryzyka i kosztów, adekwatnie do potencjalnych strat spowodowanych naruszeniem bezpieczeństwa.

Dla utrzymania odpowiedniego poziomu bezpieczeństwa informacji istotne jest systematyczne szkolenie pracowników.

10. Bezpieczeństwo fizyczne

Celem bezpieczeństwa fizycznego jest przeciwdziałanie nieautoryzowanemu dostępowi, uszkodzeniom i ingerencji w pomieszczenia BRPD i jego informacji.
Bezpieczeństwo fizyczne określają odrębne uregulowania wewnętrzne dotyczące przetwarzania informacji, w tym danych osobowych, również w systemach teleinformatycznych.

11. Bezpieczeństwo osobowe

Dla każdej grupy informacji wymagania dotyczące bezpieczeństwa osobowego wynikają z odpowiednich ustaw i postanowień umownych z wykonawcami.
Wszystkie osoby, których działalność będzie wiązała się z dostępem do danych, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa.

12. Bezpieczeństwo teleinformatyczne

Bezpieczeństwo teleinformatyczne zapewnia się poprzez wdrożenie systemu zarządzania bezpieczeństwem teleinformatycznym w zgodności z zaleceniem paragrafu 20 ust. 3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

13. Zarządzanie incydentami

Zarządzanie incydentami związanymi z bezpieczeństwem informacji jest realizowane za pomocą następujących działań:

- monitorowania i wykrywania naruszeń bezpieczeństwa w obszarach fizycznego dostępu, w tym w związku z przetwarzaniem informacji,
- monitorowania i wykrywania naruszeń bezpieczeństwa w systemach informatycznych,
- ocena skutków incydentu i ewentualne wprowadzenie działań korygujących.

14. Zarządzanie ciągłością działania

BRPD zapewnia ciągłość działania usług związanych z przetwarzaniem informacji. Dla wskazanych obszarów i systemów tworzone są plany postępowania w sytuacjach awaryjnych i kryzysowych. Celem stosowania zarządzania ciągłością działania jest przeciwdziałanie przerwom w funkcjonowaniu BRPD.

W celu skutecznego zarządzania ciągłością działania stosowane są zasady:

- opracowanie i wdrożenie planów ciągłości działania dla wskazanych elementów systemu teleinformatycznego BRPD,
- wskazanie osób odpowiedzialnych za utrzymanie ciągłości działania systemów informatycznych,
- podział odpowiedzialności za zarządzanie ciągłością działania.

15. Audyty bezpieczeństwa

W celu weryfikacji polityki bezpieczeństwa informacji przeprowadzane są okresowe audyty bezpieczeństwa. Dodatkowo audyty bezpieczeństwa powinny być przeprowadzane w przypadku wystąpienia poważnych incydentów.

16. Szczegółowe zasady bezpieczeństwa

Szczegółowe zasady bezpieczeństwa informacji przetwarzanych w Biurze RPD określają zarządzenia, postanowienia, wytyczne i polecenia Rzecznika Praw Dziecka.