CO ZROBIĆ
ŻEBY RODO NIE BYŁO
KOLEJNYM KOSZMAREM
DYREKTORA SZKOŁY?

SOI Serwis Ochrony Informacji

mgr inż. Wojciech Hoszek

ŹRÓDŁA PRAWA REGULUJĄCEGO ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (ODO)

Dz. U. z 2016 r. poz. 922

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

(Rozporządzenie techniczne)

Dz. U. z 2004 r. nr 100 poz. 1024

Rozporządzenie 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 (ogólne rozporządzenie o ochronie danych)

(RODO)

PORÓWNANIE

ODO	RODO
Art. 36. 1. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną,	Artykuł 32 1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku...

PORÓWNANIE

Rozporządzenie techniczne	RODO
A. Środki bezpieczeństwa na poziomie podstawowym V Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w § 4 pkt 1 rozporządzenia, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.	Artykuł 32 ... w tym między innymi w stosownym przypadku: a) pseudonimizację i szyfrowanie danych osobowych;

PORÓWNANIE

ODO	RODO
Art. 36. 1. Administrator danych ... ... w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.	Artykuł 32 ... w tym między innymi w stosownym przypadku: b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

PORÓWNANIE

Rozporządzenie techniczne	RODO
A. Środki bezpieczeństwa na poziomie podstawowym III System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed: 1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego; 2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.	Artykuł 32 ... w tym między innymi w stosownym przypadku: b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

PORÓWNANIE

Rozporządzenie techniczne	RODO
§ 5. Instrukcja, o której mowa w § 3 ust. 1, zawiera w szczególności: 4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;	Artykuł 32 ... w tym między innymi w stosownym przypadku: c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

PORÓWNANIE

ODO	RODO
Art. 36. 1. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną,	Artykuł 32 2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

PORÓWNANIE

ODO	RODO
Art. 37. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.	Artykuł 29 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 lub prawo państwa członkowskiego.

PORÓWNANIE

Rozporządzenie techniczne	RODO
§ 4. Polityka bezpieczeństwa, ... zawiera w szczególności: 1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;	Artykuł 24 1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

PORÓWNANIE

Rozporządzenie techniczne	RODO
§ 4. Polityka bezpieczeństwa, ... zawiera w szczególności: 1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; 2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;	Artykuł 24 1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

PORÓWNANIE

Rozporządzenie techniczne	RODO
§ 4. Polityka bezpieczeństwa, ... zawiera w szczególności: 3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;	Artykuł 24 1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

PORÓWNANIE

Rozporządzenie techniczne	RODO
§ 4. Polityka bezpieczeństwa, ... zawiera w szczególności: 3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi; 4) sposób przepływu danych pomiędzy poszczególnymi systemami;	Artykuł 24 1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

PORÓWNANIE

Rozporządzenie techniczne	RODO
§ 4. Polityka bezpieczeństwa, ... zawiera w szczególności: 5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.	Artykuł 24 1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

PORÓWNANIE

Rozporządzenie techniczne	RODO
§ 4. Polityka bezpieczeństwa, ... zawiera w szczególności: 5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.	Artykuł 5 1. Dane osobowe muszą być: f) 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”).

PORÓWNANIE

Rozporządzenie techniczne	RODO
§ 4. Polityka bezpieczeństwa, ... zawiera w szczególności: 5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.	Artykuł 5 2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).

PORÓWNANIE

Rozporządzenie techniczne	RODO
§ 5. Instrukcja, ... zawiera w szczególności: 1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;	Artykuł 24 2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

PORÓWNANIE

Rozporządzenie techniczne	RODO
§ 5. Instrukcja, ... zawiera w szczególności: 2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;	Artykuł 24 2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

PORÓWNANIE

Rozporządzenie techniczne	RODO
§ 5. Instrukcja, ... zawiera w szczególności: 3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;	Artykuł 24 2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

PORÓWNANIE

Rozporządzenie techniczne	RODO
§ 5. Instrukcja, ... zawiera w szczególności: 4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;	Artykuł 24 2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

PORÓWNANIE

Rozporządzenie techniczne	RODO
§ 5. Instrukcja, ... zawiera w szczególności: 5) sposób, miejsce i okres przechowywania: a) elektronicznych nośników informacji zawierających dane osobowe, b) kopii zapasowych, o których mowa w pkt 4,	Artykuł 24 2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

PORÓWNANIE

Rozporządzenie techniczne	RODO
§ 5. Instrukcja, ... zawiera w szczególności: 6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia; (wirusy)	Artykuł 24 2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

PORÓWNANIE

Rozporządzenie techniczne	RODO
§ 5. Instrukcja, ... zawiera w szczególności: 7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4; (rozliczalność)	Artykuł 24 2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

PORÓWNANIE

Rozporządzenie techniczne	RODO
§ 5. Instrukcja, ... zawiera w szczególności: 8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.	Artykuł 24 2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

NOWOŚCI

Artykuł 30

Rejestrowanie czynności przetwarzania

1. Każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. W rejestrze tym zamieszcza się wszystkie następujące informacje:

a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora...

b) cele przetwarzania;

c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;

d) kategorie odbiorców...

e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego

f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;

g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

ADMINISTRATOR DANYCH OSOBOWYCH	WSPÓŁADMINISTRATORZY
nazwa szkoły	

PRZEDSTAWICIEL ADMINISTRATORA	INSPEKTOR OCHRONY DANYCH OSOBOWYCH

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH	
Cel przetwarzania	*wypożyczanie książek z biblioteki*
Opis kategorii osób	*uczniowie szkoły, rodzice uczniów*
Opis kategorii danych osobowych	*imię, nazwisko, adres zamieszkania, klasa (w przypadku ucznia)*
Kategorie odbiorców	*pracownicy pedagogiczni szkoły*
	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
Przekazania danych	*brak*
	gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń; *(przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przedumownych podejmowanych na żądanie osoby, której dane dotyczą;)*
Termin usunięcia	*po zakończeniu nauki w szkole*
	Jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
Opis środków bezpieczeństwa	*dane osobowe przetwarzane na komuterze w programie "nazwa programu", dane w bazie danych programu, zabezpiecznie komputera oraz pomieszczenia zgodne z zapisami w dokumentacji ochrony danych osobowych.*
	Jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1. *(- pseudonimizację i szyfrowanie danych osobowych; - zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; - zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; - zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;)*
Uwagi	

.....
data i podpis Administratora

NOWOŚCI

Artykuł 32

Bezpieczeństwo przetwarzania

Ust 1. lit. d)

regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

NOWOŚCI

Artykuł 32

Bezpieczeństwo przetwarzania

Ust 2.

Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Lp.	Zasób	Wartość dla organizacji	Forma naruszenia bezpieczeństwa	Nasilenie	Wartość ryzyka
1	Zbiór danych „Pracownicy”	Mało ważny	naruszenie integralności	Rzadkie	1
		Mało ważny	brak umowy powierzenia	Rzadkie	1
		Mało ważny	nieautoryzowany dostęp	Rzadkie	1
		Mało ważny	nieautoryzowane skopiowanie danych	Rzadkie	1
		Mało ważny	brak aktualizacji danych	Rzadkie	1
		Mało ważny	pozostawienie dokumentu bez nadzoru	Mało prawdopodobne	2
2	Zbiór danych „Klienci”	Istotny	nieautoryzowane skopiowanie danych	Rzadkie	2
		Istotny	nieautoryzowany dostęp	Średnie	6
		Istotny	naruszenie integralności	Rzadkie	2
		Istotny	pozostawienie dokumentu bez nadzoru	Średnie	6
		Istotny	kradzież	Rzadkie	2
3	Zbiór danych „Korespondencja”	Bardzo ważny	nieautoryzowane skopiowanie danych	Mało prawdopodobne	8
		Bardzo ważny	nieautoryzowany dostęp	Mało prawdopodobne	8
		Bardzo ważny	naruszenie integralności	Rzadkie	4
		Bardzo ważny	pozostawienie dokumentu bez nadzoru	Mało prawdopodobne	8
		Bardzo ważny	kradzież	Rzadkie	4
4	Telefon firmowy 1	Bardzo ważny	kradzież	Rzadkie	4
		Bardzo ważny	awaria	Mało prawdopodobne	8
		Bardzo ważny	nieautoryzowany dostęp	Średnie	12
		Bardzo ważny	możliwość odtajnienia kodu dostępu	Średnie	12
		Bardzo ważny	nieautoryzowane skopiowanie danych	Rzadkie	4
		Bardzo ważny	brak umowy powierzenia	Rzadkie	4
		Bardzo ważny	brak dostępu do sieci	Mało prawdopodobne	8

NOWOŚCI

Artykuł 37

Wyznaczenie inspektora ochrony danych

1. Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy:

a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;

3. Jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego inspektora ochrony danych.

Przykładowy wykaz dokumentów

- Ewidencja osób upoważnionych do przetwarzania danych osobowych
- Imienne upoważnienie do przetwarzania danych osobowych
- Karta ewidencyjna stanowiska komputerowego
- Klauzula informacyjna
- Ocena ryzyka przy przetwarzaniu
- Oświadczenie pracownika
- Polityka czystego biurka i czystego ekranu
- Polityka kluczy
- Polityka monitoringu wizyjnego
- Polityka nadzoru nad oprogramowaniem i sprzętem
- Polityka zakup sprzętu i oprogramowania
- Polityka zarządzania hasłami
- Procedura antywirusowa
- Procedura nadawania uprawnień
- Procedura rozpoczęcia, zawieszenia i zakończenia pracy przez użytkownika
- Procedura tworzenia kopii zapasowych
- Procedura użytkowania nośników informacji
- Procedura wykonywania przeglądów
- Procedura zachowania ciągłości działania
- Protokół zniszczenia nośnika
- Raport z analizy ryzyka
- Raport z naruszenia bezpieczeństwa systemu informatycznego
- Rejestr czynności
- Rejestr czynności serwisowych ASI
- Rejestr udostępnień
- Umowa powierzenia przetwarzania danych osobowych
- Wniosek o nadanie uprawnień do zasobów informatycznych
- Wykaz aktywów

Zapisy w umowie powierzenia

1. Procesor zobowiązuje się do nadzoru nad przestrzeganiem zasad ochrony i przetwarzania danych lub wyznacza do tego Inspektora Ochrony Danych.
2. Procesor zobowiązuje się do dopuszczania do przetwarzania danych wyłącznie osoby posiadające upoważnienie nadane przez Procesora, przeszły szkolenie z zasad przetwarzania danych osobowych oraz zobowiązały się do przestrzegania tych zasad i zachowania tajemnicy.
3. Procesor w miarę możliwości pomaga Zleceniodawcy poprzez odpowiednie środki techniczne i organizacyjne wywiązać się obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III Rozporządzenia.
4. Procesor w razie potrzeby i posiadania stosownych informacji pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–34 Rozporządzenia.
5. Procesor udostępnia Zleceniodawcy wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w artykule 28 Rozporządzenia oraz umożliwia Zleceniodawcy lub audytorowi upoważnionemu przez Zleceniodawcę przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

Dziękuję za uwagę

mgr inż. Wojciech Hoszek

SOI Serwis Ochrony Informacji