Arkusz analizy ryzyka

P-Prawdopodobieństwo incydentu (skala od 1 do 3), S-Skutki wystąpienia incydentu (skala od 1 do 3), R-Ryzyko wystąpienia incydentu (skala od 1 do 9), Formuła: R=P*S

Zagrożenie	Opis zagrożenia	P	S	R	Zabezpieczenie (wskazane jako rozdział w Instrukcji RODO)
nieuprawnione ujawnienie	1. Przekazanie danych osobom nieuprawnionym	1	2	2	Regulamin ODO
	2. Przesłanie maila z danymi osobowymi do osób nieuprawnionych	1	2	2	Instrukcja RODO:
	3. Udostępnienie danych (baz i plików) przez internet bez logowania	1	2	2	- Zabezpieczenia fizyczne
	4. Zagubienie/kradzież nośników papierowych i elektronicznych poza organizacją (dokumentów, laptopów, dysków przenośnych, pendrive)	1	3	3	- Zabezpieczenia techniczne - Procedura nadawania uprawnień do przetwarzania danych osobowych.
	5. Zagubienie/kradzież smartfonów poza organizacją	1	1	1	- Metody i środki uwierzytelnienia (polityka haseł)
	6. Wyrzucenie niezniszczonych dokumentów	1	1	1	- Procedura tworzenia kopii zapasowych
	7. Utylizacja/sprzedaż/naprawa sprzętu z nieusuniętymi danymi osobowymi na nośnikach	1	1	1	- Utylizacja elektronicznych nośników i wydruków oraz czyszczenie danych - Procedura zabezpieczenia systemu informatycznego - Procedura wykonywania przeglądów i konserwacji
nieuprawniony dostęp do danych podczas przesyłania	1. Podsłuch przesyłanych danych podczas korzystania z aplikacji webowych oraz formularzy kontaktowych	1	1	1	Instrukcja RODO: - Procedura zabezpieczenia systemu informatycznego
	2. Podsłuch przesyłanych danych podczas pracy zdalnej informatyków oraz innych osób uprawnionych do pracy zdalnej	1	2	2	
nieuprawniony dostęp do danych podczas przechowywania	1. Niezabezpieczony dostęp do pomieszczeń z dokumentacją papierową i sprzętem komputerowym (biura, serwerownia, archiwum)	1	3	3	Instrukcja RODO: - Zabezpieczenia fizyczne
	2. Niezabezpieczony dostęp do baz danych lub do katalogów z plikami lub do chmury przez internet (przed hackerami i szkodliwym oprogramowaniem)	1	3	3	- Zabezpieczenia techniczne - Procedura nadawania uprawnień do przetwarzania danych osobowych. - Metody i środki uwierzytelnienia (polityka haseł)
	3. Brak kontroli dostępu użytkowników do baz danych lub do katalogów z plikami lub do chmury	1	3	3	- Procedura tworzenia kopii zapasowych - Utylizacja elektronicznych nośników i wydruków oraz czyszczenie danych - Procedura zabezpieczenia systemu informatycznego
przypadkowe lub niezgodne z prawem zniszczenie, uszkodzenie	1. Pożar, zalanie, wybuchy	1	3	3	Instrukcja RODO:
	2. Awarie sprzętu IT (serwerów, komputerów)	1	1	1	- Zabezpieczenia techniczne
	3. Awarie oprogramowania	1	1	1	- Procedura tworzenia kopii zapasowych
	4. Błędy w działaniu systemów i aplikacji jako skutki uboczne procesu aktualizacji	2	1	2	- Procedura wykonywania przeglądów i konserwacji
	5. Brak łączności internetowej	2	1	2	
przypadkowe lub niezgodne z prawem utracenie	1. Kopie bezpieczeństwa nieodporne na kryptowirusy	1	3	3	Instrukcja RODO:
	2. Brak kopii bezpieczeństwa lub kopie niemożliwe do odtworzenia	2	3	6	= Procedura tworzenia kopii zapasowych
przypadkowe lub niezgodne z prawem zmodyfikowanie	1. Fałszerstwo danych do przelewów na fakturach (mailowo)	1	3	3	**Procedura weryfikacji dokumentów księgowych**

07 Procedura audytu

Celem audytów wewnętrznych jest ocena, czy system ochrony danych osobowych jest skutecznie wdrożony i funkcjonuje zgodnie z wymaganiami RODO. Audyty prowadzone są w sposób obiektywny i bezstronny. Przestrzegana jest zasada, że audytorzy nie audytują własnej pracy.

1. Administrator (ewentualnie IOD) jest odpowiedzialny za planowanie i przeprowadzanie audytów wewnętrznych z roczną częstotliwością lub częściej
2. Administrator (ewentualnie IOD) opracowuje programy audytów biorąc pod uwagę ważność procesów przetwarzania oraz audytowanych obszarów, jak też wyniki wcześniejszych audytów. Określa on kryteria audytu, jego cel, zakres i ewentualnie metody.
3. Administrator (ewentualnie IOD) wyznacza audytora do przeprowadzenia audytu
4. Audytor jest zobowiązany do przygotowania się do przeprowadzenia audytu, zapoznając się z opisem audytowanego obszaru, stosowanych procedur i wyników poprzednich audytów
5. Audytor realizuje działania audytowe mające na celu uzyskanie obiektywnych dowodów potwierdzających poprawność realizowanych zadań, procedur, polityk, zabezpieczeń, celów, spełniania wymagań RODO
6. W przypadku stwierdzenia uchybień mających wpływ na skuteczność działania systemu ochrony danych zgodnego z RODO, audytor identyfikuje tzw. uchybienia lub spostrzeżenia
7. Wynik audytu zostaje udokumentowany przez audytora i przekazany Administratorowi (ewentualnie IOD)
8. Administrator (ewentualnie IOD) dokonuje przeglądu i analizy wyniku audytu oraz decyduje o inicjowaniu działań korygujących, w przypadku zaistnienia poważnych uchybień.

Opis / okoliczności naruszenia/incydentu	Ilość osób dotknięta naruszeniem/incydentem	Skutki naruszenia/incydentu

Działania zaradcze	Data rozpoczęcia wdrożenia działań	Data zakończenia wdrażania działań

Załącznik 01d– Upoważnienie do przetwarzania danych osobowych

---

UPOWAŻNIENIE/ANULOWANIE UPOWAŻNIENIA* Nr X
do przetwarzania danych osobowych
w systemach informatycznych lub w zbiorach w wersji papierowej

---

Część I – wersja podstawowa upoważnienia
Z dniem DD-MM-RRRR upoważniam / anuluję upoważnienie

Panią/Pani/Pana* podać imię nazwisko

pracownika podać nazwę jednostki lub działu do przetwarzania danych osobowych

---

Część II – wersja rozszerzona upoważnienia

w zbiorach: podać nazwy zbiorów

w zakresie: (WG) wglądu, (W) wprowadzania, (M) modyfikacji, (U) usuwania, (A) archiwizacji, (U) udostępniania innym podmiotom, (I) koniecznym do wykonywania obowiązków pracowniczych

---

Upoważnienie dotyczy przetwarzania danych osobowych **w systemach informatycznych** podać nazwy systemów lub programów

---

Upoważnienie dotyczy przetwarzania danych osobowych **w zbiorach papierowych**: podać nazwy tych zbiorów

....

(miejscowość i data) (pieczęć i podpis Administratora/IOD)

EWIDENCJA UŻYTKOWNIKA SYSTEMÓW INFORMATYCZNYCH

Nazwa systemu / programu: podać nazwę

Identyfikator użytkownika: podać identyfikator

Zakres uprawnień użytkownika: np. dostęp do modułu kadry, drukowanie list płac, odczyt, zapis

Data zarejestrowania w systemie: DD-MM-RRRR

Data wyrejestrowania użytkownika: DD-MM-RRRR

.....

podpis Administratora Systemu Informatycznego

*) niepotrzebne skreślić