Z A T W I E R D Z A M

………………………………………

(data, pieczęć i podpis)

Metodologia

oceny skutków dla ochrony danych osobowych

****

**Pełny zakres dostępu do dokumentu** – odczyt, modyfikacja, usuwanie, dodawanie:

1. Rektor UO
2. Kanclerz UO
3. Inspektor ochrony danych (IOD)
4. Dyrektor Centrum Informatycznego – Administrator Systemu Informatycznego UO (ASI)

**Zakres dostępu do dokumentu – odczyt:**

1. Osoby pisemnie upoważnione przez Rektora UO.

OPRACOWAŁ

…………………………. (data, pieczęć i podpis)

|  |  |  |  |
| --- | --- | --- | --- |
| Karta zmian w Metodologii | | | |
| Nr | Opis dokonanej zmiany w treści dokumentu | Data wprowadzonej  zmiany | Imię i nazwisko uprawnionego pracownika |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |
| 9 |  |  |  |
| 10 |  |  |  |

**SPIS TREŚCI**

[2 Wstęp 4](#_Toc34067468)

[3 Terminologia 4](#_Toc34067469)

[4 Zakres 5](#_Toc34067470)

[5 Proces przeprowadzania DPIA 5](#_Toc34067471)

[6 Odpowiedzialność w DPIA 6](#_Toc34067472)

[7 Praktyka DPIA 8](#_Toc34067473)

# WSTĘP

Niniejszy dokument jest zbiorem zasad realizacji procesu oceny skutków oraz szacowania ryzyka w bezpieczeństwie dla ochrony danych osobowych zgodnie z wytycznymi normy PN-ISO/IEC 27005:2014-01 oraz metodologii Privacy Impact Assessment CNIL June 2015 Edition.

# TERMINOLOGIA

**Ryzyko w bezpieczeństwie informacji** – rozumiane jest jako wartość zależna od wysokości potencjalnych strat, wynikających z niewłaściwego przetwarzania informacji oraz od prawdopodobieństwa wystąpienia takich strat.

**RODO** – 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).

**AD** – administrator danych osobowych.

**DPIA, ocena skutków** – ocena skutków dla ochrony danych osobowych.

**Ryzyko szczątkowe** – poziom ryzyka po wdrożeniu zabezpieczeń.

**Poziom ryzyka akceptowalnego** – poziom zapewniający, że ryzyka szczątkowe są świadomie zaakceptowane przez kierownictwo organizacji.

**Aktywo lub zasób informacyjny -** wszelkie zapisy w formie papierowej i elektronicznej, przetwarzane (zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane i usuwane) w sposób tradycyjny lub w systemach informatycznych, będące własnością AD lub wykorzystywane bądź administrowane.

**Poufność informacji –** atrybut bezpieczeństwa aktywa informacyjnego oznaczający, że dostęp do informacji powinny mieć jedynie osoby upoważnione.

**Integralność –** atrybut bezpieczeństwa aktywa informacyjnego określający jakość informacji w aspekcie kompletności, spójności i wiarygodności danych.

**Dostępność –** atrybut bezpieczeństwa aktywa informacyjnego oznaczający dostępność informacji dla osób upoważnionych wtedy, kiedy potrzebują go do przetwarzania.

**Podatności –** rozumiemy jako wady, luki lub słabości w strukturze fizycznej, organizacji, procedurach, personelu, zarządzaniu, administrowaniu, sprzęcie lub oprogramowaniu (zasobu lub grupy zasobów), które mogą być wykorzystane przez zagrożenie do spowodowania szkód.

**Zagrożenie informacji –** rozumiemy jako potencjalne działanie wobec zasobu informacyjnego lub procesu, mogące wykorzystać określoną podatność, w celu spowodowania strat.

**Prawdopodobieństwo wystąpienia zagrożenia –** rozumiemy jako potencjalną możliwość lub częstość występowania zagrożenia.

# ZAKRES

Dokument wskazuje sposób dokonywania oceny skutków dla ochrony danych osobowych zgodnie z wymaganiami RODO. Metodologia oceny skutków jest narzędziem dla ADO umożliwiającym wykazanie zgodności z zasadą rozliczalności RODO. Pozwala również zapewnić przez ADO stosowanie w swoich produktach lub usługach koncepcji Privacy by Design. Stosowanie DPIA jest użytecznym dla ADO środkiem wspierającym tworzenie systemów oraz procesów przetwarzania danych osobowych respektujących prywatność osób, których dane dotyczą.

# PROCES PRZEPROWADZANIA DPIA

**Minimalne wymagania** dla metodologii oceny skutków:

1. Opis operacji przetwarzania.
2. Opis celów przetwarzania.
3. Ocena niezbędności operacji.
4. Ocena proporcjonalności przetwarzania.
5. Środki planowane w celu:
   1. Zaradzenia ryzyku.
   2. Wykazania przestrzegania RODO.



Opis planowanych operacji przetwarzania

Ocena niezbędności i proporcjonalności

Planowane środki w celu wykazania zgodności z RODO

Ocena ryzyka dla praw i wolności

Środki planowane w celu zaradzenia ryzyku

Dokumentacja

Monitorowanie i przegląd

Celem dokonywania oceny skutków jest szacowanie ryzyka, które rozumiemy jako hipotetyczny scenariusz opisany poprzez:

1. Źródła ryzyka np. haker.
2. Podatności, które mogą być wykorzystane w zasobach wspomagających przetwarzanie danych osobowych np. jeden użytkownik w aplikacji użytkowany przez wielu pracowników pozwalający na zmianę danych bez określenia tożsamości użytkownika.
3. Zdarzenie, którego się obawiamy np. nieupoważniony dostęp do danych.
4. Rodzaj danych osobowych np. dane osobowe klientów.
5. Wpływ na osoby, których dane dotyczą np. nagabywanie, strata środków finansowych na karcie kredytowej.

# ODPOWIEDZIALNOŚĆ W DPIA

Kontekst

Decyzja

Zabezpieczenia

Ryzyko

1. **Kontekst.** Zdefiniowanie i opisanie środowiska przetwarzania danych osobowych. Wskazanie celów przetwarzania.
   1. Cele przetwarzania, opis środowiska.
   2. Opis procesów przetwarzania.
   3. Opis danych osobowych.
   4. Wykaz aktywów wspomagających.
2. **Zabezpieczenia.**Identyfikacja obecnych oraz planowanych środków zapewniających zgodność z przepisami oraz kontrolujących ryzyka dla prywatności.
   1. Wykaz zabezpieczeń prawnych. Cel, informacje, rodzaj zabezpieczanych praw.
   2. Wykaz zabezpieczeń dla danych osobowych.
3. **Ryzyka.** Ocena ryzyka dla prywatności w celu zapewniania adekwatności i właściwego zaplanowania postępowania z ryzykiem.
   1. Wskazanie źródeł ryzyka. Odpowiadamy na pytania: kto i dlaczego?
   2. Opis zdarzeń powodujących ryzyko. Odpowiadamy na pytania: co i w jaki sposób?
   3. Wskazanie zagrożeń oraz podatności.
   4. Określamy poziomy prawdopodobieństwa oraz skutki.
4. **Decyzja.** Podjęcie decyzji o sposobie uzyskania zgodności z zasadami prywatności oraz postępowania z ryzykiem.
   1. Ewaluacja ryzyka.
   2. Wskazanie celów zabezpieczeń.
   3. Opracowanie planów postępowania.
   4. Formalna walidacja.
   5. Jeżeli ryzyko nie jest akceptowalne, konsultacja z organem nadzorczym.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Etap** | **AD** | **Właściciel procesu** | **IOD** | **ASI** |
| 1a-1d | Akceptujący | Realizujący | Konsultujący | Informowany |
| 2a | Akceptujący | Konsultujący | Realizujący | Informowany |
| 2b | Akceptujący | Konsultujący | Informowany | Realizujący |
| 3a | Akceptujący | Realizujący | Informowany | Konsultujący |
| 3b | Akceptujący | Konsultujący | Realizujący | Realizujący |
| 3c | Akceptujący | Informowany | Konsultujący | Realizujący |
| 3d | Akceptujący | Informowany | Realizujący | Realizujący |
| 4a | Akceptujący | Informowany | Konsultujący | Realizujący |
| 4b | Akceptujący | Informowany | Realizujący | Informowany |
| 4c | Akceptujący | Realizujący | Konsultujący | Konsultujący |
| 4d | Realizujący | Informowany | Konsultujący | Informowany |

# PRAKTYKA DPIA

## 1a, 1b. Opis procesów przetwarzania.

|  |  |
| --- | --- |
| **Ogólny opis procesu**  **Przetwarzania** |  |
| **Cele przetwarzania** | 1. |
| **Rezultat przetwarzania** | 1. |
| **Administratorzy danych**  **(Lokalni administratorzy Danych )** |  |
| **Procesory danych** | 1. |

## 1c. Opis danych osobowych.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Dane osobowe** | **Kategorie** | **Odbiorcy**  **danych**  **(uzasadnienie)** | **Użytkownicy danych**  **(uzasadnienie)** | **Retencja**  **danych**  **(uzasadnienie)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## 1d. Opis aktywów wspomagających.

|  |  |  |  |
| --- | --- | --- | --- |
| **Etap procesu** | **Opis etapu** | **System przetwarzania** | **Aktywa wspomagające:**  **sprzęt,**  **oprogramowanie,**  **lokalizacje, ludzie.** |
| **Zbieranie** |  |  |  |
| **Przechowywanie** |  |  |  |
| **Wykorzystanie** |  |  |  |
| **Przekazywanie** |  |  |  |
| **Niszczenie** |  |  |  |

## 2a. Wykaz zabezpieczeń prawnych.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Obszar** | **Temat** | **Cel zabezpieczenia** | **Rodzaj**  **działania**  **(działa na:)** | **Opis zabezpieczenia**  **oraz**  **uzasadnienie** |
| Prawny | Cel | Konkretny, wyraźny i prawnie uzasadniony cel. | Dane |  |
| Prawny | Minimalizacja | Ograniczenie ilości danych osobowych do tego, co  niezbędne. | Dane |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Obszar** | **Temat** | **Cel zabezpieczenia** | **Rodzaj  działania**  **(działa na:)** | **Opis zabezpieczenia oraz**  **uzasadnienie** |
| Prawny | Jakość | Zapewnienie i utrzymanie jakości danych osobowych. | Dane |  |
| Prawny | Okres retencji | Zapewnienie przetwarzania tylko w czasie niezbędnym do osiągnięcia celu przetwarzania.  Przy uwzględnienie odrębnych przepisów np. dot. archiwizacji danych. | Dane |  |
| Prawny | Informacja | Przekazanie informacji  o prawach osobom, których dane są przetwarzane. | Dane |  |
| Prawny | Podstawa przetwarzania | Uzyskanie podstawy przetwarzania w postaci przepisu lub zgodny osoby, której dane dotyczą. | Dane |  |
| Prawny | Sprzeciw | Zapewnienie prawa sprzeciwu dla osób, których dane dotyczą. | Dane |  |
| Prawny | Dostęp | Zapewnienie dostępu do danych dla osób, których dane dotyczą. | Dane |  |
| Prawny | Sprostowanie | Zapewnienie możliwości sprostowania i usunięcia danych dla osób, których dane dotyczą. | Dane |  |
| Prawny | Transfer | Zapewnienie zgodności podczas przekazywania danych poza UE. | Dane |  |
| Prawny | Precheck | Zapewnienie wypełnienia formalności przed rozpoczęciem  przetwarzania. | Dane |  |

## 2b. Wykaz zabezpieczeń organizacyjnych, informatycznych oraz fizycznych.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Obszar** | **Temat** | **Cel zabezpieczenia** | **Rodzaj działania**  **(działa na:)** | **Opis zabezpieczenia oraz**  **uzasadnienie** |
| Prawny | Cel | Konkretny, wyraźny  i prawnie uzasadniony cel. | Dane |  |
| Prawny | Minimalizacja | Ograniczenie ilości danych osobowych do tego, co  niezbędne. | Dane |  |
| Prawny | Jakość | Zapewnienie  i utrzymanie jakości danych osobowych. | Dane |  |
| Prawny | Okres retencji | Zapewnienie przetwarzania tylko w czasie niezbędnym do osiągnięcia celu przetwarzania.  Przy uwzględnienie odrębnych przepisów np. dot. archiwizacji danych. | Dane |  |
| Prawny | Informacja | Przekazanie osobom których dane są przetwarzane, informacji o ich prawach. | Dane |  |
| Prawny | Podstawa przetwarzania | Uzyskanie podstawy przetwarzania w postaci przepisu lub zgodny osoby, której dane dotyczą. | Dane |  |
| Prawny | Sprzeciw | Zapewnienie prawa  sprzeciwu dla osób, których dane dotyczą. | Dane |  |
| Prawny | Dostęp | Zapewnienie dostępu do danych dla osób, których dane dotyczą. | Dane |  |
| Prawny | Sprostowanie | Zapewnienie możliwości sprostowania i usunięcia danych dla osób, których  dane dotyczą. | Dane |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Obszar** | **Temat** | **Cel zabezpieczenia** | **Rodzaj działania**  **(działa na:)** | **Opis zabezpieczenia oraz**  **uzasadnienie** |
| Prawny | Transfer | Zapewnienie zgodności podczas przekazywania  danych poza UE. | Dane |  |
| Prawny | Sprawdzenie przed rozpoczęciem przetwarzania | Zapewnienie wypełnienia formalności przed rozpoczęciem  przetwarzania. | Dane |  |
| Organizacyjny | Struktura | Wskazanie struktury organizacyjnej  i odpowiedzialności. | Organizacja |  |
| Organizacyjny | Polityka | System zarządzania danymi osobowymi  w postaci zasad  postępowania. | Organizacja |  |
| Organizacyjny | Zarządzanie ryzykiem | Zasady zarządzania  ryzykiem. | Organizacja |  |
| Organizacyjny | Zarządzanie projektem | Zasady zarządzania projektami  z uwzględnieniem spełnienia wymagań RODO. | Organizacja |  |
| Organizacyjny | Zarządzanie incydentami i włamaniami | Zasady zarządzania,  w tym reagowania na incydenty. | Skutki |  |
| Organizacyjny | Zarządzanie personelem | Zasady zarządzania związanymi z zatrudnianiem osób przetwarzających. | Źródła |  |
| Organizacyjny | Zarządzanie relacjami ze stroną trzecią | Zasady zarządzania przy współpracy  z podmiotami  trzecimi/stronami trzecimi. | Źródła |  |
| Organizacyjny | Przegląd | Zasady dokonywania przeglądów zarządzania. | Źródła |  |
| Organizacyjny | Nadzór | Prowadzenie monitorowania  i audytu systemu zarządzania  danymi osobowymi. | Organizacja |  |
| Organizacyjny | Oznaczanie dokumentów | Wprowadzanie zasad oznaczania informacji  z danymi osobowymi adekwatnie do ich  klasyfikacji. | Źródła |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Obszar** | **Temat** | **Cel zabezpieczenia** | **Rodzaj działania**  **(działa na:)** | **Opis zabezpieczenia oraz**  **uzasadnienie** |
| Organizacyjny | Archiwizacja | Wprowadzenie zasad  archiwizacji danych zgodnie z przepisami odrębnymi. | Organizacja |  |
| Informatyczny | Anonimizacja | Wprowadzenie procesu anonimizacji  w wybranych środowiskach np. testowych, przed  przekazaniem stronie  trzeciej. | Dane |  |
| Informatyczny | Szyfrowanie | Określenie polityki kryptografii jej stosowanie. | Źródła |  |
| Informatyczny | Sumy kontrolne, skróty, weryfikacja poprawności  danych. | Wdrożenie metod weryfikacji wprowadzanych  zmian w danych. | Skutki |  |
| Informatyczny | Kopie zapasowe | Wprowadzenie zabezpieczeń przed utratą danych. | Skutki |  |
| Informatyczny | Dzielenie danych | Zabezpieczenie przed dostępem nieupoważnionym. | Źródła |  |
| Informatyczny | Kontrola dostępu | Zapewnienie adekwatnych uprawnień dla osób upoważnionych do przetwarzania. | Źródła |  |
| Informatyczny | Możliwość śledzenia | Zapewnienie możliwości śledzenia wprowadzanych  zmian w danych. | Źródła |  |
| Informatyczny | Monitorowanie | Wykrywanie incydentów. | Źródła |  |
| Informatyczny | Zarządzanie zmianami i konfiguracją | Zapewnienie kontroli nad zmianami  w infrastrukturze  i aktywach wspomagających. | Aktywa wspomagające |  |
| Informatyczny | Zarządzanie stacjami roboczymi | Zapewnienie stosowania standardów bezpieczeństwa  na stanowisku  komputerowym. | Aktywa wspomagające |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Obszar** | **Temat** | **Cel zabezpieczenia** | **Rodzaj działania**  **(działa na:)** | **Opis zabezpieczenia oraz**  **uzasadnienie** |
| Informatyczny | Zabezpieczenia przed malware | Stosowanie AV, IPS, IDS, zasad bezpieczeństwa przy dostępie do Internetu. | Źródła |  |
| Informatyczny | Bezpieczeństwo sieci | Stosowanie zasad podziału na segmenty, ACL, kontrola dostępu do usług sieciowych. | Aktywa wspomagające |  |
| Fizyczny | Kontrola dostępu do budynków  i pomieszczeń. | Zapewnienie adekwatnych uprawnień dla osób upoważnionych do przetwarzania. | Źródła |  |
| Fizyczny | Bezpieczeństwo sprzętu | Zapewnienie stosowania standardów bezpieczeństwa  eksploatacji sprzętu. | Aktywa wspomagające |  |
| Fizyczny | Bezpieczeństwo dokumentacji papierowej | Wdrożenie zasad postępowania  z dokumentami papierowymi  na stanowisku pracy. | Aktywa wspomagające |  |
| Fizyczny | Bezpieczeństwo obiegu papierowego | Wprowadzenie zabezpieczeń podczas przekazywania  i transferu  dokumentów papierowych. | Aktywa wspomagające |  |
| Fizyczny | Bezpieczeństwo środowiskowe | Zabezpieczenie przed pożarem, zalaniem, wyładowaniem elektromagnetycznym  utratą zasilania itp. | Źródła |  |

## 3a. Wskazanie źródeł ryzyka.

|  |  |  |
| --- | --- | --- |
| **Rodzaj źródła ryzyka** | **Opis źródła ryzyka** | **Opis powodów działania**  **Opis dostępnych zasobów dla źródła** |
| Wewnętrzne źródło ludzkie działające  przypadkowo |  |  |
| Wewnętrzne źródło ludzkie działające  celowo |  |  |
| Zewnętrzne źródło ludzkie działające  przypadkowo |  |  |
| Zewnętrzne źródło ludzkie działające  celowo |  |  |
| Wewnętrzne źródło inne niż ludzkie |  |  |
| Zewnętrzne źródło inne niż ludzkie |  |  |

## 3b. Opis zdarzeń powodujących ryzyko.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Potencjalne naruszenie danych osobowych** | **Źródło ryzyka** | **Skutek naruszenia: Brak wyniku**  **Przechowywanie Usterka Redystrybucja Wykorzystanie Korelacja Zablokowanie Inne (opis)** | **Opis wpływu na osoby, których dane dotyczą** | **Zabezpieczenia** | **Poziom wpływu**  **[1- 4]** | **Uzasadnienie** |
| Nieupoważniony dostęp |  | Brak skutku Przechowywanie Redystrybucja Wykorzystanie Korelacja  Inne (opis) |  |  |  |  |
| Niepożądana zmiana |  | Brak skutku Usterka Wykorzystanie Inne (opis) |  |  |  |  |
| Znikniecie danych |  | Usterka Zablokowanie Inne (opis) |  |  |  |  |

## 3c. Wskazanie zagrożeń oraz podatności.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Zagrożenie** | **Źródło ryzyka** | **Podatność** | **Zabezpieczenia** | **Prawdopodobieństwo** | **Uzasadnienie** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## 4a-4c. Estymacja ryzyka, cele zabezpieczeń, plany postępowania z ryzykiem.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Nr ryzyka** | **Nazwa** | **Źródło ryzyka** | **Klasa z.d.o/aktywa [1-4]** | **Podatność (opis)** | **Opis wykorzystania podatności przez zagrożenie (opis sytuacja/zagrożenie)** | **Opis skutku na osoby, których dane dotyczą.** | **Prawdopodobieństwo zdarzenia [1-4]** | **Wpływ [1-4]** | **Ryzyko = P x**  **Wpływ x WA**  **= 4\*8\*9** | **Właściciel ryzyka** |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** |
|  |  |  |  |  | Ujawnienie danych osobowych nieupoważnionym. |  |  |  |  |  |
|  |  |  |  |  | Przekazanie danych podmiotom nieuprawnionym. |  |  |  |  |  |
|  |  |  |  | Brak właściwego informowania osób, których dane dotyczą. |  |  |  |  |  |  |
|  |  |  |  | Brak właściwych zgód na przetwarzanie  danych osobowych. |  |  |  |  |  |  |
|  |  |  |  | Brak polityki prywatności. |  |  |  |  |  |  |
|  |  |  |  | Brak właściwych klauzul w umowach z dostawcami usług cloudowych. |  |  |  |  |  |  |
|  |  |  |  | Brak możliwości dostępu do danych dla podmiotów danych. |  |  |  |  |  |  |
|  |  |  |  | Brak możliwości sprostowania danych przez podmioty danych. |  |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Postępowanie z ryzykiem (plan właściciela)** | **Prawdopodobieństwo zdarzenia (1-4)**  **\po wdrożeniu planu postępowania z ryzykiem** | **Wpływ [1-4]** | **Ryzyko po wdrożeniu planu postępowania z ryzykiem**  **= P x**  **Wpływ x WA Integralność**  **(4\*13\*14)** | **Decyzja** |
| **12** | **13** | **14** | **15** | **16** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## 4d. Formalna walidacja.

W dniu [data], [tożsamość lub funkcja] zatwierdza DPIA w świetle przeprowadzonego badania i raportu DPIA. Postępowanie z ryzykiem powinno pozwolić na [synteza planowanego osiągnięcia rezultatów działań].

Sposób, w jaki planowane jest wdrożenie wymagań prawnych oraz postępowania z ryzykiem jest uważane za akceptowalne względem osiąganych rezultatów działań.

Wdrożenie planu działania oraz ciągłe doskonalenie DPIA powinny być wykazane.

[Podpis]

## 4e. Ryzyko nie jest akceptowalne.

Konsultacja z organem nadzorczym.