Zarządzenie Nr 15 /2018
Dyrektora Konińskiego Domu Kultury w Koninie
z dnia 22 czerwca 2018 roku

w sprawie: procedury oceny skutków dla ochrony danych osobowych (privacy impact assessment)

1. Administrator danych osobowych jest odpowiedzialny za zapewnienie przeprowadzenia oceny skutków dla ochrony danych osobowych (PIA).
2. Przeprowadzenie PIA może zostać dokonane w ramach organizacji (wewnętrznie) lub przez podmiot zewnętrzny, natomiast to Administrator Danych pozostaje ostatecznie odpowiedzialny za to zadanie.
3. Dokonując PIA, Administrator Danych konsultuje się z IOD.
4. W przypadku jeśli przetwarzanie danych osobowych dokonywane jest przy udziale podmiotu przetwarzającego, powinien on uczestniczyć w przeprowadzeniu oceny skutków oraz udzielać niezbędnych informacji.
5. Administrator Danych dokonuje oceny skutków planowanych operacji przed rozpoczęciem przetwarzania danych osobowych. Należy jednak pamiętać, że ocenę skutków należy poddawać przeglądowi i w razie potrzeby aktualizować, w sytuacji gdy zmienia się ryzyko wynikające z operacji przetwarzania (zmiana/ewolucja elementu procesu).
6. PIA może dotyczyć pojedynczej operacji przetwarzania danych lub kilku podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem.
7. W sytuacji, w której operacja przetwarzania dotyczy współadministratorów – ich obowiązki zostają dokładnie określone i rozdzielone. PIA jasno wskazuje, która strona jest odpowiedzialna za stosowanie odpowiednich środków przewidzianych do zaradzenia ryzyku oraz ochrony praw osób, których dane dotyczą
8. Przeprowadzenie PIA jest obowiązkowe zawsze, gdy:

9.1. ze względu na swój charakter, zakres, kontekst i cele, przetwarzanie danych może z dużym prawdopodobieństwem powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych,

9.2. dany rodzaj przetwarzania został wskazany w wykazie ustanowionym przez organ nadzorczy jako podlegający wymogowi dokonana oceny.

9. W przypadkach, gdy przeprowadzenie oceny skutków nie jest wyraźnie wymagane przepisami prawa, Administrator Danych ze względu na jej przydatność dla celów zapewnienia rozliczalności powinien ją zrealizować. Procedura ta:

10.1. może pomóc Administratorowi Danych w zapewnieniu zgodności z prawem ochrony danych;

10.2. stanowi dowód, że Administrator Danych podjął odpowiednie środki w celu dostosowywania swojej działalności do wymogów RODO;

10.3. pomaga Administratorowi danych poznać słabe strony planowanego procesu;

10.4. sprawia, że działania Administratora Danych są bardziej transparentne, co może prowadzić do zwiększenia zaufania wśród osób, których dotyczy planowany proces (pracownicy, klienci, kontrahenci);

10.5. jest jedną z metod zwiększania świadomości ochrony danych osobowych wśród pracowników zaangażowanych w planowaną operację przetwarzania.

10. W celu przeprowadzenie PIA Administrator Danych wypełnia Szablon oceny skutków ochrony danych osobowych.

11. Administrator Danych dokonując oceny uwzględnia co najmniej:

12.1. opis procesu przetwarzania danych osobowych (operacja i cele przetwarzania),

12.2. ocenę niezbędność i proporcjonalność tego przetwarzania (przedstawienie uzasadnionego interesu realizowanego przez Administratora),

12.3. ocenę ryzyka naruszenia praw lub wolności osób fizycznych,

12.4. wykaz środków, mających zaradzić temu ryzyku (zabezpieczenia oraz środki i mechanizmy bezpieczeństwa).

12. Po przeprowadzeniu PIA, Administrator Danych sporządza Raport, na który składają się:

    13.1. strona tytułowa (*informacje*: nazwa i adres Administratora Danych, nazwa planowanej operacji przetwarzania, komórka odpowiedzialna za przeprowadzenie PIA, osoba kontaktowa, wersja raportu, data sporządzenia raportu),

    13.2. wstęp (*informacje*: dlaczego PIA została przeprowadzona, kiedy została przeprowadzona, kto był zaangażowany w przeprowadzenie oceny, zwięzły opis planowanej operacji, ewentualne nawiązanie do dokumentacji ochrony danych osobowych obowiązującej w organizacji),

    13.3. ocena skutków dla ochrony danych osobowych (*informacje*: szczegółowy opis procesu, zakres i cel przetwarzania danych osobowych, sposób zbierania danych, kwestie związane z przekazywaniem danych, uprzednie konsultacje z osobami zainteresowanymi, stosowane środki przetwarzania oraz zabezpieczenia organizacyjne i techniczne, potencjalne zachowania powodujące ryzyko, analiza ryzyka, plan naprawczy),

    13.4. podsumowanie i wyniki przeprowadzonej oceny (*informacje*: końcowe wnioski z przeprowadzonej oceny skutków).

13. W sytuacji, w której przeprowadzona ocena wykaże, że przetwarzanie danych powodowałoby wysokie ryzyko, gdyby Administrator Danych nie zastosował środków w celu zminimalizowania ryzyka to przed rozpoczęciem przetwarzania, konsultuje się z organem nadzoru w trybie art. 36 RODO.

14. Po przeprowadzonej ocenie skutków Administrator Danych, przy pomocy IOD, jeśli jest wyznaczony lub innego podmiotu monitoruje na bieżąco realizacje planowanej operacji przetwarzania, aby upewnić się czy nie występuje nowe ryzyko naruszenia praw i wolności.

pola oznaczone na pomarańczowo uzupełnia osoba odpowiedzialna (od strony merytorycznej) za planowaną operację przetwarzania

pola oznaczone na niebiesko uzupełnia IOD

WZORCOWY MOŻLIWY DO ZASTOSOWANIA SZABLON OCENY SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH		
LP	**ZAGADNIENIE**	**ODPOWIEDŹ**
1.	**Osoba(-y) odpowiedzialna za planowaną operację przetwarzania** *Formularz powinien być uzupełniony przez osobę (osoby) posiadającą wiedzę na temat planowanej operacji przetwarzania.*	**Imię i nazwisko:** **Stanowisko:**
2.	**Inspektor Ochrony Danych**	**Imię i nazwisko:**
3.	**Przetwarzanie danych osobowych** *Jeśli odpowiedź na pytanie brzmi NIE – uzupełnianie niniejszego formularza jest zbędne.*	Czy planowana operacja wiąże się z przetwarzaniem danych osobowych? ☐ tak ☐ nie
4.	**Szczegółowy opis planowanej operacji przetwarzania**	

	Należy zidentyfikować planowany proces. Na czym polega? Jaki jest cel jego wdrożenia? *Dlaczego wprowadzane są zmiany do już istniejącego procesu? Czy wdrożenie planowanego procesu podyktowane jest potrzebą biznesową czy wynika z przepisów prawa? Jak najbardziej wyczerpująco*	
5.	**Wstępna analiza** *Należy ocenić czy przeprowadzenie PIA jest obowiązkowe.* *Czy w ramach planowanej operacji przetwarzania:* • *dochodzi do profilowania?* • *przetwarzane są na dużą skalę szczególne kategorie danych lub dane dotyczące wyroków skazujących i naruszeń prawa?* • *dochodzi do systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie?* • *wprowadzana jest nowa technologia*	

	związana z przetwarzaniem danych? *Czy planowana operacja przetwarzania jest uwzględniona w wykazie organu nadzorczego opisującym rodzaje operacji przetwarzania podlegające wymogowi dokonania PIA?*	
6.	**Zakres danych osobowych przetwarzanych w ramach planowanego rozwiązania** *Jaki rodzaj danych będzie przetwarzany? Czy przetwarzane będą szczególne kategorie danych lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa?*	Proszę opisać jakie dane będą przetwarzane:
		Czy przetwarzane dane będą ujawniać: ☐ pochodzenie rasowe lub etniczne ☐ poglądy polityczne ☐ przekonania religijne lub światopoglądowe ☐ przynależność do związków zawodowych ☐ dane genetyczne ☐ dane biometryczne ☐ dane dotyczące zdrowia ☐ seksualność lub orientację seksualną Czy będą przetwarzane dane dotyczące: ☐ wyroków skazujących

		□ naruszeń prawa
7.	**Cel przetwarzania danych osobowych** *Dlaczego dane osobowe będą zbierane?*	
8.	**Sposób zbierania danych osobowych** *W jaki sposób dane będą pozyskiwane?*	Proszę opisać w jaki sposób dane będą pozyskiwane:
		Czy: □ dane będą zbierane bezpośrednio od osób, których dane dotyczą □ istnieje konieczność korzystania z zewn. baz danych □ dane będą zbierane w wersji papierowej □ dane będą zbierane z wykorzystaniem systemu informatycznego
9.	**Kategorie osób, których dane dotyczą** *Czyje dane osobowe będą przetwarzane?*	Czy planowana operacja przetwarzania wiąże się z przetwarzaniem danych: □ pracowników □ klientów □ kontrahentów □ innych osób
		Jeżeli zaznaczono checkbox „innych osób”, proszę o

		doprecyzowanie jakie to osoby:
10.	**Podstawa przetwarzania danych osobowych** *Czy dane będą przetwarzane:* • *na podstawie zgody* • *w związku z koniecznością wykonania umowy* • *w związku z obowiązkiem prawnym ciążącym na Administratorze danych* • *na podstawie prawnie uzasadnionego interesu* • *inna podstawa.*	
11.	**Przekazywanie danych** *Czy dane są przekazywane innym podmiotom? W jakim celu są im przekazywane? Czy dochodzi do powierzania przetwarzania danych osobowych? Czy dane przekazywane są do państwa trzeciego?*	Czy dane przekazywane są (lub mogą być przekazywane): ☐ wewnątrz organizacji ☐ podmiotom zewnętrznym ☐ za granicę
		Jeżeli dane są przekazywane, proszę wskazać (o ile to możliwie) dokładne komórki organizacyjne, podmioty zewnętrzne lub kraje, do których dane są przekazywane. Proszę również

		wskazać cel takiego przekazywania danych.
12.	**Powierzenie danych osobowych – analiza**	
13.	**Udostępnianie danych osobowych – analiza**	
14.	**Uprzednie konsultacje z uczestnikami procesu (stronami zainteresowanymi)** *Na kogo przetwarzanie danych może mieć realny wpływ?* * *Przeprowadzenie konsultacji można zrealizować np. poprzez przeprowadzenie ankiety.*	
15.	**Środki, za pomocą których dochodzi do przetwarzania danych osobowych** *W jaki sposób dane są przetwarzane?*	Czy do przetwarzania danych osobowych wykorzystywane są: ☐ hardware (komputery, routery, smartfony, tablety) ☐ software (systemy informatyczne, programy pocztowe, aplikacje, oprogramowanie) ☐ sieć (kablowa, wi-fi, światłowód) ☐ dokumenty papierowe (wydruki, kopie) ☐ kanały przesyłania dokumentów (fax, e-mail, poczta tradycyjna) ☐ inne środki

		Proszę o wyszczególnienie / opisanie środków, wykorzystywanych do przetwarzania danych osobowych.
16.	**Zabezpieczenia organizacyjne** *Jakie są procedury: wykonywania kopii zapasowych, odzyskiwania danych,*	
17.	**Zabezpieczenia techniczne** *W jaki sposób dane są zabezpieczane? Czy stosuje się kontrolę dostępu? W jaki sposób dochodzi do uwierzytelnienia użytkownika?*	
18.	**Retencja danych** *Przez jaki okres dane będą przetwarzane? Jakie są kryteria ustalania okresu przetwarzania danych?*	
19.	**Przestrzeganie zasad** *Czy przetwarzanie danych następuje zgodnie z ogólnymi zasadami przetwarzania danych osobowych (tj. zasadą legalności, rzetelności, przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania, integralności i poufności)*	

20.	**Prawa osób, których dane dotyczą** *Czy specyfika planowanej operacji przetwarzania umożliwia osobom, których dane dotyczą realizację ich praw.*	
21.	**Identyfikacja źródeł ryzyka** *Jakie są potencjalne zachowania mogące mieć negatywny wpływ na przetwarzane dane? Np. nieumiejętna obsługa ustawień bezpieczeństwa/ prywatności, utrata urządzenia, niewłaściwe użycie, nieuzasadniony okres przechowywania danych*	
22.	**Analiza ryzyka** *Szacowanie prawdopodobieństwa wystąpienia ryzyka oraz powagi tego ryzyka. Ocena potencjalnych skutków dla praw i wolności osób, których dane dotyczą.*	
23.	**Plan naprawczy** *Opisanie środków przewidziane w celu:* *- zaradzenia ryzyku bądź jego zminimalizowania*	

	- przestrzegania rozporządzania	
24.	**Reguły kontrolne** *Ustalenie zasad aktualizacji przeprowadzonej oceny skutków*	

Załączniki:

1. …
2. …

……
…

Data i podpis osoby odpowiedzialnej za planowaną operację przetwarzania

……
…

Data i podpis Inspektora Ochrony Danych