**ZAŁĄCZNIK 1**

**Formularz szablonu oceny skutków dla prywatności danych**

Część A: Wprowadzenie

Definicje terminów używanych w tym Załączniku 1 podane są w dołączonej do niego Części E (*Glosariuszu*).

Część B zawiera schemat poglądowy Procesu DPIA. W Części C zawarte są pewne pytania wstępne, pomagające ustalić charakter Projektu i stwierdzić, czy DPIA jest konieczna („**Informacja wstępna**”). Część D to formularz DPIA, który zawiera szereg pytań dotyczących proponowanego Projektu i proponowanego w jego ramach stosowania danych osobowych („**Formularz DPIA**”).

*Zastrzeżenie:* Formularz DPIA nie dotyczy sytuacji, w której administrator musi skonsultować się z organem nadzorczym ds. ochrony danych. Takim przypadkiem powinien kierować **Dział prawny**.

Część B Przegląd Procesu DPIA

Część C: Pytania wstępne w celu ustalenia, czy DPIA jest konieczna oraz, jeśli jest, jak przeprowadzić DPIA („Informacja wstępna”)

**Ogólne informacje o projekcie**

|  |  |
| --- | --- |
| **Pytanie** | **Odpowiedź** |
| **[*Właściwy podmiot HES*]** proszący o Projekt/podejmujący się Projektu. |  |
| Dane lidera projektu | Imię i nazwisko:  Stanowisko:  Telefon:  E-mail: |
| Czy projekt obejmuje Przetwarzanie Danych osobowych? Jeśli nie, nie ma potrzeby dalszych działań. Proszę przesłać ten formularz lokalnemu specjaliście ds. zgodności w celu oceny i zatwierdzenia. |  |
| Proszę opisać możliwie najbardziej szczegółowo w jaki sposób Projekt będzie obejmować Przetwarzanie Danych osobowych. |  |
| Czy HES będzie Przetwarzać Dane osobowe jako Administrator danych lub Podmiot przetwarzający? W każdym przypadku proszę wyjaśnić dlaczego. |  |
| Jaki jest cel Projektu? |  |
| Jakie są korzyści dla HES? |  |
| Jakie są potencjalne korzyści dla innych stron (w tym klientów HES i osób, których to dotyczy, w mającym zastosowanie zakresie)? |  |
| Czy istnieją dokumenty istotne dla Projektu, takie jak propozycje projektu, które mogłyby być przydatne na użytek DPIA (np. opisujące w jaki sposób stosowane będą dane osobowe)? Jeśli tak, proszę je wymienić i dołączyć do tego Formularza. |  |
| Do kiedy Projekt powinien zostać wdrożony? |  |

**Projekt i Dane osobowe**

|  |  |  |
| --- | --- | --- |
| **Pytanie** | **Tak/Nie** | **Ryzyko dla prywatności** |
| Czy Projekt obejmuje zbieranie Danych osobowych o osobach fizycznych? |  | Niskie-średnie |
| Czy Projekt będzie wymagać od osób fizycznych podania informacji na ich temat w celu świadczenia usługi przetwarzania, lub czy będzie to dobrowolne? |  | Średnie |
| W jaki sposób osoby fizyczne będą zawiadamiane/informowane? |  | Średnie |
| Czy Dane osobowe będą ujawniane lub przechowywane w obrębie organizacji HES lub osób trzecich w sposób, w jaki wcześniej tego nie robiono? |  | Średnie |
| Czy Dane osobowe będą stosowane w nowym lub innym celu? |  | Niskie-średnie |
| Czy Projekt obejmuje wykorzystanie nowych technologii? |  | Średnie-Wysokie |
| Czy Projekt spowoduje podejmowanie decyzji lub działań przeciwko osobom fizycznym na takie sposoby, jakie mogłyby odnieść dla tych osób znaczący skutek (np. profilowanie)? |  | Wysokie |
| Czy Projekt będzie obejmować jakiekolwiek zautomatyzowane procesy podejmowania decyzji lub profilowanie osób fizycznych? |  | Wysokie |
| Czy Projekt będzie obejmować Przetwarzanie Danych osobowych na masową skalę? |  | Średnie-Wysokie |
| Czy Projekt będzie obejmować Przetwarzanie na masową skalę specjalnych kategorii danych lub danych dotyczących wyroków skazujących i naruszeń prawa? |  | Wysokie |
| Czy będzie prowadzone transgraniczne Przetwarzanie? |  | Wysokie |

**Podsumowanie**

|  |  |
| --- | --- |
| **Pytanie** | **T/N** |
| Czy na podstawie powyższych informacji i odpowiedzi wydaje się, że jest prawdopodobne, że Przetwarzanie Danych osobowych stworzy wysokie ryzyko dla osób, których dane dotyczą lub stanowi ryzykowną czynność przetwarzania? |  |
| Jeśli odpowiedź na powyższe pytanie brzmi nie, proszę podać tutaj szczegółowe powody tego wniosku oraz przekazać ten formularz lokalnemu specjaliście ds. zgodności w celu zatwierdzenia. |  |
| Jeśli odpowiedź brzmi tak, proszę przejść do następnej części. |  |

Część D: Formularz oceny skutków dla prywatności danych („Formularz DPIA”)

| Nr | **Pytanie** | **Odpowiedź** |
| --- | --- | --- |
| Dane osobowe | | |
|  | Jakie dane osobowe będą zbierane? (proszę zakreślić w kółko odpowiednio T/N) | Imię i nazwisko: T / N  Adres: T / N  Data urodzenia: T / N  Pochodzenie rasowe lub etniczne: T / N  Stan cywilny: T / N  Informacje o rodzinie i związku: T / N  Wyznanie: T / N  Informacje zdrowotne: T / N  Orientacja seksualna: T / N  Poglądy polityczne: T / N  Dane genetyczne: T / N  Informacje o wyrokach skazujących: T / N  Informacje o cechach fizycznych (wzrost, waga itp.): T / N  Numer karty kredytowej/rachunku bankowego: T / N  Informacje o stanie posiadania (samochody, domy, mieszkania, mienie osobiste): T / N  Historia kredytowa: T / N  Informacje o sieciach społecznościowych: T / N  Inne (proszę sprecyzować): T / N |
|  | W jaki sposób są zbierane? |  |
|  | Na czym polega czynność Przetwarzania? |  |
|  | Czy Przetwarzanie jest konieczne lub czy czynność można by wykonywać w inny sposób? |  |
|  | Czy Projekt nadal można by było z powodzeniem przeprowadzić bez zbierania niektórych lub wszystkich tych Danych osobowych? |  |
|  | O kim Dane osobowe mogłyby być zbierane/Przetwarzane? (proszę zakreślić w kółko odpowiednio T/N) | Pracownicy: T / N  Osoby niebędące pracownikami: T / N  W przypadku osób niebędących pracownikami proszę podać kto (klienci, sprzedawcy, inne osoby trzecie itp.): |
|  | W jakim konkretnym celu Dane osobowe będą Przetwarzane (np. do prowadzenia nowego wykonanego na zamówienie portalu świadczeń pracowniczych)? Proszę opisać możliwie szczegółowo dlaczego dane są przetwarzane. |  |
|  | Jak długo Dane osobowe będą przechowywane? |  |
| Podstawa prawna | | |
|  | Czy Dane osobowe będą Przetwarzane na podstawie zgody wyrażonej przez osoby, których dane dotyczą? Jeśli tak, w jaki sposób zgoda jest uzyskiwana? |  |
|  | Czy Dane osobowe będą Przetwarzane w ramach wykonywania umowy z odpowiednimi Osobami, których dane dotyczą? |  |
|  | Czy Dane osobowe będą Przetwarzane ze względu na prawnie uzasadnione interesy biznesowe HES (np. wewnętrznej administracji HR)? |  |
|  | Czy Dane osobowe będą Przetwarzane na podstawie innego prawnego uzasadnienia (patrz Część F, w której znajduje się wykaz legalnych uzasadnień)? |  |
| Przepływy danych | | |
|  | Po zebraniu Danych osobowych od Osób, których dane dotyczą, gdzie dane te będą przechowywane? |  |
|  | Kto będzie mieć dostęp do Danych osobowych? |  |
|  | Czy sporządzane będą sprawozdania wymagające stosowania i ujawniania Danych osobowych? |  |
|  | Czy Dane osobowe będą przekazywane jakiemukolwiek podmiotowi spoza HES? Jeśli tak, któremu podmiotowi i w jakich celach? |  |
|  | Czy Dane osobowe będą przekazywane do jakichkolwiek państw poza Europejskim Obszarem Gospodarczym lub czy będą do nich mieć dostęp osoby spoza EOG? |  |
|  | Czy podjęto się mapowania Danych osobowych? |  |
|  | Jeśli odpowiedź na (18) brzmi „Tak”, dostarczyć mapę Danych osobowych ilustrującą przepływy Danych osobowych w ramach tego Projektu (zawierającą typ danych osobowych, podmioty, pomiędzy którymi dane są dzielone, lokalizacje tych podmiotów oraz miejsca przechowywania). |  |
|  | Jak długo Dane osobowe będą przechowywane? |  |
| Wymagania dotyczące konsultacji | | |
|  | Z kim w obrębie przedsiębiorstwa skonsultujesz się w sprawie związanego z Projektem ryzyka dla prywatności i bezpieczeństwa? |  |
|  | Czy zasięgnąłeś(-aś) porady lokalnego specjalisty ds. zgodności, Chief Compliance Officer lub działu prawnego? |  |
|  | Czy trzeba skonsultować się z radą pracowników lub innymi organami pracowniczymi (w przypadku, gdy dotyczy HR/danych pracowników)? |  |
|  | Jeśli występuje przekazywanie transgraniczne, czy potrzebne jest szczegółowe opisanie akceptacji ze strony innego porządku prawnego? |  |
|  | Jeśli odpowiedzi na powyższe (23) lub (24) brzmią „Tak”, czy podjąłeś(-aś) odpowiednie konsultacje z właściwymi osobami? Proszę potwierdzić tutaj i podać szczegóły konsultacji: z kim i daty. |  |
| Identyfikacja ryzyka | | |
|  | Jakie, jeśli w ogóle, stwierdziłeś(-aś) konkretne problemy dotyczące prywatności na podstawie powyższych odpowiedzi? Na przykład ryzyko, że do Danych osobowych będzie mieć dostęp osoba nieupoważniona, na przykład:   * ryzyko, że dojdzie do naruszenia bezpieczeństwa danych osobowych; * ryzyko, że osoby fizyczne sprzeciwią się przetwarzaniu, jeśli zostaną poinformowane; * ryzyko, że nie zostanie utrzymana dokładność danych; * ryzyko, że dane osobowe będą przechowywane dłużej niż jest to konieczne. |  |
|  | Jakie są konkretne szkody, którymi grozi takie ryzyko dla osób fizycznych (np. ryzyko, że Dane osobowe zostaną skradzione, co spowoduje, że odpowiednie osoby fizyczne będą narażone na oszustwo i kradzież tożsamości)? |  |
|  | Czy występuje konkretne ryzyko braku zgodności? |  |
|  | Czy występuje szersze ryzyko organizacyjne (np. wysokie kary na skutek naruszenia i następnie niekorzystne doniesienia w mediach)? |  |
| Działania i środki w celu zabezpieczenia i ochrony Danych osobowych | | |
|  | Jakie środki będą stosowane w celu zabezpieczenia i ochrony Danych osobowych (np. szyfrowanie, uwierzytelnianie wielopoziomowe) w odniesieniu do każdego zidentyfikowanego powyżej ryzyka? |  |
|  | W odniesieniu do każdego zidentyfikowanego powyżej ryzyka - w jaki sposób będziemy umożliwiać wykonywanie Osobom, których dane dotyczą, ich praw (np. prawa dostępu)? |  |
|  | W jaki sposób odpowiednie informacje na temat Projektu i związanego z nim ryzyka dla prywatności będą komunikowane Osobom, których dane dotyczą? |  |
|  | Czy działania te w całości wyeliminują albo po prostu zminimalizują ryzyko? |  |
|  | Biorąc pod uwagę zidentyfikowane ryzyko i proponowane rozwiązania w celu jego minimalizacji, czy ostateczny skutek dla praw związanych z prywatnością Osób, których dane dotyczą, uznaje się za akceptowalny w świetle celów i korzyści Projektu? |  |
| Włączenie rezultatów i środków w celu wyeliminowania/zminimalizowania zidentyfikowanego ryzyka | | |
|  | W jaki sposób te rezultaty zostaną włączone do Projektu? |  |
|  | Kto będzie odpowiadać za prawidłowe włączenie tych rezultatów? |  |
|  | Do kiedy? |  |
|  | Jak wygląda proces przewidziany dla Osób, których dane dotyczą, które chcą omówić swoje obawy związane z prywatnością i Projektem? |  |

**Podsumowanie**

|  |  |
| --- | --- |
| **Pytanie** | **T/N** |
| Czy zidentyfikowane ryzyko zostało wyeliminowane, zredukowane lub zaakceptowane? |  |
| Jeśli nie, nie można rozpocząć przetwarzania dopóki DPIA nie zostanie przekazana [•] i nie będą mogły zostać wprowadzone odpowiednie środki. |  |

|  |  |
| --- | --- |
| **Akceptacja i zatwierdzenie/odmowa** | |
| **Lider projektu** | |
| Imię i nazwisko |  |
| Stanowisko |  |
| Podpis |  |
| Data |  |
| **Przedstawiciel zespołu ds. zgodności (jeśli dotyczy)** | |
| Imię i nazwisko |  |
| Stanowisko |  |
| Podpis |  |
| Data |  |
|  |  |

|  |  |
| --- | --- |
| **Wskazanie lokalnego specjalisty ds. zgodności** | |
| Imię i nazwisko |  |
| Data |  |
| Odpowiedź |  |
| Wyjaśnienie (jeśli dotyczy) |  |
| Podpis |  |

Część E

**Glosariusz**

|  |  |
| --- | --- |
| **Termin** | **Definicja** |
| RODO: | Ogólne rozporządzenie o ochronie danych osobowych, które weszło w życie 25 maja 2018 r. RODO dotyczy wyłącznie Danych osobowych, nie obejmuje Danych osobowych związanych z przedsiębiorstwami lub innymi nieżyjącymi osobami. |
| Administrator danych: | Spółka, która określa cele i środki Przetwarzania Danych osobowych. |
| Podmiot przetwarzający: | Spółka, która przetwarza Dane osobowe w imieniu Administratora. |
| Lokalny specjalista ds. zgodności | Osoba w obrębie podmiotu HES, która jest odpowiedzialna za Oceny skutków dla prywatności danych. |
| Dane osobowe: | Wszystkie informacje dotyczące zidentyfikowanych osób fizycznych. Przykłady Danych osobowych: |
| A. Nazwisko (takie jak pełne imię i nazwisko, nazwisko panieńskie lub przydomek). |
| B. Osobisty numer identyfikacyjny (taki jak krajowy numer ubezpieczenia, numer paszportu, numer prawa jazdy oraz numer rachunku bankowego lub karty kredytowej). |
| C. Dane adresowe (takie jak adres pocztowy lub e-mail). |
| D. Informacje o zasobach (takie jak adres protokołu internetowego (IP) lub MAC). |
| E. Numery telefonów (w tym numery telefonów komórkowych). |
| F. Cechy osobiste, w tym zdjęcia (np. twarzy), zdjęcia RTG, odciski palców lub inne obrazy biometryczne / wzory danych osobowych (np. skan siatkówki, podpis głosowy, geometria twarzy). |
| G. Informacje identyfikujące majątek osobisty (takie jak numer rejestracyjny pojazdu i informacje powiązane). |
| H. Informacje o osobie fizycznej, które są połączone lub możliwe do połączenia z powyższymi (np. data urodzenia, miejsce urodzenia, rasa, wyznanie, działalność, wskaźniki geograficzne, informacje o zatrudnieniu lub edukacji, informacje medyczne lub finansowe). |
| I. Pozornie błahe informacje, takie jak fakt, że osoba wysłała e-mail o określonym czasie, lub fakt, że osoba jest pracownikiem klienta HES (lub innej organizacji); |
| J. Opinie o osobie (takie jak opinie wyrażane przez osobę udzielającą referencji lub wyrażone w ocenie). |
| Przetwarzanie: | Niemal wszystkie czynności wykonywane w odniesieniu do Danych osobowych, w tym: |
| A. zbieranie, przechowywanie i utrwalanie; |
| B. organizowanie lub porządkowanie; |
| C. adaptowanie lub modyfikowanie; |
| D. pobieranie, przeglądanie lub stosowanie; |
| E. ujawnianie lub rozpowszechnianie; |
| F. dopasowywanie lub łączenie; oraz |
| G. ograniczanie, usuwanie lub niszczenie. |

Część F

**Wykaz legalnych uzasadnień Przetwarzania**

* **Osoba fizyczna, której dotyczą Dane osobowe wyraziła zgodę na Przetwarzanie.**
* Zgoda musi być wyraźna, świadoma i dobrowolna. Osoba fizyczna musi mieć możliwość wycofania udzielonej zgody. Więcej informacji na temat zgody - patrz Polityka prywatności HES.
* **Przetwarzanie jest niezbędne:**
  + w związku z umową, którą osoba fizyczna zawarła; lub
  + ponieważ osoba fizyczna poprosiła o zrobienie czegoś, aby mogła zawrzeć umowę.
* **Przetwarzanie jest niezbędne z powodu spoczywającego na tobie obowiązku prawnego (z wyjątkiem obowiązku wynikającego z umowy).**
* Na przykład, dane należy zachować w celu spełnienia wymagań regulacyjnych, wymagań sprawozdawczości finansowej lub przepisów z obszaru przeciwdziałania przekupstwu i korupcji.
* **Przetwarzanie jest niezbędne w celu ochrony „żywotnych interesów” osoby fizycznej.**
  + Ten warunek ma zastosowanie jedynie w przypadku, gdy chodzi o życie lub śmierć, np. gdy historia medyczna osoby fizycznej jest ujawniana szpitalowi, w którym osoba ta jest leczona po poważnym wypadku drogowym.
* **Przetwarzanie spełnia warunek „prawnie uzasadnionego interesu”.**
* Prawnie uzasadnione interesy stanowią najbardziej elastyczną podstawę prawną przetwarzania, ale nie wolno wychodzić z założenia, że zawsze będzie właściwa.
* Będzie ona najbardziej odpowiednia, gdy stosujesz dane w sposób, którego osoby, których dane dotyczą, mogą się racjonalnie spodziewać i który ma minimalny skutek dla prywatności, lub gdy istnieje ważne uzasadnienie dla przetwarzania.
* Prawnie uzasadniony interes składa się z trzech elementów. Pomocne jest traktowanie tego jako trzyczęściowego testu. Musisz: (i) zidentyfikować prawnie uzasadniony interes; (ii) wykazać, że przetwarzanie jest niezbędne w celu jego realizacji; i (iii) wyważyć go względem interesów osoby fizycznej, jej praw i wolności.
* Prawnie uzasadnione interesy mogą być interesami twoimi lub osób trzecich. Mogą obejmować interesy handlowe, indywidualne lub szersze korzyści społeczne. Przetwarzanie musi być niezbędne. Jeśli możesz osiągnąć ten sam skutek w mniej natarczywy sposób, prawnie uzasadnione interesy nie będą mieć zastosowania.