|  |  |  |
| --- | --- | --- |
| Ocena skutków przetwarzania nr [•] z dn. [•] | | |
| Nazwa procesu: | [Np.:   * „Rekrutacja do programu XYZ”.] | |
| Nowy proces / / aktualizacja oceny: | [„Nowy proces” lub „aktualizacja oceny skutków przetwarzania nr [•] z dn. [•].”] | |
| Opis planowanych operacji przetwarzania: | [Np.:   * „zebranie i utrwalenie danych przekazywanych przez kandydata do programu prowadzonego przez Fundację (kwestionariuszy, innych dokumentów), przeglądanie i wykorzystanie tych danych przez osobę upoważnioną na potrzeby dokonania oceny kandydata, przechowywanie danych przez okres retencji zgodnie z wymogami programu”, itp.] | |
| Kategorie podmiotów danych: | [Np.:   * „kandydaci do programu XYZ”, * „osoby wchodzące i wychodzące z pomieszczeń biurowych wykorzystywanych na potrzeby siedziby Fundacji”, * „użytkownicy systemów IT Fundacji”, * „pracownicy i współpracownicy Fundacji”, itp.] | |
| Cel przetwarzania: | [Np.:   * „dokonanie oceny kwalifikacyjnej kandydata do programu XYZ”, * „ustalenie, dochodzenie i obrona roszczeń Fundacji”, itp.] | |
| Podstawa prawna: | [Podstawa prawna w rozumieniu art. 6 ust. 1 lub art. 9 ust. 2 RODO, np.:   * „zgoda podmiotu danych – art. 6 ust. 1 lit. a) RODO”, względnie „art. 9 ust. 2 lit. a) RODO”, * „wymóg prawny – art. 6 ust. 1 lit. c) RODO; obowiązek prawny ciążący na Fundacji na podst. [•]”, * „uzasadniony interes Fundacji – art. 6 ust. 1 lit. f) RODO; ustalanie, dochodzenie i obrona roszczeń (w sposób przeważający nad interesem podmiotu danych w ich nieprzetwarzaniu)”, itp.] | |
| Ocena niezbędności i proporcjonalności: | [Oceniając operacje przetwarzania, Fundacja musi zweryfikować, czy planowane czynności są adekwatne i stosowne względem wyznaczonych celów, oraz czy ich podjęcie nie jest nadmiarowe w relacji do tych celów.  Ocena, czy operacje przetwarzania są niezbędne oraz proporcjonalne do celu przetwarzania, powinna zawierać:   1. ustalenie, jakie dane są niezbędne do realizacji celu, 2. wskazanie, jakie dane będą podlegać planowanym operacjom przetwarzania, 3. stwierdzenie, czy wszystkie dane, które mają podlegać planowanym operacjom przetwarzania, są do realizacji celu niezbędne (stwierdzenie, czy z procesu wyeliminowano dane zbędne i nadmiarowe), 4. ustalenie, jakie operacje przetwarzania są niezbędne do prawidłowego przetwarzania tych danych w świetle celu, 5. wskazanie, jakie operacje przetwarzania będą wykonywane (patrz opis powyżej), 6. stwierdzenie, czy wszystkie poszczególne operacje przetwarzania, które mają być wykonywane, są do realizacji celu niezbędne, i czy realizacji tego celu nie można osiągnąć za pomocą środków mniej ingerujących w prywatność jednostki.] | |
| Ocena ryzyka naruszenia praw i wolności podmiotu danych | [Oceniając ryzyko naruszenia praw i wolności osób, których dane dotyczą, Fundacja musi rozważyć możliwie pełne spektrum faktycznych oraz prawnych zagrożeń wynikających dla tych osób z przetwarzania ich danych, wybierając metodę top‑down/bottom-up lub ich kombinację wg. zasadności danej metodyki. Ocena powinna uwzględniać ryzyka nie tylko w toku prawidłowego, ale także nieprawidłowego przebiegu procesu przetwarzania, także z udziałem podmiotów trzecich (tak upoważnionych – np. powierzenie przetwarzania – jak i nieupoważnionych).  Ustalenia powinny móc sprowadzić się do jednej z następujących, wzajemnie się wykluczających konkluzji, stanowiącej punkt wyjścia do określenia środków zaradczych:   * nie zidentyfikowano ryzyka naruszenia praw lub wolności osób, których dane dotyczą, * zidentyfikowano ryzyko, które nie zostało jednak uznane za wysokie, * zidentyfikowano ryzyko, które uznano za wysokie.] | |
| Obowiązek uprzedniej konsultacji z PUODO: | https://upload.wikimedia.org/wikipedia/commons/thumb/6/66/Znak_A-30.svg/80px-Znak_A-30.svg.png | [Jeśli ocena ryzyka wskaże, że przetwarzanie powodowałoby wysokie ryzyko (niezależnie od podjęcia środków w celu zminimalizowania tego ryzyka), przed rozpoczęciem przetwarzania Fundacja konsultuje się z organem nadzorczym.] |
| Planowane środki  zapobieżenia ryzyku oraz  wykazania zgodności: | [Określenie środków podejmowanych w celu zaradzenia ryzyku wiążącemu się z przetwarzaniem, w tym ryzykom wynikającym z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.  Wykazanie zastosowania zasady ochrony danych osobowych już w momencie projektowania procesu oraz zasady domyślnej ochrony danych osobowych.  Wyszczególnienie sposobu, w jaki środki te ukierunkowane są na respektowanie praw i wolności podmiotów danych, a także środków pozwalających udokumentować i wykazać zapewnioną zgodność, z uwzględnieniem:   * stanu wiedzy technicznej, * kosztu wdrożenia, * charakteru, zakresu, kontekstu i celów przetwarzania, * ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.   Do rozważenia przykładowe środki techniczne i organizacyjne:   * zabezpieczenia fizyczne i logiczne (ograniczenie i kontrola dostępu, CCTV), * środki ochrony kryptograficznej, szyfrowanie i pseudonimizacja, * środki ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, * wdrożenie procedur i instrukcji, szkolenia personelu, * bariery informacyjne („need-to-know-basis”, „Chinese wall”), itp.] | |
| Ocena ryzyka po zastosowaniu środków zapobieżenia ryzyku: | [Np.:  „Jak wykazały wyniki analiz, studium wykonalności oraz przeprowadzonych testów, planowane środki pozwolą na wyeliminowanie stwierdzonych ryzyk; należy zapewnić należytą kontrolę właściwego wdrożenia planowanych środków oraz dokonać audytu ich skuteczności po upływie miesiąca od wdrożenia, oraz dokonywać audytów okresowych w interwałach półrocznych.”, itp.] | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ za administratora danych osobowych Fundacja PO DRUGIE: [imię, nazwisko, funkcja]     \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Inspektor Ochrony Danych dla Fundacji PO DRUGIE: [imię, nazwisko] | | |