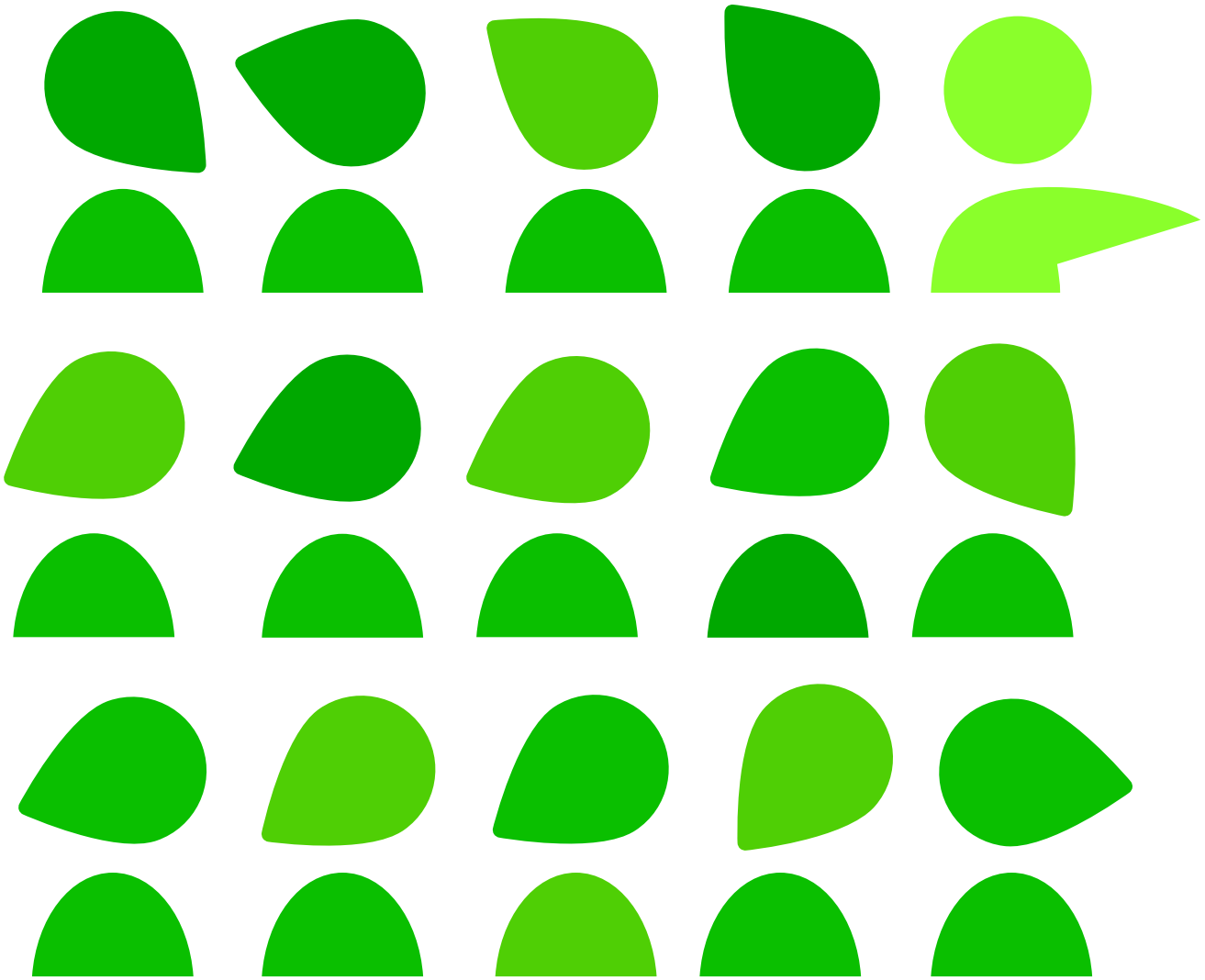
Katarzyna Sadło

Rady na rodo

Poradnik dla zespołów inkubatorów innowacji społecznych



Rady na RODO

Poradnik dla zespołów inkubatorów innowacji społecznych

Autorka: Katarzyna Sadło
Korekta i redakcja: Agata Błaszczyk
Opracowanie graficzne i skład: Studio Kotbury (www.kotbury.pl)
Wydawca: Fundacja Stocznia (www.stocznia.org.pl)
Warszawa, 2023
ISBN: 978-83-62590-51-3

Podręcznik powstał w ramach projektu „Katalizator Innowacji Społecznych" realizowanego przez Fundację Stocznia i Fundację Inicjatyw Społeczno-Ekonomicznych, współfinansowanego ze środków Europejskiego Funduszu Społecznego.

Spis treści

1. Wstęp

Celem poradnika jest wsparcie zespołów inkubatorów innowacji społecznych[1] **finansowanych z Europejskiego Funduszu Społecznego w realizacji obowiązków związanych z przetwarzaniem danych osobowych.** Obowiązki te wynikają z umowy o dofinansowanie[2] oraz ogólnych przepisów dotyczących przetwarzania danych osobowych, w tym przede wszystkim z RODO.

RODO to skrót od nazwy Rozporządzenie o ochronie danych osobowych, która z kolei jest skróconą nazwą Rozporządzenia 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).

RODO reguluje zasady przetwarzania danych osobowych, a wszystkie podmioty przetwarzające takie dane mają obowiązek dostosować do niego obowiązujące u siebie procedury. Ponieważ do dobrego zrozumienia naszego poradnika niezbędna jest znajomość logiki rozporządzenia, a wiemy, że nie zawsze jest to łatwe, przedstawiamy (przypominamy) jego najważniejsze założenia.

RODO gwarantuje osobom fizycznym maksymalną kontrolę nad ich danymi osobowymi, a podmiotom je przetwarzającym nakazuje zachowanie pełnej przejrzystości procesu przetwarzania danych i zapewnienie bezpieczeństwa stosownego do zidentyfikowanego ryzyka. To właśnie podmioty przetwarzające dane osobowe mają obowiązek przeanalizowania planowanych działań i określenia, czy i jakie dane osobowe będą niezbędne do ich przeprowadzenia, zapewnienia bezpieczeństwa tych danych oraz czytelnej komunikacji na ten temat z osobami, których dane dotyczą. Osoba będąca podmiotem danych (czyli, inaczej mówiąc, osoba, której te dane dotyczą) na każdym etapie ich przetwarzania ma prawo wiedzieć, kto przetwarza jej dane, w jakim celu, skąd je pozyskał i komu je udostępnia, jak długo

[1] W dalszej części poradnika, dla uproszczenia, posługujemy się terminem „inkubator".

[2] Poradnik przygotowaliśmy w oparciu o wzór umowy o dofinansowanie obowiązujący inkubatory działające w ramach Programu Operacyjnego Wiedza Edukacja Rozwój (w perspektywie finansowej 2014–2020). Przy kolejnej perspektywie poradnik zostanie zaktualizowany i dostosowany do nowych wytycznych.

zamierza je przechowywać, a także na jakiej podstawie prawnej je przetwarza. Wszystkie opisane w poradniku procedury i wzory dokumentów służą realizacji obowiązków podmiotu przetwarzającego dane osobowe oraz zagwarantowaniu praw przysługujących osobom, których dane są przetwarzane.

Z uwagi na obszerność tematu ochrony danych osobowych oraz fakt, że podmioty prowadzące inkubatory – podobnie jak wszystkie inne instytucje publiczne i prywatne – musiały już w 2018 roku wdrożyć u siebie RODO, **w poradniku skupiamy się głównie na tym obszarze ich działalności, który dotyczy inkubacji innowacji społecznych**. Zakładamy, że podstawowe dokumenty i procedury dotyczące pozostałych procesów przetwarzania danych już znają i stosują.

Przedstawione w poradniku propozycje rozwiązań celowo pozostają na pewnym poziomie ogólności. Ostateczne rozwiązania mogą być bowiem różne w poszczególnych inkubatorach, w zależności od specyfiki podmiotu prowadzącego dany inkubator oraz od procedur w nim obowiązujących. Nasze propozycje należy więc za każdym razem dostosować do konkretnego kontekstu.

W przypadku inkubatorów finansowanych z innych źródeł warunki realizacji działań będą się z pewnością różnić, a zatem inne będą ich obowiązki określone w umowach o dofinansowanie. Niemniej wydaje się, że większość informacji i wzorów dokumentów może być, po odpowiedniej adaptacji, stosowana także w takich przypadkach.

RODO często jest przedstawiane jako zbiór trudnych do wdrożenia przepisów komplikujących lub wręcz uniemożliwiających sprawne funkcjonowanie instytucji. Naszym zdaniem tak nie jest i mamy nadzieję, że w poradniku uda nam się wyjaśnić, jak rozumieć i realizować obowiązki związane z ochroną danych osobowych w taki sposób, by poradził sobie z tym każdy podmiot prowadzący inkubator. Zależy nam na pokazaniu, że proces przetwarzania danych osobowych jest logiczny i zrozumiały, a przede wszystkim pożyteczny z punktu widzenia praw i interesów osób, których dane przetwarzamy.

Kończąc ten wstęp i zapraszając do lektury poradnika, winni jesteśmy jeszcze jedną techniczno-językową uwagę. Ze względu na klarowność przekazu – zagadnienia, które omawiamy, same w sobie są dość skomplikowane – zrezygnowaliśmy z używania feminatywów, jednak za każdym razem, gdy piszemy na przykład o uczestnikach, to mamy oczywiście na myśli zarówno uczestników, jak i uczestniczki.

2. Podstawowe pojęcia dotyczące przetwarzania danych osobowych

Zanim przejdziemy do omówienia specyfiki przetwarzania danych osobowych w procesie inkubacji innowacji społecznych, chcemy przedstawić kluczowe pojęcia natury bardziej ogólnej. Będziemy się do nich odnosić w kolejnych częściach poradnika.

Dane osobowe – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, czyli takie, na podstawie których można bezpośrednio lub pośrednio ustalić tożsamość osoby, której te dane dotyczą. Definicja jest bardzo otwarta, orzecznictwo w niektórych przypadkach bywa sprzeczne, ale dla bezpieczeństwa najlepiej uznać, że każda informacja dotycząca osoby fizycznej, na podstawie której przypadkowy znalazca mógłby ustalić, kogo ona dotyczy, jest daną osobową. Informacji nie uznaje się za umożliwiającą ustalenie tożsamości osoby, jeśli wymagałoby to nadzwyczajnych nakładów środków.

Dane osobowe wrażliwe (w RODO zwane „szczególnymi kategoriami danych") – w przeciwieństwie do zwykłych danych osobowych, które w RODO są katalogiem otwartym, dane osobowe wrażliwe są bardzo ściśle określone i są to informacje ujawniające:

- pochodzenie rasowe lub etniczne,
- poglądy polityczne,
- przekonania religijne lub światopoglądowe,
- przynależność do związków zawodowych,
- dane genetyczne,
- dane biometryczne,
- dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Danymi wrażliwymi w rozumieniu RODO, wbrew powszechnej intuicji, nie są np. takie dane jak PESEL czy miejsce zamieszkania. Nie znaczy to oczywiście, że takie dane nie podlegają szczególnej ochronie, mogą być bowiem wykorzystane z dużą szkodą dla osoby, której dotyczą.

Dane biometryczne – to dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby. Dane biometryczne to na przykład wizerunek twarzy lub dane daktyloskopijne.

Dane dotyczące zdrowia – oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej (w tym o korzystaniu z usług opieki zdrowotnej) ujawniające informacje o stanie jej zdrowia.

Zbiór danych osobowych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany, rozproszony funkcjonalnie lub geograficznie. Przykładem zbioru danych jest zbiór danych pracowników, zbiór danych wolontariuszy, zbiór danych uczestników projektu. Nie ma tutaj znaczenia sposób przechowywania danych zawartych w zbiorze – mogą być one przechowywane w jednym miejscu lub podzielone i trzymane w różnych miejscach. Kluczowy jest fakt, że zbiór to pewien zestaw danych posiadających wspólny mianownik.

Przetwarzanie danych – każda operacja na danych osobowych, począwszy od gromadzenia, poprzez przechowywanie i pracę na danych, aż po usuwanie. Przetwarzanie, mimo technicznie brzmiącego terminu, nie musi odbywać się z wykorzystaniem komputera ani nawet być ustrukturyzowanym procesem. Samo przeglądanie danych jest już ich przetwarzaniem. Należy o tym pamiętać szczególnie w kontekście wydawania upoważnień do przetwarzania danych osobowych oraz zawierania umów powierzenia przetwarzania danych osobowych.

Operacje przetwarzania danych – każde działanie wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a także przeglądanie. Operacje przetwarzania danych osobowych to po prostu pojedyncze działania, które – jeśli są wykonywane w konkretnym wspólnym celu – stanowią czynność przetwarzania danych.

Oba terminy – operacje i czynności – są dość nieintuicyjne. W ich zrozumieniu może pomóc kuchenna analogia, w której odpowiednikiem czynności będzie gotowanie zupy, a odpowiednikiem operacji – obieranie, krojenie, przyprawianie, mieszanie.

Czynności przetwarzania danych – zespół powiązanych ze sobą operacji na danych wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy w związku z celem, w jakim te czynności są podejmowane. Dane z jednego zbioru mogą być przetwarzane w ramach różnych czynności przetwarzania danych.

Administrator – podmiot, który samodzielnie lub wspólnie ze współadministratorami ustala cele i sposoby przetwarzania danych osobowych.

Procesor (podmiot przetwarzający) – podmiot, który przetwarza dane osobowe w imieniu administratora na podstawie umowy powierzenia przetwarzania danych.

Podprocesor (podmiot podprzetwarzający) – podmiot, któremu procesor podpowierzył przetwarzanie danych, czyli, innymi słowy, podwykonawca podwykonawcy administratora.

Odbiorca – osoba fizyczna lub prawna, której ujawnia się dane osobowe. Definicja odbiorcy jest szeroka, obejmuje też procesorów, podprocesorów, a także inne podmioty, którym ujawniono lub zamierza się ujawnić dane osobowe. Odbiorcami danych są również podmioty, które na zlecenie podmiotu prowadzącego inkubator, Instytucji Zarządzającej lub innowatora uczestniczą w realizacji jakichś działań wymagających przetwarzania danych osobowych. Mogą to być np. podmioty realizujące badania ewaluacyjne na zlecenie Instytucji Zarządzającej lub podmiotu prowadzącego inkubator, specjalistyczne firmy przeprowadzające na zlecenie Instytucji Zarządzającej kontrole i audyt w ramach PO WER, a także podmioty świadczące na rzecz Instytucji Zarządzającej, podmiotu prowadzącego inkubator lub innowatora usługi związane z utrzymaniem i obsługą systemów teleinformatycznych. Odbiorcami danych nie są natomiast organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, czyli np. organy podatkowe, organy celne, organy ścigania itd.

Profilowanie – dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej. Profilowaniem będzie na przykład psychotest,

w którym na podstawie udzielonych odpowiedzi algorytm automatycznie ocenia, czy dana osoba ma zadatki na lidera. Nie jest natomiast profilowaniem w rozumieniu RODO dokonywanie takiej oceny przez człowieka. Nie spodziewamy się, aby w ramach inkubatorów profilowanie miało miejsce, ale ponieważ informacja o profilowaniu lub jego braku jest elementem klauzuli informacyjnej, należy to wiedzieć.

Pseudonimizacja – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie bez użycia dodatkowych informacji – pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są odpowiednio zabezpieczone przed nieuprawnionym dostępem. Pseudonimizacja jest jednym ze środków zabezpieczających dane. Będzie zatem stosowana szczególnie w przypadku danych, których niekontrolowane ujawnienie mogłoby wywołać znaczące szkody. Przykładem pseudonimizacji danych będzie np. nadanie uczestnikowi projektu numeru lub pseudonimu oraz przechowywanie w osobnym miejscu legendy umożliwiającej rozszyfrowanie pseudonimów. Pseudonimizacja, w przeciwieństwie do anonimizacji, znacząco utrudnia ustalenie tożsamości osoby, ale go nie uniemożliwia: aby skojarzyć dane z personaliami konkretnej osoby, wystarczy mieć dostęp do legendy.

Anonimizacja – przetworzenie danych w sposób trwale uniemożliwiający identyfikację osoby, której dane dotyczyły. Może być przydatna, gdy z jakichś względów (statystycznych czy archiwizacyjnych) chcemy zachować pewne informacje o danej osobie, ale nie potrzebujemy już jej personaliów – na przykład chcemy wiedzieć, jaki odsetek wśród osób, które skorzystały z naszych szkoleń, stanowią kobiety, ale nie są nam potrzebne ich nazwiska. Możemy wtedy zachować część opisową, charakterystykę osoby, ale trwale usunąć wszystkie informacje umożliwiające ustalenie jej tożsamości.

Naruszenie danych osobowych – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do przetwarzanych danych. Należy pamiętać, że termin jest dość nieintuicyjny i może być szerszy niż tak oczywiste naruszenie bezpieczeństwa jak ujawniony wyciek danych. Ponieważ zarówno w roli administratora, jak i w roli procesora danych (o tych funkcjach wspominamy niżej) mamy określone obowiązki raportowania naruszeń, w każdym przypadku należy

dobrze przeanalizować, czy doszło do naruszenia, a jeśli tak – ocenić jego skalę, charakter i możliwe skutki dla osoby, której dane dotyczą.

Ograniczenie przetwarzania danych – odpowiednie oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania. Osoba będąca podmiotem danych może w określonej sytuacji zażądać ograniczenia ich przetwarzania. Jeśli w danym przypadku to prawo faktycznie jej przysługuje, nie usuwamy jej danych, ale oznaczamy je (np. w bazie danych) w taki sposób, by nie mogły być na nich wykonywane żadne operacje (poza tymi dokonywanymi na żądanie tej osoby) i by było jasne, że te dane są jedynie przechowywane.

Zgoda na przetwarzanie – konkretne, świadome, jednoznaczne i dobrowolne okazanie przyzwolenia na przetwarzanie danych osobowych osoby udzielającej takiej zgody. W inkubatorze zgoda jest podstawą przetwarzania danych głównie w następujących przypadkach: w związku z rekrutacją, gdy przetwarzane są dane pomysłodawców (a także w innych procesach rekrutacyjnych, np. personelu, ekspertów, uczestników), w przypadku przetwarzania wizerunku (pracowników, innowatorów, uczestników testowania) w celach promocji i upowszechniania innowacji i inkubatora, a także w związku z ewaluacją innowacji prowadzoną wśród tych uczestników testowania innowacji, którzy wyrazili zgodę na przekazanie swoich danych kontaktowych inkubatorowi na potrzeby ewaluacji. Trzeba pamiętać, że jeśli podstawą przetwarzania danych osobowych jest zgoda osoby, której te dane dotyczą, i zgoda ta zostanie przez nią wycofana, należy niezwłocznie wszystkie przetwarzane dane usunąć z zasobów oraz nie wykorzystywać ich inaczej niż w sposób, którego nie da się już obiektywnie zmienić (np. gdy wizerunek został już opublikowany w materiałach promocyjnych). W pozostałych przypadkach inkubator ma inne podstawy prawne przetwarzania danych osobowych niż zgoda osoby, której dane dotyczą – omawiamy je w dalszej części poradnika.

3. Proces przetwarzania danych

3.1. Wprowadzenie

W powyższym słowniczku wspomnieliśmy już o czynnościach przetwarzania danych. Chcemy jednak rozwinąć ten wątek, bo jego właściwe zrozumienie jest niezbędne do prawidłowego wypełnienia obowiązków wynikających z RODO. Czynności przetwarzania danych w praktyce możemy rozumieć jako taki proces przetwarzania danych, który jest podporządkowany jednemu konkretnemu celowi.

Określenie celu przetwarzania danych jest kluczowe dla ustalenia właściwiej podstawy prawnej, a co za tym idzie – dla ustalenia praw osób, których dane dotyczą, terminu usunięcia danych itd. Inaczej mówiąc, cel przetwarzania danych to powód, dla którego te dane przetwarzamy. Nie jest nim sama realizacja projektu, ale np. rekrutacja uczestników, upowszechnianie innowacji, prowadzenie ewidencji pracowników. Cel przetwarzania danych musi być konkretny i zrozumiały dla osoby, której dane dotyczą.

Zrozumienie czynności przetwarzania jest niezbędne do prawidłowego wypełnienia rejestru czynności przetwarzania danych (o którym wspominamy w podrozdziale 4.9.), a sam termin jest na tyle nieintuicyjny, że w interpretacji niektórych organizacji w rejestrze powinno zostać odnotowane każde działanie przeprowadzone na danych osobowych. Tymczasem takie pojedyncze działania to operacje przetwarzania danych, a tych nigdzie nie musimy spisywać.

Przedstawimy to na przykładzie przetwarzania danych związanych z zatrudnianiem pracowników na konkretne stanowisko.

Zbiór danych osobowych: kandydaci na stanowisko, którzy wysłali swoje zgłoszenia

Czynność (proces) przetwarzania danych: proces rekrutacji pracowników

Cel przetwarzania: rekrutacja pracowników na dane stanowisko

Operacje przetwarzania: zebranie zgłoszeń, kwalifikacja do rozmów rekrutacyjnych, umawianie rozmów rekrutacyjnych, przeprowadzenie rozmów rekrutacyjnych, wybór najlepszego kandydata i usunięcie danych pozostałych

Ponieważ celem tej czynności przetwarzania jest rekrutacja pracowników na to konkretne stanowisko, dane kandydatów są nam potrzebne tylko do momentu podjęcia decyzji o tym, kogo ostatecznie zatrudnimy. Po zrealizowaniu tego celu ustaje powód przetwarzania danych pozostałych osób. Musimy je więc usunąć, chyba że w procedurze rekrutacyjnej poprosimy kandydatów również o zgodę na przechowywanie ich danych na potrzeby przyszłych rekrutacji.

Po zrekrutowaniu pracownika kończy się jedna czynność przetwarzania danych (czyli proces rekrutacji), a zaczyna kolejna, a właściwe kilka odrębnych czynności, takich jak np. ewidencja czasu pracy (cel przetwarzania: ewidencjonowanie czasu pracy), ewidencja dokumentacji ZUS (cel przetwarzania: spełnienie obowiązku ciążącego na pracodawcy).

3.2. Przetwarzanie danych w procesie inkubacji innowacji społecznych

W przypadku inkubowania innowacji społecznych finansowanego z Europejskiego Funduszu Społecznego mamy do czynienia z co najmniej trzema głównymi aktorami:

- podmiotami prowadzącymi inkubatory,
- Instytucją Zarządzającą (czyli Ministerstwem Funduszy i Polityki Regionalnej),
- innowatorami.

W zależności od etapu inkubowania innowacji każdy z tych aktorów występuje wobec danych osobowych w różnych rolach (administratora, procesora, podprocesora,

odbiorcy), definiowanych przez umowę o dofinansowanie oraz rodzaj czynności przetwarzania danych. Poniżej omawiamy te role na poszczególnych etapach[3]:

1. Naboru wstępnych pomysłów na innowacje społeczne
2. Preinkubacji innowacji społecznych, czyli od momentu przyjęcia danego innowatora do programu wsparcia świadczonego przez inkubator aż do podpisania umowy grantowej
3. Testowania innowacji społecznych, czyli od momentu podpisania umowy grantowej aż do momentu rozliczenia grantu
4. Upowszechniania innowacji społecznych

Skupmy się najpierw na samych rolach.

Jak już wspominaliśmy, **administrator** to podmiot, który samodzielnie lub wspólnie ze współadministratorami ustala cele i sposoby przetwarzania danych osobowych. Administrator danych osobowych odgrywa w procesie przetwarzania kluczową rolę. W angielskiej wersji językowej RODO określa tę funkcję słowem *controller*, które opisuje ją dużo lepiej niż polski „administrator" sugerujący rolę techniczną. Tymczasem administrator to gospodarz danego procesu przetwarzania danych osobowych i kluczowy decydent.

Wszystkie podmioty – niezależnie od etapu inkubacji – są zawsze administratorami danych osobowych swoich pracowników, zleceniobiorców czy wolontariuszy. Nie zawsze są jednak administratorami wszystkich danych, które zbierają i przetwarzają.

W przypadku inkubacji innowacji, podmioty prowadzące inkubatory są administratorami[4] danych osób zgłaszających wstępne pomysły na innowacje i uczestników etapu preinkubacji.

---

[3] Zdajemy sobie sprawę, że etapy te wyglądają nieco inaczej w poszczególnych inkubatorach i inne noszą nazwy. Postanowiliśmy jednak – dla uproszczenia – przyjąć jeden schemat, który ułatwi przedstawienie kwestii przetwarzania danych osobowych.

[4] W inkubatorach prowadzonych przez więcej niż jeden podmiot partnerzy występują najczęściej jako współadministratorzy i w drodze wspólnych uzgodnień w przejrzysty sposób określają zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO. Ustalenia te powinny dotyczyć w szczególności sposobu realizacji żądań osób, których dane są przetwarzane.

Instytucja Zarządzająca jest natomiast administratorem danych innowatorów na etapie testowania (czyli od momentu podpisania umowy o przekazanie grantu), a sami innowatorzy są administratorami danych osobowych uczestników testowania.

Procesor (podmiot przetwarzający) to podmiot, który przetwarza dane osobowe w imieniu administratora na podstawie umowy powierzenia przetwarzania danych. Procesor jest niejako podwykonawcą realizującym na rzecz administratora konkretne zadania na powierzonych mu danych osobowych. Procesorem będzie na przykład zewnętrzne biuro rachunkowe, firma hostująca bazę danych, podmiot prowadzący na zlecenie ewaluację projektu.

W odniesieniu do danych, których administratorem jest Instytucja Zarządzająca, a więc danych innowatorów, z którymi podpisano umowę o powierzenie grantu, procesorem jest podmiot prowadzący inkubator.

Podprocesor (podmiot podprzetwarzający) to z kolei podmiot, któremu procesor podpowierzył przetwarzanie danych, czyli jakby podwykonawca podwykonawcy administratora. Z procesami podpowierzenia przetwarzania danych osobowych będziemy mieć do czynienia na tym etapie inkubacji, na którym to Instytucja Zarządzająca jest administratorem danych osobowych, inkubator jest ich procesorem, któremu IZ powierzyła przetwarzanie danych osobowych, a podprocesorem będzie podmiot, któremu inkubator podpowierzył przetwarzanie danych, którego dokonuje z polecenia i na rzecz administratora. Procesor może podpowierzyć przetwarzanie danych osobowych podprocesorowi tylko, jeśli zezwala mu na to umowa powierzenia przetwarzania danych osobowych zawarta z administratorem i na określonych w niej warunkach.

Ostatnią z ról jest **odbiorca**, czyli osoba fizyczna lub prawna, której ujawnia się dane osobowe. Odbiorcą danych będzie np. Instytucja Zarządzająca na etapie, na którym inkubator jest administratorem danych, ale IZ ma prawo wglądu w dane osobowe (np. w celu skontrolowania prawidłowości wydatków). Odbiorcą danych będzie też sam inkubator, np. w przypadku danych uczestników testowania innowacji, którzy wyrazili zgodę na przekazanie inkubatorowi swoich informacji kontaktowych na potrzeby ewaluacji. Odbiorca, który z ujawnionymi mu danymi osobowymi zaczyna nowy proces przetwarzania danych osobowych, staje się ich administratorem.

W rozumieniu RODO nie są odbiorcami te organy publiczne, które na mocy odrębnych przepisów prawa mogą otrzymywać dane osobowe w ramach konkretnego postępowania (np. urząd skarbowy, prokuratura, Najwyższa Izba Kontroli).

Poniższa tabela przedstawia kolejne etapy inkubacji i wskazuje rolę każdego z trzech kluczowych aktorów – podmiotów prowadzących inkubator, Instytucji Zarządzającej i innowatora – na każdym z nich.

	Podmiot prowadzący inkubator	**Instytucja Zarządzająca**	**Innowator**
1. Nabór wstępnych pomysłów na innowacje społeczne			
Dane pomysłodawców	Administrator	Nie dotyczy	Osoba, której dane są przetwarzane
2. Preinkubacja innowacji społecznych			
Dane uczestników preinkubacji	Administrator	Odbiorca	Osoba, której dane są przetwarzane
3. Testowanie innowacji społecznych			
Dane innowatorów testujących innowacje (uczestników projektu grantowego)	Procesor	Administrator	Osoba, której dane są przetwarzane
Dane uczestników testowania	Odbiorca	Odbiorca	Administrator
Dane osób wykorzystywane na potrzeby ewaluacji	Administrator	Nie dotyczy	Nie dotyczy
4. Upowszechnianie innowacji społecznych			
Dane innowatorów, których innowacje są upowszechniane	Administrator	Administrator	Osoba, której dane są przetwarzane
Dane uczestników testowania (np. wizerunek) wykorzystywane w ramach upowszechniania	Administrator	Administrator	Administrator

Więcej szczegółów na temat specyfiki przetwarzania danych osobowych na poszczególnych etapach inkubacji znajduje się w rozdziale 5.

3.3. Zasady przetwarzania danych osobowych

Zasada zgodności z prawem, rzetelności i przejrzystości – dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą. Przy inkubacji innowacji społecznych (ale też zawsze, gdy mamy do czynienia z osobami o nieznanym poziomie kompetencji) należy przyłożyć szczególną wagę do takiego formułowania informacji (np. podczas realizowania obowiązku informacyjnego), aby były one zrozumiałe także dla osoby niewykształconej i nieobytej z prawniczym językiem. RODO nie narzuca prawniczego języka, priorytetem jest jego zrozumiałość.

Zasada ograniczenia celu – dane osobowe mogą być zbierane tylko w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie mogą być przetwarzane dalej w sposób niezgodny z tymi celami. Cele przetwarzania danych wyznacza administrator danych, a zakres gromadzonych danych i sposób ich przetwarzania jest ściśle podporządkowany temu celowi.

Zasada minimalizacji danych – zbierane dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co jest niezbędne do realizacji celów przetwarzania. Podstawową zasadą jest ograniczenie gromadzenia danych tylko do tych, bez których nie będziemy w stanie zrealizować założonego celu przetwarzania danych. Na przykład na etapie rekrutacji, kiedy nie wiemy, czy kandydat się zakwalifikuje i będziemy z nim podpisywać umowę grantową, nie potrzebujemy jeszcze kompletnych danych niezbędnych do podpisania takiej umowy – wystarczy, że zgromadzimy dane niezbędne do dokonania dobrego wyboru.

Zasada prawidłowości danych – przetwarzane dane muszą być prawidłowe i w razie potrzeby uaktualniane. Należy więc podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane. Każda osoba, której dane dotyczą, ma prawo do ich sprostowania.

Zasada ograniczenia przechowywania – dane osobowe mogą być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów przetwarzania. Jeśli celem jest np. wybór najlepszych kandydatów do inkubatora, po zakończeniu rekrutacji nie potrzebujemy już danych

osób, które nie zostały wybrane, i powinniśmy je niezwłocznie usunąć. Z kolei dane osób, które otrzymają grant na przetestowanie innowacji, będą przechowywane jeszcze bardzo długo po zakończeniu testowania, bo celem ich przetwarzania jest nie tylko przetestowanie innowacji, ale także rozliczenie grantu oraz rozliczenie całego programu[5], w ramach którego dofinansowanie zostało przyznane.

Zasada integralności i poufności – dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem. W tym celu należy zastosować odpowiednie środki techniczne, organizacyjne i informatyczne. RODO nie narzuca sposobu realizacji tej zasady, ale to administrator jest ostatecznie rozliczany z działania w zgodzie z nią i ewentualnie pociągany do odpowiedzialności za naruszenie integralności i poufności danych.

Zasada rozliczalności – administrator/procesor jest odpowiedzialny za wypełnianie obowiązków wynikających z RODO i musi być w stanie wykazać, że się z tych obowiązków wywiązał. W praktyce zasada rozliczalności jest realizowana przez gromadzenie dowodów poświadczających stosowanie się do odpowiednich przepisów, co niestety oznacza konieczność tworzenia dodatkowej dokumentacji. Dlatego w załącznikach do naszego poradnika znajdziecie aż tyle wzorów dokumentów. Dokumentowanie własnych działań na różnych etapach przetwarzania danych osobowych pozwoli wykazać, że faktycznie realizowaliśmy nałożone na nas przez RODO i umowę o dofinansowanie obowiązki.

3.4. Podstawy prawne przetwarzania danych osobowych w procesie inkubacji innowacji społecznych

Do zgodnego z prawem przetwarzania danych osobowych, wbrew często spotykanej opinii, nie zawsze potrzebne jest podpisane przez osobę będącą podmiotem danych oświadczenie o wyrażeniu zgody na ich przetwarzanie. Przeciwnie, w organizacjach pozarządowych bardzo często zastosowanie mają inne przesłanki legalizujące.

[5] Chodzi o Program Operacyjny Wiedza Edukacja Rozwój 2014–2020, w ramach którego finansowane są inkubatory.

Także w przypadku podmiotów prowadzących inkubatory zgoda będzie dość rzadko podstawą prawną przetwarzania danych. Poniżej wymieniamy te przesłanki, które mają zastosowanie w inkubatorach w zależności od etapu inkubacji, rodzaju danych i celu przetwarzania.

3.4.1. Zgoda osoby, której dane dotyczą

Podstawa prawna: art. 6 ust. 1 lit. a i art. 9 ust. 2 lit. a RODO

Zgoda to konkretne, świadome, jednoznaczne i dobrowolne wyrażenie woli osoby, której dane dotyczą.

Trzeba jednak pamiętać, że zgoda to tylko jedna z podstaw prawnych przetwarzania danych osobowych i, zanim podsuniemy danej osobie formułkę „Wyrażam zgodę na przetwarzanie…", należy sobie zadać pytanie, czy możemy obiecać tej osobie, że będzie mogła w dowolnym momencie wycofać tę zgodę, a my wtedy usuniemy całkowicie jej dane. Jeśli odpowiedź na to pytanie jest negatywna, bo np. przepis prawa lub umowa o dofinansowanie nakazuje nam przechowywanie tych danych przez ileś lat, to znaczy, że musimy powołać się na inną przesłankę.

W inkubatorze zgoda będzie odpowiednią podstawą przetwarzania danych w następujących przypadkach:

- przetwarzanie danych autorów wstępnych pomysłów na innowacje (pomysłodawców) na etapie rekrutacji,
- przetwarzanie danych innych osób na etapie rekrutacji do pracy, na szkolenia itp.,
- przetwarzanie danych osób, które zapisały się na newsletter inkubatora,
- przetwarzanie wizerunku osób na potrzeby promocji inkubatora lub samych innowacji,
- przetwarzanie danych odbiorców testujących innowacje przez innowatorów i przekazywanie ich inkubatorowi na potrzeby ewentualnej ewaluacji prowadzonej przez inkubator lub wybrany przez niego podmiot.

RODO nie określa, w jaki sposób podmiot danych osobowych powinien wyrazić zgodę na ich przetwarzanie: wystarczy, że miało miejsce „wyraźne działanie potwierdzające

wolę", czyli nawet ustne oświadczenie. Wyjątkiem są dane osobowe wrażliwe, bo w ich przypadku zgoda musi mieć zawsze formę pisemną. Zgodnie jednak z zasadą rozliczalności najbezpieczniej będzie, jeśli, niezależnie od rodzaju danych, potwierdzenie udzielonej zgody będziemy mieć na piśmie. Niekoniecznie jednak musi być to dokument podpisany odręcznie: wyrazić zgodę można za pośrednictwem profilu zaufanego, w treści maila albo zaznaczając odpowiednie okienko na stronie internetowej. Pozwoli to wykazać nie tylko fakt udzielenia zgody przez daną osobę, ale także zagwarantuje prawidłowość samej zgody – aby mogła zostać uznana za ważną, musi ona bowiem spełniać cztery kryteria: być konkretna, świadoma, jednoznaczna i dobrowolna. Podpisana zgoda pozbawiona którejś z tych cech będzie nieważna.

W załączniku nr 1 znajduje się przykładowa zgoda na wykorzystanie wizerunku na potrzeby promocji i upowszechniania innowacji. Załącznik nr 1a dotyczy przetwarzania danych innowatorów, a 1b – uczestników testowania innowacji.

3.4.2. Umowa z osobą, której dane dotyczą

Podstawa prawna: art. 6 ust. 1 lit. b RODO

Jeśli w ramach inkubatora zawieramy z osobami fizycznymi umowy (np. o pracę, cywilnoprawną, porozumienie wolontariackie), podstawą przetwarzania ich danych nie jest ich zgoda, ale właśnie wiążąca nas z nimi umowa. Przetwarzanie jest bowiem niezbędne do realizacji umowy, której są stroną, a wcześniej – do podjęcia działań przed zawarciem tej umowy. Umowa wiąże się też z możliwymi roszczeniami, a w przypadku umów o pracę, cywilnoprawnych, kupna lub sprzedaży, także z ustawowymi obowiązkami dotyczącymi przechowywania takich danych.

3.4.3. Prawny obowiązek ciążący na administratorze

Podstawa prawna: art. 6 ust. 1 lit. c RODO

Jeśli istnieje przepis prawa, który nakazuje przetwarzać czyjeś dane osobowe, podstawą legalizującą to przetwarzanie będzie prawny obowiązek ciążący na administratorze. W procesie inkubacji Instytucja Zarządzająca, będąca

administratorem danych uczestników projektu grantowego (czyli innowatorów na etapie testowania), ma prawny obowiązek przetwarzania ich danych – taka też informacja znajduje się w klauzuli informacyjnej, którą inkubator ma obowiązek przedstawiać uczestnikom tego etapu inkubacji. Dla inkubatora prawny obowiązek jest podstawą przetwarzania danych pracowników i zleceniobiorców już po zakończeniu umowy z nimi – prawo nakazuje bowiem przechowywać takie dane przez długi czas po ustaniu zatrudnienia/zlecenia.

W niektórych przypadkach prawny obowiązek przetwarzania danych może ciążyć na samych innowatorach, jeśli np. ich innowacja zakłada pracę z osobami poniżej osiemnastego roku życia (mają wtedy prawny obowiązek przetwarzania danych wszystkich osób dopuszczonych do pracy z takimi osobami w tzw. rejestrze pedofilów).

3.4.4. Prawnie uzasadnione interesy administratora

Podstawa prawna: art. 6 ust. 1 lit. f RODO

Przetwarzanie danych osobowych jest zgodne z prawem także, jeśli wymaga tego prawnie uzasadniony interes administratora. W przypadku podmiotów prowadzących inkubatory prawnie uzasadniony interes, jakim jest konieczność rozliczenia projektu przed Instytucją Zarządzającą, może być podstawą prawną przetwarzania danych osobowych uczestników etapu preinkubacji – jeśli np. kontrola ze strony Instytucji Zarządzającej zażąda wglądu do list uczestników szkoleń dla potwierdzenia kwalifikowalności poniesionych na te szkolenia wydatków. Prawnie uzasadniony interes jest także podstawą prawną przetwarzania danych w przypadku stosowania monitoringu wizyjnego dla zapewnienia bezpieczeństwa czy w przypadku dochodzenia roszczeń lub obrony przed nimi. Na prawnie uzasadniony interes można się też powoływać, prowadząc marketing produktów lub usług lub kontaktując się z osobami fizycznymi w ramach działań fundraisingowych. W każdym przypadku powoływania się na przesłankę prawnie uzasadnionego interesu należy ten interes nazwać i wskazać.

4. Obowiązki instytucji przetwarzających dane osobowe

4.1. Inspektor ochrony danych

Inspektor ochrony danych (IOD) to termin ściśle zdefiniowany w RODO: oznacza osobę, która została wyznaczona do koordynowania zgodności działania instytucji z przepisami dotyczącymi danych osobowych. Powołanie IOD jest formalną procedurą, a sam IOD musi mieć zagwarantowany odpowiedni status w ramach struktury organizacyjnej. Dane IOD podlegają zgłoszeniu Urzędowi Ochrony Danych Osobowych.

Samo prowadzenie inkubatora nie wiąże się z obowiązkiem powołania inspektora ochrony danych. Podmiot realizujący inkubator ma prawny obowiązek wyznaczenia takiego inspektora tylko, jeśli spełnia któryś z poniższych warunków:

- jest organem lub podmiotem publicznym, lub
- jego główna działalność polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób na dużą skalę, lub
- jego główna działalność polega na przetwarzaniu na dużą skalę danych osobowych wrażliwych i/lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Z tych trzech kryteriów tylko pierwsze jest zero-jedynkowe. W przypadku projektu realizowanego w partnerstwie obowiązek dotyczy tylko partnera będącego podmiotem publicznym, a nie całego inkubatora. W przypadku, gdy inkubator jest prowadzony przez podmiot publiczny w partnerstwie z podmiotem niepublicznym, jedynie ten pierwszy ma obowiązek wyznaczenia inspektora ochrony danych. Obowiązek ten nie wypływa bowiem z faktu prowadzenia inkubatora, a z prawnego statusu podmiotu publicznego.

Pozostałe dwie okoliczności skutkujące obowiązkiem powołania inspektora ochrony danych są oparte o nieostre kryteria („główna działalność", „duża skala") i to na każdym podmiocie spoczywa obowiązek ustalenia (i udokumentowania tych ustaleń), czy któreś z nich spełnia. Samo RODO nie wyznacza jednoznacznych przesłanek, przyjmuje się jednak, że przetwarzanie danych osobowych jest „główną działalnością podmiotu", jeżeli stanowi jego „zasadnicze, a nie poboczne czynności". Z kolei „operacje przetwarzania o dużej skali" to te, które „służą przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą, oraz które mogą powodować wysokie ryzyko". W przypadku organizacji pozarządowych bardzo rzadko będziemy mieć do czynienia z sytuacją, w której organizacja będzie spełniać któreś z powyższych kryteriów i w związku z tym będzie mieć obowiązek powołania IOD.

Zgodnie z zasadą rozliczalności, która ma zastosowanie do wszystkich procesów przetwarzania danych osobowych, ustalenia dotyczące (braku) obowiązku powołania inspektora ochrony danych należy udokumentować. Można to zrobić w formie notatki lub uchwały, z której będzie wynikać, że podmiot przeprowadził analizę procesów przetwarzania danych, jakie realizuje, a także zakresu przetwarzanych danych, i w jej wyniku ustalił, że nie ciąży na nim obowiązek powołania IOD, nie spełnia bowiem żadnego z kryteriów wskazanych w art. 37 RODO. Przykładowa treść uchwały została zamieszczona w załączniku nr 2.

Oczywiście organizacja, która nie ma prawnego obowiązku powołania IOD, może go powołać na zasadzie dobrowolności, pamiętając jednak o dopełnieniu wszystkich wiążących się z tym formalności i obowiązków. Wydaje się, że w przypadku organizacji pozarządowych dobrowolne powoływanie inspektora ochrony danych nie jest wskazane z uwagi na konieczność spełnienia przy tym dodatkowych warunków i brak wyraźnej wartości dodanej w stosunku do sytuacji, w której po prostu wyznaczona osoba dba o zgodne z prawem przetwarzanie danych osobowych bez formalnego statusu IOD.

Nawet jeśli podmiot prowadzący inkubator nie jest zobowiązany przez prawo do powołania IOD, nic nie stoi na przeszkodzie, a wręcz jest zalecane, wyznaczenie w ramach struktury organizacyjnej osoby, która będzie odpowiedzialna za zgodne z prawem przetwarzanie danych w inkubatorze (czy też osobno w każdym podmiocie współprowadzącym inkubator) i z którą będą mogły kontaktować się osoby, których

dane są przetwarzane. Należy jednak pamiętać, by w odniesieniu do roli tej osoby używać innej nazwy niż inspektor ochrony danych, na przykład koordynator ds. danych osobowych. Odpowiednia będzie tutaj dowolna inna nomenklatura wskazująca na kompetencje danej osoby, ale bez stosowania do niej terminu zastrzeżonego dla osób spełniających warunki określone dla IOD.

4.2. Upoważnienia do przetwarzania danych

Każda osoba dopuszczona do przetwarzania danych, nawet jeśli jej rola ma się sprowadzać do przepisywania listy obecności uczestników do komputera czy samego tylko przeglądania danych osobowych (ono również jest przetwarzaniem danych w rozumieniu RODO), musi posiadać pisemne **upoważnienie do tego przetwarzania** nadane jej przez administratora danych. Upoważnienie może być wydane na czas określony. Jeśli obowiązuje na czas nieokreślony, to administrator powinien je formalnie **odwołać** w momencie, w którym dana osoba przestaje przetwarzać dane.

Ani RODO, ani umowa o dofinansowanie zawarta z Instytucją Zarządzającą nie narzucają inkubatorom jednego wzoru upoważnienia, może to być zatem upoważnienie stosowane zwyczajowo w danej instytucji.

Wydaje się jednak, że w przypadku tak dużych przedsięwzięć jak prowadzenie inkubatorów finansowanych z Europejskiego Funduszu Społecznego, ze względów praktycznych warto skorzystać ze wzoru upoważnienia znajdującego się w załączniku nr 9 do umowy o dofinansowanie, a w przypadku odwołania upoważnienia zastosować wzór z załącznika nr 10 tej umowy. Ułatwi to bieżące kontrolowanie i dokumentowanie procesu.

Nie ma też obowiązku tworzenia **ewidencji upoważnień**, ale i ona może pomóc monitorować kompletność niezbędnych danych. Odwołanie upoważnienia należy w takiej ewidencji odnotować na przykład w przypadku zakończenia współpracy z daną osobą. Wzór ewidencji upoważnień znajduje się w załączniku nr 3.

Specyficznym przypadkiem, z jakim mamy do czynienia w trakcie realizacji tego rodzaju projektów, jest kwestia **upoważnienia do przetwarzania danych osobowych w zbiorze Centralny system teleinformatyczny wspierający realizację**

programów operacyjnych[6]. Są to upoważnienia imienne, wydawane wyłącznie przez Instytucję Zarządzającą i ważne do dnia odwołania, nie dłużej jednak niż do dnia zakończenia ostatecznej archiwizacji dokumentacji Programu Operacyjnego Wiedza Edukacja Rozwój. Upoważnienie wydane przez Instytucję Zarządzającą dla pracownika lub pracowników podmiotu prowadzącego inkubator wygasa z chwilą ustania stosunku prawnego łączącego ten podmiot z danym pracownikiem, ale umowa zobowiązuje podmioty prowadzące inkubatory do posiadania przynajmniej jednej osoby legitymującej się imiennym upoważnieniem do przetwarzania danych osobowych odpowiedzialnej za nadzór nad zarchiwizowaną dokumentacją do dnia zakończenia jej archiwizowania.

4.3. Powierzenie przetwarzania danych

Jeśli zlecamy przetwarzanie danych osobowych własnemu pracownikowi, zleceniobiorcy czy wolontariuszowi, wystarczy upoważnienie go do przetwarzania danych osobowych opisane w poprzednim punkcie. Jeśli natomiast zlecamy przetwarzanie danych osobowych zewnętrznemu podmiotowi, nad którym nie sprawujemy bezpośredniej kontroli, samo upoważnienie nie będzie wystarczające – należy sporządzić odpowiednią umowę. Umowa powierzenia przetwarzania danych osobowych nie musi być odrębną umową, często jest częścią umowy na realizację danej usługi czy danych prac.

Podmiot, któremu w formie takiej umowy powierzamy przetwarzanie danych osobowych, staje się procesorem danych. Umowę powierzenia przetwarzania danych (lub umowę zawierającą tego rodzaju zapisy) będziemy musieli zawrzeć np. z podmiotem prowadzącym ewaluację projektu, firmą hostującą bazę danych uczestników projektu. Wzór umowy powierzenia przetwarzania danych znajduje się w załączniku nr 4.

[6] Jest to zbiór danych prowadzony przez Instytucję Zarządzającą, w którym gromadzone są dane uczestników projektu grantowego. Instytucja Zarządzająca w umowie o dofinansowanie projektu upoważnia podmioty prowadzące inkubator do wprowadzania do niego danych zawartych w oświadczeniu uczestnika.

Powierzenie przetwarzania danych osobowych – niezależnie od tego, czy będzie miało formę odrębnej umowy powierzenia przetwarzania danych, czy będzie elementem umowy o realizację jakichś działań – musi mieć formę pisemną i zawierać następujące informacje:

- przedmiot i czas trwania przetwarzania,
- charakter i cel przetwarzania,
- rodzaj danych osobowych oraz kategorie osób, których dane dotyczą,
- obowiązki i prawa administratora.

Umowa określa też, że podmiot przetwarzający:

- przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora,
- gwarantuje, że osoby upoważnione do przetwarzania danych osobowych zobowiążą się do zachowania tajemnicy lub że podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
- podejmuje wszelkie środki mające na celu ochronę bezpieczeństwa danych,
- przestrzega warunków korzystania z usług innego podmiotu przetwarzającego,
- w miarę możliwości pomaga administratorowi, poprzez odpowiednie środki techniczne i organizacyjne, wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą,
- po zakończeniu świadczenia usług związanych z przetwarzaniem, zależnie od decyzji administratora, usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie,
- udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w RODO oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

Na podstawie art. 28 RODO administrator, chcąc przetwarzać dane przy pomocy innego podmiotu, powinien korzystać wyłącznie z usług takich podmiotów, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych. Przed powierzeniem przetwarzania danych należy, zgodnie

z prawem, przeprowadzić proces weryfikacji podmiotu przetwarzającego. Trzeba sprawdzić, czy podmiot ten zapewnia wdrożenie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie danych osobowych było zgodne z RODO[7].

Brak weryfikacji podmiotu przetwarzającego oraz jego gwarancji dla przetwarzania zgodnie z przepisami o ochronie danych osobowych może wiązać się z konsekwencjami dla osób fizycznych, których dane osobowe zostały powierzone podmiotowi przetwarzającemu, na przykład w postaci utraty danych osobowych. Zatem decyzja, komu administrator ma powierzyć przetwarzanie danych osobowych, nie może być podejmowana bezpodstawnie. Dopiero po zbadaniu kompetencji i adekwatności wybranego podmiotu przetwarzającego administrator może przystąpić do zawarcia stosownej umowy powierzenia.

Trudno sobie wyobrazić przeprowadzanie drobiazgowej kontroli podmiotu, któremu chcemy zlecić jakieś zadanie wymagające przetwarzania danych osobowych, ale pomocne może być poproszenie go o wypełnienie listy kontrolnej zawierającej pytania o stosowane w tym podmiocie procedury. Nie gwarantuje to pełnego bezpieczeństwa danych, ale będzie dowodem, że podjęliśmy działania mające na celu weryfikację potencjalnego zleceniobiorcy. Wzór takiej listy kontrolnej znajduje się w załączniku nr 5.

Powyższe wymagania dotyczą przetwarzania danych, w przypadku których podmiot prowadzący inkubator jest administratorem. Natomiast szczegółowe informacje na temat obowiązków inkubatora odnośnie do danych, których inkubator jest podmiotem przetwarzającym, a których administratorem jest Instytucja Zarządzająca, omawiamy w dalszej części.

[7] W 2022 r. Urząd Ochrony Danych Osobowych nałożył karę na administratora danych, który przed powierzeniem przetwarzania danych osobowych nie upewnił się, że podmiot przetwarzający stosuje wymagane procedury. UODO wskazał, że administrator nie posiada żadnych dowodów dokumentujących przeprowadzenie stosownej weryfikacji podmiotu, któremu zamierzał powierzyć (i ostatecznie powierzył) przetwarzanie danych.

4.4. Obowiązek informacyjny

Art. 13 RODO nakłada obowiązek udzielania osobom, których dane są przetwarzane, szczegółowych informacji na temat przetwarzania ich danych i podmiotów biorących udział w tym procesie. Jeżeli dane osobowe są zbierane bezpośrednio od osoby, której dotyczą, administrator podczas pozyskiwania tych danych podaje jej następujące informacje:

- swoją tożsamość i dane kontaktowe,
- dane kontaktowe inspektora ochrony danych, jeśli został powołany,
- cel przetwarzania danych osobowych,
- podstawę prawną przetwarzania,
- jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f RODO: prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią,
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
- gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa spoza Europejskiego Obszaru Gospodarczego lub do organizacji międzynarodowej,
- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
- informacje o prawie osoby, której dane dotyczą, do żądania od administratora dostępu do tychże danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
- jeżeli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą (art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
- informację o prawie wniesienia skargi do organu nadzorczego,

- informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy, oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.

Przepisy nie określają, w jaki sposób ma być spełniony obowiązek informacyjny, ale ze względu na zasadę rozliczalności wskazane jest wywiązanie się z niego w taki sposób, by można było to udowodnić. Jeśli jest taka możliwość, warto pozyskać podpis osoby, której dane dotyczą, pod odpowiednią klauzulą (oświadczeniem). Gdy w projekcie tworzymy na przykład listy obecności, najlepiej będzie zamieścić treść klauzuli informacyjnej na liście. W przypadku zawierania umów klauzule można też umieszczać bezpośrednio w treści umowy. Warto załączać je także w korespondencji, publikować w informacjach na stronie.

W przypadkach, w których podmioty prowadzące inkubator są administratorami danych, same przygotowują stosowne klauzule informacyjne. W sytuacjach, gdy to Instytucja Zarządzająca jest administratorem danych (np. danych innowatorów na etapie testowania innowacji), zgodnie z umową o dofinansowanie podmiot prowadzący inkubator jest zobowiązany do pozyskania od uczestników projektu grantowego oświadczenia uczestnika według wzoru stanowiącego załącznik nr 8 tej umowy.

4.5. Prawa osób, których dane dotyczą

Każda osoba będąca podmiotem przetwarzanych danych posiada prawa, o których należy ją poinformować, by spełnić tzw. obowiązek informacyjny. Niektóre prawa są uniwersalne, inne zależą od tego, jaka w danym przypadku jest podstawa prawna przetwarzania danych osobowych.

Poniżej zamieszczamy zestawienie podstaw prawnych mających najczęściej zastosowanie w przypadku podmiotów prowadzących inkubatory. Zebraliśmy tu także informacje wskazujące na rodzaj praw przysługujących osobie, której dane dotyczą. Poniżej omawiamy każde z tych praw.

Podstawa prawna przetwarzania danych / Prawa przysługujące osobie, której dane dotyczą, w przypadku przetwarzania na tej podstawie prawnej	Zgoda osoby, której dane dotyczą (art. 6 ust. 1 lit. a/art. 9 ust. 2 lit. a)	Umowa zawarta z osobą, której dane dotyczą (art. 6 ust. 1 lit. b)	Prawny obowiązek ciążący na administratorze danych (art. 6 ust. 1 lit. c)	Prawnie uzasadnione interesy administratora danych (art. 6 ust. 1 lit. f)
Prawo dostępu do dotyczących jej danych	tak	tak	tak	tak
Prawo do sprostowania danych nieprawdziwych lub nieścisłych	tak	tak	tak	tak
Prawo do usunięcia danych (tzw. prawo do bycia zapomnianym)	tak, na żądanie	nie	nie	tak, pod warunkiem uznania sprzeciwu przez administratora[8]
Prawo do przenoszenia danych	tak	tak	nie	nie
Prawo do ograniczenia przetwarzania danych	tak	tak	tak	tak
Prawo do wniesienia sprzeciwu wobec przetwarzania danych	nie	nie	nie	tak
Prawo do wniesienia skargi do organu nadzoru (Urzędu Ochrony Danych Osobowych)	tak	tak	tak	tak

Prawo wycofania zgody – jeśli podstawą przetwarzania danych była zgoda osoby, której dane dotyczą, osoba ta może cofnąć wyrażoną przez siebie zgodę w każdym momencie i bez podawania przyczyny (art. 7 RODO). Wycofanie zgody nie ma wpływu na legalność przetwarzania danych, jakiego dokonano przed tym wycofaniem.

[8] W przypadku przetwarzania danych, którego podstawą prawną jest prawnie uzasadniony interes administratora, osobie będącej podmiotem przetwarzanych danych prawo do bycia zapomnianym przysługuje, jeśli wniosła sprzeciw wobec tego przetwarzania, a administrator danych osobowych ten sprzeciw uwzględnił – gdy nie miał żadnych nadrzędnych wobec powodów wniesienia sprzeciwu przesłanek.

Prawo dostępu – każda osoba może żądać informacji o przetwarzaniu jej danych osobowych, tj. potwierdzenia, czy i jak są przetwarzane jej dane osobowe. Jeżeli dane o osobie są przetwarzane, jest ona uprawniona do uzyskania do nich dostępu, otrzymania ich kopii oraz do uzyskania informacji o celach przetwarzania, kategoriach danych osobowych, o odbiorcach lub kategoriach odbiorców, którym dane zostały lub zostaną ujawnione, o okresie przechowywania danych lub o kryteriach jego ustalania, o przysługujących jej prawach związanych z przetwarzaniem jej danych osobowych, o możliwości wniesienia skargi do organu nadzoru, o źródle pozyskania danych osobowych (jeżeli nie zostały pozyskane bezpośrednio od osoby, której dane dotyczą) oraz o profilowaniu i zautomatyzowanym przetwarzaniu decyzji (art. 15 RODO).

Prawo do sprostowania – każda osoba, której dane przetwarzamy, może sprostować dane osobowe jej dotyczące. Jeżeli osoba uzyska informację o tym, że jej dane osobowe są nieprawidłowe, nieaktualne lub niekompletne, ma ona prawo żądać ich niezwłocznego sprostowania lub uzupełnienia (art. 16 RODO), a administrator danych ma obowiązek podjąć kroki, aby dane te zostały sprostowane również przez podmioty, którym je udostępnił.

Prawo do usunięcia danych (zwane też prawem do bycia zapomnianym) – w określonych przypadkach osoba, której dane są przetwarzane, może żądać usunięcia jej danych osobowych. Jeżeli osoba wyraziła zgodę na przetwarzanie danych osobowych, żądanie usunięcia odniesie taki sam skutek jak cofnięcie zgody (art. 17 RODO).

Prawo do usunięcia danych nie przysługuje jednak w każdej sytuacji. Żądanie usunięcia danych należy zawsze spełnić wobec osoby, która wycofała zgodę na przetwarzanie (jeśli to zgoda była podstawą prawną tego przetwarzania) lub osoby, która wniosła sprzeciw wobec przetwarzania jej danych w celach marketingowych (czyli wtedy, jeśli podstawą przetwarzania danych osobowych były prawnie uzasadnione interesy administratora, polegające na promocji jego produktów lub usług). Poza tymi przypadkami prawo do usunięcia danych przysługuje w ograniczonym zakresie, czyli wtedy, gdy administrator nie potrzebuje już danych do celu, w którym zostały zebrane, gdy osoba, której dane dotyczą, wniosła uzasadniony sprzeciw wobec ich przetwarzania, a administrator nie ma przesłanki nadrzędnej, by tego sprzeciwu nie uwzględnić, lub gdy dane osobowe były przetwarzane niezgodnie z prawem.

Prawo do ograniczenia przetwarzania – osoba, której dane dotyczą, może żądać ograniczenia przetwarzania jej danych osobowych (art. 18 RODO), to znaczy zaprzestania ich przetwarzania z wyjątkiem ich przechowywania. Ma do tego prawo, gdy:

- kwestionuje prawidłowość danych osobowych – na okres, w którym administrator będzie weryfikował ich prawidłowość,
- kwestionuje zgodność z prawem przetwarzania danych osobowych przez administratora,
- administrator nie potrzebuje już tych danych, ale są one potrzebne osobie, której dotyczą, do ustalenia, dochodzenia lub obrony jej roszczeń,
- wniosła sprzeciw wobec przetwarzania – do czasu rozpatrzenia sprzeciwu przez administratora.

Prawo do wniesienia sprzeciwu – jeśli dane są przetwarzane na podstawie przesłanki prawnie uzasadnionych interesów administratora, osoba, której te dane dotyczą, może wnieść sprzeciw wobec ich przetwarzania. Administrator ma obowiązek rozpatrzyć ten sprzeciw, ale ostatecznie nie zawsze musi go uwzględnić. Jeśli na przykład przetwarza dane w swoim prawnie uzasadnionym interesie, jakim jest konieczność rozliczenia projektu finansowanego ze środków publicznych, może uznać, że jego przesłanka jest nadrzędna wobec sprzeciwu osoby.

Prawo do przenoszenia danych – osoba, której dane są przetwarzane w sposób zautomatyzowany, a podstawą prawną ich przetwarzania jest jej zgoda lub wiążąca ją z administratorem umowa, może przenieść swoje dane osobowe, tj. otrzymać je w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, lub zażądać od administratora przesłania tych danych innemu podmiotowi, który wskaże (art. 20 RODO).

Na każdy wniosek o realizację praw złożony przez osobę, której dane osobowe dotyczą, odpowiedź musi zostać udzielona maksymalnie w ciągu miesiąca. W wyjątkowych sytuacjach przewidzianych w RODO można przedłużyć ten termin, należy jednak poinformować o tym zainteresowaną osobę.

Nie w każdej sytuacji podmiot prowadzący inkubator będzie właściwym adresatem żądań związanych ze wspomnianymi wyżej prawami. To, czy należy je kierować do inkubatora, zależy od tego, czy jest on w danej sytuacji administratorem danych.

Na przykład, jak już wspominaliśmy, na etapie testowania innowacji administratorem danych innowatorów jest Instytucja Zarządzająca. Zatem na tym etapie to ona będzie adresatem wszystkich żądań. Jeśli więc żądanie trafi do podmiotu prowadzącego inkubator, powinien on przekazać je inspektorowi ochrony danych w Instytucji Zarządzającej.

Specyfikę poszczególnych etapów omawiamy w rozdziale 5. Na następnej stronie zamieszczamy natomiast tabelę ilustrującą, jakie prawa przysługują na danym etapie osobom, których dane dotyczą, i kto rozpatruje związane z nimi żądania.

Czynność przetwarzania danych	Przetwarzanie danych osobowych pomysłodawców	Przetwarzanie danych uczestników preinkubacji innowacji
Podmiot rozpatrujący żądania osób, których dane dotyczą	Podmiot prowadzący inkubator	Podmiot prowadzący inkubator
Podstawa prawna przetwarzania danych osobowych	Zgoda osoby, której dane dotyczą (art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a)	Prawnie uzasadnione interesy podmiotu prowadzącego inkubator (art. 6 ust. 1 lit. f)
Prawa przysługujące osobie, której dane dotyczą		
Prawo dostępu do dotyczących jej danych	tak	tak
Prawo do sprostowania danych nieprawdziwych lub nieścisłych	tak	tak
Prawo do usunięcia danych (tzw. prawo do bycia zapomnianym)	tak, na żądanie	tak, jeśli administrator uwzględnił sprzeciw osoby, której dane dotyczą, wobec przetwarzania jej danych
Prawo do przenoszenia danych	tak	nie
Prawo do ograniczenia przetwarzania danych	tak	tak
Prawo do wniesienia sprzeciwu wobec przetwarzania danych	nie	tak
Prawo do wniesienia skargi do organu nadzoru (Urzędu Ochrony Danych Osobowych)	tak	tak
Prawo dostępu do dotyczących jej danych	tak	tak

Przetwarzanie danych osobowych innowatorów testujących innowacje (uczestników projektu grantowego)	**Przetwarzanie danych osobowych uczestników testowania innowacji na potrzeby z tym związane**	**Przetwarzanie danych osobowych lub wizerunku na potrzeby promocji i upowszechniania innowacji**	**Przetwarzanie danych uczestników testowania innowacji na potrzeby ewaluacji**
Instytucja Zarządzająca	Innowator	Administrator wykorzystujący te dane w takim celu	Administrator prowadzący ewaluację
Prawny obowiązek ciążący na Instytucji Zarządzającej jako administratorze tych danych osobowych (art. 6 ust. 1 lit. c)	Zgoda osoby, której dane dotyczą (art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a)	Zgoda osoby, której dane dotyczą (art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a)	Zgoda osoby, której dane dotyczą (art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a)
tak	tak	tak	tak
tak	tak	tak	tak
nie	tak, na żądanie	tak, na żądanie	tak, na żądanie
nie	tak	tak	tak
tak	tak	tak	tak
nie	tak	tak	nie
tak	tak	tak	tak
tak	tak	tak	tak

4.6. Przeprowadzenie analizy ryzyka

Każdy podmiot przetwarzający dane osobowe, niezależnie od swojej roli w procesie, ma obowiązek przeprowadzenia analizy ryzyka. Analiza ta powinna zostać przeprowadzona osobno dla poszczególnych czynności przetwarzania danych, jeśli znacząco różnią się one zakresem przetwarzanych danych lub sposobem zabezpieczenia tych danych. Inny będzie bowiem poziom ryzyka w przypadku przetwarzania danych wrażliwych w komputerze podłączonym do Internetu, a inny w przypadku przechowywanej w formie papierowej listy obecności uczestników spotkania, na której znajdują się wyłącznie ich imiona i nazwiska. Analizę ryzyka należy przeprowadzić z perspektywy osoby, której dane dotyczą, uwzględniając konsekwencje dla niej i jej praw.

Przepisy nie precyzują, jak powinien wyglądać sam proces analizy ryzyka ani w jaki sposób ma zostać udokumentowany. Może to być wewnętrzny grupowy namysł przeprowadzony przez zespół projektu, którego ustalenia znajdą odzwierciedlenie w notatce podsumowującej zidentyfikowane zagrożenia i sposoby zaradzenia im. Proces analizy ryzyka to po prostu poszukiwanie najbardziej konkretnej i pełnej odpowiedzi na trzy pytania rozpatrywane ściśle w kontekście danej organizacji i przetwarzanych przez nią danych:

- Jakie niepożądane zdarzenia dotyczące przetwarzanych przez inkubator danych mogą wystąpić przy obecnie stosowanych środkach bezpieczeństwa?
- Jakie jest prawdopodobieństwo wystąpienia tych niepożądanych zdarzeń?
- Jakie będą szkody dla osób, których dane dotyczą, w przypadku wystąpienia tych zdarzeń?

W materiałach udostępnionych przez Urząd Ochrony Danych Osobowych jako przykład metody analizy ryzyka wskazano macierz ryzyka, za pomocą której – używając ustalonej przez siebie punktacji (w tym przypadku 1–5, ale można przyjąć dowolną skalę) – oceniamy prawdopodobieństwo zaistnienia niepożądanego zdarzenia oraz rozmiary negatywnych skutków, jakie by ono przyniosło dla osób, których dane dotyczą. Przyznawane oceny pozwolą umieścić ryzyko na jednym z czterech pól określających jego poziom.

SKUTEK	PRAWDOPODOBIEŃSTWO				
	Rzadkie	Mało prawdopodobne	Możliwe	Prawdopodobne	Prawie pewne
Bardzo niski	N	N	N	Ś	Ś
Niski	N	Ś	Ś	W	W
Średni	Ś	Ś	W	W	K
Wysoki	W	W	W	K	K
Bardzo wysoki	W	W	K	K	K

N
(niski)

Poziom ryzyka akceptowany – działania podejmowane w zależności od wymaganych nakładów

Ś
(średni)

Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania

W
(wysoki)

Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania

K
(krytyczny)

Poziom ryzyka nietolerowany – wymaga natychmiastowego działania

Źródło: materiały Urzędu Ochrony Danych Osobowych

Należy pamiętać o konieczności okresowego weryfikowania już przeprowadzonej analizy ryzyka. Trzeba to zrobić szczególnie wtedy, gdy zajdzie któraś z następujących okoliczności:

- rozpoczynamy nowy proces przetwarzania danych (dla tego procesu należy przeprowadzić analizę ryzyka, jeśli zasadniczo różni się od procesów, dla których taką analizę już przeprowadziliśmy),
- rozszerzamy zakres przetwarzanych danych (analizę ryzyka przeprowadziliśmy dla tych danych, które początkowo zamierzaliśmy gromadzić, ale jeśli w trakcie realizacji projektu zakres tych danych znacząco się rozszerzy, może to zwiększać potencjalne ryzyko, a zatem analizę należałoby uzupełnić o nowe czynniki),
- znacząco zmieniamy sposób przetwarzania danych (na przykład wprowadzamy do znajdującej się w chmurze bazy danych dane osobowe dotychczas przetwarzane wyłącznie w formie papierowej).

W przeprowadzeniu analizy ryzyka pomocne mogą być wskazówki przygotowane przez Urząd Ochrony Danych Osobowych. Należy jednak pamiętać, że w procesie analizy ryzyka nie trzeba stosować bardzo skomplikowanej metodologii. Kluczowe jest bowiem racjonalne przeanalizowanie potencjalnych zagrożeń pod kątem prawdopodobieństwa ich wystąpienia oraz potencjalnych skutków. Proces powinien być zatem możliwie najbardziej partycypacyjny, zrozumiały dla wszystkich i podporządkowany podstawowemu celowi, jakiemu służy, czyli zastosowaniu adekwatnych środków bezpieczeństwa danych eliminujących lub minimalizujących zidentyfikowane potencjalne ryzyko i jego skutki dla osób, których dane dotyczą.

W załączniku nr 6 znajduje się przykładowy arkusz analizy ryzyka do samodzielnego wypełnienia zgodnie z zawartymi w nim wskazówkami. Przypominamy jednak, że analizy można dokonać w dowolny sposób, zarówno dużo bardziej uproszczony, jak i dużo bardziej rozbudowany. Podobnie jak w przypadku wszystkich obowiązków wynikających z RODO, także przeprowadzenie analizy ryzyka należy udokumentować. W wersji minimalnej może to być notatka z samego procesu. Wzór takiej notatki znajduje się w załączniku nr 7.

4.7. Zastosowanie środków bezpieczeństwa

Dobrze przeprowadzona analiza ryzyka daje odpowiedź na pytanie, jakie zdarzenia niepożądane mogą wystąpić, jakie jest prawdopodobieństwo, że wystąpią, i jakie zagrożenie ich wystąpienie może spowodować dla osób, których dane dotyczą. Analiza ryzyka powinna zatem skutkować określeniem najbardziej adekwatnych środków mających na celu zapewnienie bezpieczeństwa danych. Zastosowane środki bezpieczeństwa danych będą odnotowane w odpowiedniej rubryce w rejestrze przetwarzania danych.

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Mogą to być np.:

- pseudonimizacja lub anonimizacja danych osobowych,
- szyfrowanie danych,
- zapewnianie w sposób ciągły poufności, integralności, dostępności i odporności systemów i usług przetwarzania (np. szyfrowanie przekazywanych danych osobowych, uwierzytelnianie użytkowników komputera zawierającego dane, automatyczne procedury wylogowywania po dłuższej bezczynności, UPS-y podtrzymujące działanie komputera w razie nagłej utraty zasilania),
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego (np. poprzez regularne tworzenie kopii zapasowych i przechowywanie ich w osobnym miejscu),
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem i wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Środki bezpieczeństwa można podzielić na trzy grupy.

4.7.1. Organizacyjne środki ochrony danych

Są to wszelkie procedury wewnętrzne, jakie stosujemy, aby zminimalizować ryzyko naruszenia bezpieczeństwa danych, na przykład:

- do przetwarzania danych dopuszczane są wyłącznie osoby do tego upoważnione,
- każda upoważniona osoba jest zobowiązana do zachowania poufności danych,
- pracownicy przetwarzający dane znają zasady bezpieczeństwa danych,
- osoby korzystające ze wspólnych komputerów lub zasobów informatycznych mają w nich osobne konta użytkownika, by można było monitorować, kto jakich operacji dokonał,
- obowiązuje polityka czystego biurka – dokumenty zawierające dane osobowe nie mogą być przechowywane w miejscu łatwo dostępnym dla osoby nieupoważnionej,
- wprowadzone są procedury komisyjnego trwałego niszczenia danych,
- obowiązują procedury postępowania z komputerami służbowymi zawierającymi dane osobowe (np. naprawy, transportu).

4.7.2. Techniczne środki ochrony danych

Są to zabezpieczenia techniczne utrudniające lub uniemożliwiające dostęp do danych osobom nieuprawnionym, na przykład:

- kontrola dostępu do pomieszczeń, w których przechowywane są dane osobowe,
- zamykanie na klucz pomieszczeń, w których przechowywane są dane osobowe,
- kraty lub rolety antywłamaniowe w oknach pomieszczeń,
- monitoring biura,
- zamykane na klucz szafki, w których przechowywane są dane osobowe.

4.7.3. Informatyczne środki ochrony danych

Są to zabezpieczenia stosowane w przypadku przetwarzania danych w formie elektronicznej, na przykład:

- ograniczenie dostępu do systemów teleinformatycznych tylko do upoważnionych użytkowników,
- własny login i hasło utworzone dla każdego z użytkowników według wytycznych zwiększających bezpieczeństwo,
- stosowanie ochrony kryptograficznej w przypadku przesyłania danych przez Internet (choćby w wersji podstawowej, takiej jak chronienie dokumentów z danymi hasłem),
- zastosowanie protokołu SSL w przypadku pozyskiwania danych przez stronę internetową,
- rozwiązania chroniące systemy informatyczne przed skutkami awarii zasilania elektrycznego (UPS),
- programy antywirusowe i firewalle,
- trwałe usuwanie danych poprzez specjalne programy.

To tylko przykłady możliwych zabezpieczeń. Każdy podmiot prowadzący inkubator powinien dobrać je w zależności od zidentyfikowanych w procesie analizy ryzyka zagrożeń, a także, oczywiście, własnych możliwości organizacyjnych i finansowych.

Warto podkreślić, że „szafy zgodne z RODO" to tylko chwyt marketingowy, RODO nie narzuca bowiem konkretnego sposobu zabezpieczenia danych. Rozliczani będziemy z adekwatności i skuteczności zabezpieczeń. Ponieważ w najbardziej doskonałym systemie najsłabszym ogniwem jest zazwyczaj człowiek, należy zwrócić szczególną uwagę na zapoznanie wszystkich osób mających kontakt z danymi z obowiązującymi w organizacji zasadami i upewnić się, że je rozumieją i będą ich przestrzegać.

W załączniku nr 8 znajduje się przykład zasad bezpiecznego przetwarzania danych.

4.8. Dokumentowanie zastosowanych środków bezpieczeństwa

RODO nie narzuca podmiotom przetwarzającym dane osobowe wprowadzenia konkretnej polityki przetwarzania danych osobowych. Niemniej posiadanie tego rodzaju dokumentu bardzo ułatwia usystematyzowanie i dokumentowanie procesów przetwarzania danych osobowych, zarówno na użytek bieżącego zarządzania tymi procesami, jak i na użytek ewentualnej kontroli.

W umowie o dofinansowanie Instytucja Zarządzająca zobowiązuje natomiast podmioty prowadzące inkubatory innowacji, aby przed rozpoczęciem przetwarzania danych osobowych przygotowały dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę i bezpieczeństwo przetwarzanych danych osobowych, które uwzględniają warunki przetwarzania, w szczególności te, o których mowa w art. 32 RODO.

Artykuł 32 RODO wskazuje, że administrator i podmiot przetwarzający zobowiązani są wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa adekwatny do zidentyfikowanego przez siebie ryzyka. Więcej informacji o analizie ryzyka znajduje się w podrozdziale 4.6. Przykładowe środki bezpieczeństwa opisaliśmy z kolei w podrozdziale 4.7.

4.9. Rejestrowanie czynności przetwarzania

Każdy administrator oraz podmiot przetwarzający dane (procesor) ma obowiązek prowadzenia rejestrów – odpowiednio będą to rejestr czynności przetwarzania danych (dla administratora) i rejestr kategorii czynności przetwarzania danych (dla procesora).

Nie oznacza to oczywiście obowiązku szczegółowego odnotowywania prowadzonych na danych operacji ani tym bardziej tworzenia jakichkolwiek dodatkowych baz danych. Rejestrowanie czynności i kategorii czynności to stworzenie czegoś w rodzaju zestawienia tego, czyje dane przetwarzamy, w jakim celu i w jaki sposób. W załączniku nr 9 znajduje się wstępnie wypełniony rejestr czynności przetwarzania danych oraz

rejestr kategorii czynności przetwarzania danych (są one ujęte w jednym dokumencie, w osobnych arkuszach). Z kolei w załączniku nr 10 zamieszczamy instrukcję ich wypełniania.

4.10. Postępowanie z naruszeniami

Zgodnie z art. 4 pkt 12 RODO naruszenie ochrony danych oznacza „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych".

Przykłady naruszenia podane przez Urząd Ochrony Danych Osobowych to:

- zgubienie lub kradzież nośnika/urządzenia, dokumentacji papierowej (zawierającej dane osobowe),
- zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy,
- nieuprawnione uzyskanie dostępu do informacji, nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń,
- złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych,
- uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (*phishing*),
- nieprawidłowa anonimizacja danych osobowych w dokumencie,
- nieprawidłowe usunięcie danych osobowych z nośnika danych przed jego zbyciem,
- niezamierzona publikacja,
- dane osobowe wysłane do niewłaściwego odbiorcy, ujawnienie danych niewłaściwej osobie, ustne ujawnienie danych osobowych.

W przypadku stwierdzenia naruszeń administrator ma obowiązek zgłosić je do Urzędu Ochrony Danych Osobowych bez zbędnej zwłoki – nie później jednak niż w terminie

72 godzin po stwierdzeniu naruszenia. Od zgłoszenia można odstąpić, jeśli jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych (np. dane osobowe w formie papierowej uległy zniszczeniu – zniszczenie mieści się co prawda w definicji naruszenia, ale nie wiąże się z ryzykiem dla osób, których dane uległy zniszczeniu, jedynie sam administrator będzie miał kłopot z realizacją i rozliczeniem projektu). Jeśli naruszenie ma miejsce po stronie procesora, zgłasza je on bezpośrednio i niezwłocznie administratorowi, który następnie analizuje konieczność zgłoszenia do UODO.

Gdy dojdzie do naruszenia, administrator musi zastosować odpowiednie procedury:

- powiadomić inspektora ochrony danych (jeśli go ma),
- ocenić, czy naruszenie może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, których dane dotyczą,
- zgłosić naruszenie do organu nadzorczego – gdy jest to konieczne,
- powiadomić osoby, których dane dotyczą, o naruszeniu – gdy jest to konieczne,
- udokumentować wszelkie naruszenia w ewidencji naruszeń (jej wzór znajduje się w załączniku nr 11).

Naruszenia należy zgłaszać Urzędowi Ochrony Danych Osobowych. Można to zrobić, wypełniając formularz dostępny bezpośrednio na platformie biznes.gov.pl, a następnie wysyłając go drogą internetową na elektroniczną skrzynkę podawczą ePUAP lub tradycyjną pocztą na adres Urzędu.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko dla praw lub wolności osób fizycznych, należy także bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą, o jego zaistnieniu. Zawiadomienie może mieć formę indywidualną (np. wiadomość mailowa bezpośrednio do zainteresowanych osób) lub zbiorową (np. komunikat na stronie). Ta pierwsza forma jest rekomendowana, ale nie zawsze możliwa. Ważne, aby administrator mógł wykazać, że zrobił wszystko, by informacja o naruszeniu dotarła do najbardziej zainteresowanych – osób, których dotyczą dane zagrożone naruszeniem.

5. Specyfika przetwarzania danych osobowych na poszczególnych etapach inkubacji innowacji społecznych

5.1. Etap naboru wstępnych pomysłów na innowacje społeczne

5.1.1. Dane osób zgłaszających wstępne pomysły na innowacje

Administrator: podmiot prowadzący inkubator

Procesor: podmiot, któremu powierzono przetwarzanie danych osób zgłaszających wstępne pomysły (jeśli dotyczy)

Odbiorca: podmiot, któremu administrator udostępnia dane osób zgłaszających wstępne pomysły (jeśli dotyczy)[9]

Cel przetwarzania: wybór wstępnych pomysłów na innowacje społeczne

Podstawa prawna: art. 6 ust. 1 lit. a RODO (zgoda osoby, której dane dotyczą)

Termin usunięcia danych: X miesięcy po zakończeniu rekrutacji (określona liczba miesięcy w zależności od potrzeb)

Rejestr, w którym należy odnotować proces: rejestr czynności przetwarzania danych

[9] Odbiorcą danych w inkubatorach na tym etapie będą wszystkie podmioty, którym podmiot prowadzący inkubator zlecił realizację jakichś zadań związanych z przetwarzaniem tych danych. Może to być na przykład firma obsługująca od strony informatycznej bazę danych, w której gromadzone są dane pomysłodawców zgłaszających się do inkubatora.

Na tym etapie administratorem danych osobowych jest podmiot prowadzący inkubator (a w przypadku projektu realizowanego w partnerstwie – wszyscy partnerzy jako współadministratorzy) i to on decyduje o celach i środkach przetwarzania danych, a także o zakresie danych, jakie są mu na tym etapie niezbędne do przeprowadzenia rekrutacji. Procesorem będzie podmiot, któremu inkubator powierzył przetwarzanie danych (może to być np. firma hostująca bazę danych, w której gromadzimy dane osobowe zgłaszających się pomysłodawców).

Podstawą prawną przetwarzania danych osobowych osób zgłaszających wstępne pomysły na innowacje (pomysłodawców) jest ich zgoda, którą mogą wycofać w dowolnym momencie trwania rekrutacji. Celem przetwarzania danych pomysłodawców jest tylko wybranie tych, którzy przejdą do kolejnego etapu, a dane osobowe kandydatów odrzuconych muszą być usunięte po osiągnięciu tego celu (czyli po zakończeniu rekrutacji). Należy zatem z góry określić termin usunięcia danych tych pomysłodawców, którzy nie przejdą do kolejnego etapu. Inkubator sam określa ostateczny moment zakończenia rekrutacji i w klauzuli informacyjnej dla pomysłodawców podaje im ostateczny termin usunięcia ich danych. Okres ten nie powinien być jednak zbyt długi, administrator ma bowiem prawo przetwarzania danych tylko do czasu zrealizowania celu, w jakim je zbierał.

Usunięcie danych osobowych może zostać przeprowadzone w dowolny sposób, ważne, aby nie można ich było odtworzyć. Nie ma obowiązku zatrudniania specjalistycznej firmy, dane można po prostu zniszczyć w niszczarce czy nawet spalić. Należy pamiętać o trwałym usunięciu danych nie tylko w wersji papierowej, ale także ze wszystkich pozostałych nośników, czyli z komputerów i serwerów. Usunięcie danych jest ważnym elementem zamknięcia procesu przetwarzania, rekomendujemy zatem udokumentowanie tego notatką, z której będzie wynikało kto, kiedy i w jaki sposób trwale te dane usunął. Wzór notatki dotyczącej usunięcia danych znajduje się w załączniku nr 12.

Informacja o przetwarzaniu danych osobowych na tym etapie powinna zostać ujęta w rejestrze czynności przetwarzania danych.

Prawa osób, których dane dotyczą

Podstawą przetwarzania danych osobowych pomysłodawców jest ich zgoda na przetwarzanie danych w celach niezbędnych do przeprowadzenia rekrutacji, dlatego przysługuje im prawo wycofania zgody w dowolnym momencie, o czym administrator ma obowiązek ich poinformować w klauzuli informacyjnej przedstawianej razem z dokumentami rekrutacyjnymi. Poza prawem do wycofania zgody w dowolnym momencie pomysłodawcom przysługują wszystkie inne omawiane wcześniej prawa z wyjątkiem prawa do wniesienia sprzeciwu – jako że podstawą przetwarzania danych jest dobrowolna zgoda osoby, której dane dotyczą, trudno, żeby wnosiła sprzeciw wobec własnej zgody. Może po prostu tę zgodę wycofać i skorzystać z tzw. prawa do bycia zapomnianym, czyli zażądać usunięcia wszystkich dotyczących jej danych.

Zgłaszanie naruszeń

Zgłaszanie ewentualnych naruszeń na tym etapie jest obowiązkiem podmiotu prowadzącego inkubator.

W przypadku stwierdzenia naruszeń należy je zgłosić do Urzędu Ochrony Danych Osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Od zgłoszenia można odstąpić, jeśli jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych (na przykład dane osobowe w formie papierowej uległy zniszczeniu – zniszczenie mieści się co prawda w definicji naruszenia, ale nie wiąże się z ryzykiem dla osób, których dane uległy zniszczeniu, jedynie sam inkubator może mieć kłopot z realizacją i rozliczeniem projektu).

Naruszenia należy zgłaszać Urzędowi Ochrony Danych Osobowych. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, inkubator powinien bez zbędnej zwłoki zawiadomić o nim osobę, której dane dotyczą.

5.2. Etap preinkubacji innowacji społecznych

5.2.1. Dane innowatorów uczestniczących w etapie preinkubacji

Administrator: podmiot prowadzący inkubator

Procesor: podmiot, któremu powierzono przetwarzanie danych (jeśli dotyczy)

Odbiorca: Instytucja Zarządzająca oraz każdy podmiot, któremu na tym etapie ujawnia się dane osobowe innowatorów[10]

Cel przetwarzania danych: dopracowanie wstępnych pomysłów na innowacje społeczne oraz prawidłowa realizacja projektu, jego sprawozdanie i rozliczenie zgodnie z umową o dofinansowanie

Podstawa prawna: art. 6 ust. 1 lit. f RODO (prawnie uzasadnione interesy inkubatora polegające na konieczności zgodnego z umową o dofinansowanie zrealizowania i rozliczenia projektu)

Termin usunięcia: po rozliczeniu Programu Operacyjnego Wiedza Edukacja Rozwój 2014–2020 oraz zakończeniu archiwizowania dokumentacji (o upływie tego terminu poinformuje Instytucja Zarządzająca)

Rejestr, w którym należy odnotować proces: rejestr czynności przetwarzania danych

Na tym etapie administratorem danych osobowych jest podmiot prowadzący inkubator (a w przypadku projektu realizowanego w partnerstwie – wszyscy partnerzy jako współadministratorzy), procesorem – podmiot, któremu inkubator powierzył przetwarzanie danych (może to być np. firma hostująca bazę danych, w której gromadzimy dane osobowe uczestników), a odbiorcą danych – Instytucja Zarządzająca, która w ramach kontroli projektu może mieć wgląd w listy uczestników poszczególnych działań.

[10] Zobacz definicję odbiorcy przedstawioną w rozdziale 2 oraz w podrozdziale 5.1.

Ponieważ, realizując projekt finansowany ze środków publicznych, podmiot prowadzący inkubator będzie musiał wykazać kwalifikowalność wydatków, podstawą prawną przetwarzania danych osobowych jest na tym etapie prawnie uzasadniony interes tego podmiotu polegający na konieczności realizacji projektu i jego prawidłowego rozliczenia.

Prawa osób, których dane dotyczą

Na tym etapie podmiot prowadzący inkubator będzie realizować żądania osób, których dane dotyczą. Powinien to robić bez zbędnej zwłoki, maksymalnie w ciągu miesiąca od zgłoszenia żądania. RODO przewiduje co prawda możliwość wydłużenia tego czasu, ale nie wydaje się, aby w projekcie zachodziły jakieś okoliczności uzasadniające wydłużanie podstawowego terminu.

Jak już wspomnieliśmy, podstawą prawną przetwarzania danych jest tu prawnie uzasadniony interes podmiotu prowadzącego inkubator, czyli konieczność rozliczenia umowy o dofinansowanie zawartej z Instytucją Zarządzającą. W związku z tym prawo do żądania usunięcia swoich danych, o którym uczestnicy zostali poinformowani w klauzuli informacyjnej, przysługuje im tylko teoretycznie i to w absolutnie wyjątkowych (trudnych wręcz do wyobrażenia) okolicznościach. Prawo do żądania usunięcia danych uczestnika przysługuje mu bowiem tylko wtedy, gdy wniósł uzasadniony sprzeciw wobec przetwarzania, motywując to swoją szczególną sytuacją, a podmiot prowadzący inkubator nie wykazał istnienia ważnych i prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą. Ponieważ jednak prawnie uzasadnionym interesem inkubatora jest tu konieczność rozliczenia zadania publicznego sfinansowanego ze środków publicznych, trudno sobie wyobrazić interes uczestnika, który byłby wobec tego nadrzędny. Gdyby jednak takie żądanie się pojawiło – a bywa, że osoby błędnie rozumieją tzw. prawo do bycia zapomnianym i uważają, że przysługuje im ono w każdej sytuacji – należy je rozpatrywać indywidualnie.

Zgłaszanie naruszeń

Postępowanie identyczne jak na etapie naboru wstępnych pomysłów na innowacje społeczne.

5.3. Etap testowania innowacji społecznych

5.3.1. Dane innowatorów testujących innowacje (uczestników projektu grantowego)

Administrator: Instytucja Zarządzająca

Procesor: podmiot prowadzący inkubator

Podprocesor: podmiot, któremu podmiot prowadzący inkubator powierzył przetwarzanie danych (jeśli dotyczy)

Odbiorca: podmiot prowadzący inkubator, podmiot, który na jego zlecenie uczestniczy w realizacji projektu tego inkubatora, podmiot realizujący badania ewaluacyjne na zlecenie Instytucji Zarządzającej lub podmiotu prowadzącego inkubator, specjalistyczna firma realizująca na zlecenie Instytucji Zarządzającej oraz podmiotu realizującego inkubator kontrole i audyt w ramach PO WER, a także podmiot świadczący na rzecz Instytucji Zarządzającej usługi związane z obsługą i rozwojem systemów teleinformatycznych

Cel przetwarzania danych: realizacja projektu grantowego, w szczególności potwierdzenie kwalifikowalności wydatków, udzielanie wsparcia, monitoring, ewaluacja, kontrola, audyt i sprawozdawczość oraz działania informacyjno-promocyjne w ramach PO WER

Podstawa prawna: art. 6 ust .1 lit. c RODO (prawny obowiązek ciążący na administratorze)[11]

Termin usunięcia: po rozliczeniu Programu Operacyjnego Wiedza Edukacja Rozwój 2014–2020 oraz zakończeniu archiwizowania dokumentacji (o upływie tego terminu poinformuje Instytucja Zarządzająca).

Rejestr, w którym należy odnotować proces: rejestr kategorii czynności przetwarzania danych

[11] Wszystkie akty prawne, które zobowiązują Instytucję Zarządzającą do przetwarzania danych uczestników projektu grantowego, są wymienione w klauzuli informacyjnej będącej częścią oświadczenia uczestnika projektu grantowego.

Administratorem danych osobowych innowatorów testujących innowacje (uczestników projektu grantowego) jest już Instytucja Zarządzająca, a sam podmiot prowadzący inkubator jest procesorem, któremu Instytucja Zarządzająca powierzyła przetwarzanie tych danych w umowie o dofinansowanie projektu. Nie ma tutaj znaczenia, że to podmiot prowadzący inkubator sam pozyskuje dane osobowe uczestników projektu grantowego i przekazuje je Instytucji Zarządzającej – w rozumieniu RODO to ona jest administratorem danych osobowych, a podmiot prowadzący inkubator jest ich procesorem.

Podstawą prawną przetwarzania danych osobowych przez administratora jest prawny obowiązek ciążący na Instytucji Zarządzającej, a podstawą prawną przetwarzania danych osobowych przez podmiot prowadzący inkubator – umowa powierzenia przetwarzania danych osobowych zawarta z Instytucją Zarządzającą.

Zakres przetwarzanych danych osobowych

Jako że w odniesieniu do tych danych podmiot prowadzący inkubator nie jest administratorem danych, a jedynie procesorem, który przetwarza je na polecenie administratora – Instytucji Zarządzającej – to nie on decyduje o tym, jakie dane będą przetwarzane i w jaki sposób. Umowa o dofinansowanie projektu zobowiązuje go bowiem do gromadzenia i przetwarzania danych wskazanych w niej przez IZ.

W umowie o dofinansowanie Instytucja Zarządzająca umocowała podmiot prowadzący inkubator do wydawania i odwoływania imiennych upoważnień do przetwarzania danych osobowych (ich wzór stanowią załączniki 9 i 10 do umowy o dofinansowanie) w prowadzonych centralnie dwóch zbiorach danych osobowych (obsługiwanych w systemie SL2014):

- Program Operacyjny Wiedza Edukacja Rozwój,
- Centralny system teleinformatyczny wspierający realizację programów operacyjnych.

Upoważnienie to dotyczy zakresu niezbędnego do wykonywania zadań związanych z realizacją projektu. Podmiot prowadzący inkubator ma obowiązek przechowywania upoważnień w swojej siedzibie oraz wyznaczenia przynajmniej jednej osoby legitymującej się imiennym upoważnieniem do przetwarzania danych osobowych

odpowiedzialnej za nadzór nad zarchiwizowaną dokumentacją do dnia zakończenia jej archiwizowania. Upoważnienia do przetwarzania danych osobowych w zbiorze Centralny system teleinformatyczny wspierający realizację programów operacyjnych wydaje wyłącznie Instytucja Zarządzająca.

Zgodnie z umową inkubator, w imieniu Instytucji Zarządzającej, realizuje wobec uczestników projektu grantowego tzw. obowiązek informacyjny. Musi poinformować ich szczegółowo o przetwarzaniu ich danych w projekcie, przedkładając im do podpisania oświadczenie uczestnika projektu grantowego, którego wzór znajduje się w załączniku nr 8 do umowy o dofinansowanie. Zasadniczej treści oświadczenia nie powinno się modyfikować. Należy je tylko uzupełnić we wskazanych miejscach.

Umowa zawarta z Instytucją Zarządzającą zezwala inkubatorowi, jako procesorowi danych osobowych, na podpowierzenie przetwarzania danych uczestników projektu grantowego, ale jest to obwarowane pewnymi wymogami, których bezwzględnie należy przestrzegać.

Jednym z takich warunków jest obowiązek zgłoszenia IZ zamiaru takiego podpowierzenia – IZ daje sobie bowiem 7 dni roboczych na wyrażenie sprzeciwu.

Umowa podpowierzenia przetwarzania danych osobowych, jaką podmiot prowadzący inkubator będzie zawierał, musi zobowiązywać podprocesora do wydawania imiennych upoważnień swoim pracownikom na takich samych zasadach, jakie obowiązują podmioty prowadzące inkubator przy wydawaniu upoważnień swoim pracownikom (czyli imienne upoważnienie przygotowane zgodnie z wzorami z załącznika 9 i 10 do umowy o dofinansowanie). Instytucja Zarządzająca zobowiązuje też inkubator do tego, by podmioty świadczące usługi na jego rzecz zagwarantowały wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa, odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych tak, aby przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Załącznikiem do umowy z podprocesorem może być też omawiana wcześniej lista kontrolna dla podmiotów, którym powierza się przetwarzanie danych.

W umowie podpowierzenia należy także wskazać, że podprocesor ponosi odpowiedzialność (zarówno wobec osób trzecich, jak i wobec administratora) za szkody powstałe w związku z nieprzestrzeganiem ustawy o ochronie danych

osobowych, RODO, przepisów prawa powszechnie obowiązującego dotyczącego ochrony danych osobowych oraz za przetwarzanie powierzonych do przetwarzania danych osobowych niezgodnie z umową powierzenia przetwarzania danych osobowych. Podmioty, którym inkubator powierza przetwarzanie danych osobowych, mają także obowiązek prowadzenia rejestru wszystkich kategorii czynności przetwarzania, o którym mowa w art. 30 ust. 2 RODO.

Umowa z Instytucją Zarządzającą zobowiązuje także podmiot prowadzący inkubator do przekazania jej wykazu podmiotów, którym powierzono przetwarzanie danych osobowych. Wykaz podmiotów powinien zawierać co najmniej nazwę podmiotu oraz dane kontaktowe podmiotu. Wzór wykazu podmiotów, którym powierzono przetwarzanie, znajduje się w załączniku nr 13.

Prawa osób, których dane dotyczą

Ponieważ administratorem danych osobowych innowatorów testujących innowacje (uczestników projektu grantowego) jest Instytucja Zarządzająca, to ona jest gospodarzem całego procesu i to ona rozpatruje żądania osób, których dane dotyczą. Wyjątkiem jest prawo dostępu do danych i prawo do ich sprostowania. Tym zajmuje się inkubator jako podmiot odpowiedzialny za gromadzenie danych zgodnych ze stanem faktycznym.

W przypadku skierowania do inkubatora innego żądania dotyczącego danych osobowych, należy je przekazać inspektorowi ochrony danych powołanemu w Instytucji Zarządzającej.

Zgłaszanie naruszeń

Inna – względem wcześniejszych etapów – rola podmiotu prowadzącego inkubator pociąga za sobą także zmianę obowiązków związanych ze zgłaszaniem naruszeń dotyczących danych osobowych innowatorów testujących innowacje (uczestników projektu grantowego). W przypadku stwierdzenia takiego naruszenia inkubator nie zgłasza go do Urzędu Ochrony Danych Osobowych, ale do Instytucji Zarządzającej (za pośrednictwem powołanego w niej inspektora ochrony danych). Powinien to zrobić

bez zbędnej zwłoki, nie później niż w ciągu 24 godzin. To bowiem Instytucja Zarządzająca, jako administrator danych uczestników projektu grantowego, jest na tym etapie odpowiedzialna za komunikację z Urzędem Ochrony Danych Osobowych.

5.3.2. Dane uczestników testowania

Administrator: innowator

Procesor: podmiot, któremu powierzono przetwarzanie danych (jeśli dotyczy)

Odbiorca: podmiot, któremu innowator udostępnił lub zamierza udostępnić dane uczestników testowania (jeśli dotyczy)

Cel: testowanie innowacji społecznej

Podstawa prawna: art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. b RODO (zgoda osoby, której dane dotyczą)

Termin usunięcia: po ustaniu celu przetwarzania (czyli zakończeniu testowania innowacji) lub wycofaniu zgody przez uczestnika testowania innowacji

Rejestr, w którym należy odnotować proces: rejestr czynności przetwarzania danych prowadzony przez innowatora

Dane uczestników testowania przetwarzane są przez innowatorów, którzy są administratorami tych danych. Podmiot prowadzący inkubator jest natomiast możliwym odbiorcą danych jako podmiot, któremu innowatorzy mogą ujawnić dane osób uczestniczących w testowaniu, np. na potrzeby ewaluacji danej innowacji lub jej upowszechniania. To samo dotyczy także wizerunków, na których przetwarzanie innowatorzy pozyskali zgodę od uczestników testowania i przekazali je inkubatorowi w celach promocji i upowszechniania innowacji. Będą to jednak odrębne procesy i jako takie zostały omówione niżej. To, co jest jednak istotne na tym etapie, to pozyskiwanie zgody uczestników testowania innowacji społecznych, jeśli ich dane mają być wykorzystane w celu innym niż samo testowanie innowacji, w której uczestniczą.

Innowatorami na tym etapie mogą być osoby fizyczne oraz podmioty o różnym stopniu świadomości swoich wynikających z RODO obowiązków związanych z przetwarzaniem danych uczestników testowania innowacji. Zachęcamy więc podmioty prowadzące inkubatory do przygotowania wytycznych dla swoich innowatorów lub przeprowadzenia szkoleń pomagających innowatorom zrozumieć obowiązki wynikające z RODO.

Prawa osób, których dane dotyczą

Ponieważ podstawą przetwarzania danych osobowych uczestników testowania innowacji jest ich zgoda na przetwarzanie danych osobowych przez innowatora w celach niezbędnych do tego testowania, przysługuje im prawo wycofania zgody w dowolnym momencie. Innowator, jako administrator danych uczestników, ma obowiązek poinformować ich o tym prawie w klauzuli informacyjnej załączonej do zgody na przetwarzanie danych, którą podpisują. Uczestnikom testowania innowacji, poza prawem do wycofania zgody w dowolnym momencie, przysługują wszystkie inne omawiane wcześniej prawa z wyjątkiem prawa do wniesienia sprzeciwu – jako że podstawą przetwarzania danych jest dobrowolna zgoda osoby, której dane dotyczą, trudno, żeby wnosiła sprzeciw wobec własnej zgody. Może po prostu tę zgodę wycofać i skorzystać z tzw. prawa do bycia zapomnianym (czyli zażądać usunięcia wszystkich dotyczących jej danych).

Zgłaszanie naruszeń

Zgłaszanie ewentualnych naruszeń na tym etapie jest obowiązkiem innowatora. Mają tutaj zastosowane wytyczne omówione w punkcie dotyczącym przetwarzania danych autorów wstępnych pomysłów na innowacje społeczne omówione w podrozdziale 5.1.1.

5.3.3. Dane osób wykorzystywane na potrzeby ewaluacji

Administrator: podmiot prowadzący inkubator

Procesor: podmiot, któremu inkubator powierzył przetwarzanie danych (jeśli dotyczy) – może to być np. zewnętrzny wobec niego podmiot realizujący samą ewaluację, a także podmiot świadczący usługi informatyczne dotyczące serwisów, w których dane uczestników innowacji są przetwarzane

Odbiorca: podmiot, któremu inkubator udostępnił lub zamierza udostępnić dane uczestników testowania (jeśli dotyczy)

Cel: ewaluacja innowacji społecznej

Podstawa prawna: art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. b RODO (zgoda osoby, której dane dotyczą)

Termin usunięcia: po ustaniu celu przetwarzania (czyli zakończeniu ewaluacji innowacji) lub wycofaniu zgody przez uczestnika testowania innowacji

Rejestr, w którym należy odnotować proces: rejestr czynności przetwarzania danych

Dane uczestników testowania innowacji, które na podstawie ich zgody przekazane zostały podmiotowi prowadzącemu inkubator w celu przeprowadzenia ewaluacji, są przez niego przetwarzane w celach i w sposób przez niego ustalony. Oznacza to, że po otrzymaniu danych osobowych podmiot prowadzący inkubator z odbiorcy staje się administratorem tych danych i przetwarza je w celu ewaluacji innowacji społecznych.

Podstawą prawną przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą, a samo przetwarzanie odbywa się na zasadach opisanych w części dotyczącej przetwarzania danych pomysłodawców innowacji społecznych.

5.4. Etap upowszechniania innowacji społecznych

5.4.1. Dane innowatorów, których innowacje są upowszechniane

Administrator: podmiot prowadzący inkubator

Procesor: podmiot, któremu inkubator powierzył przetwarzanie danych (jeśli dotyczy) – może to być np. zewnętrzny wobec niego podmiot wspierający upowszechnianie, a także podmiot świadczący usługi informatyczne dotyczące serwisów, w których dane uczestników innowacji są przetwarzane

Odbiorca: Instytucja Zarządzająca, każdy podmiot, któremu inkubator udostępnił lub zamierza udostępnić dane innowatorów w celach dalszego upowszechniania ich innowacji (jeśli dotyczy)

Cel: upowszechnianie innowacji społecznej

Podstawa prawna: art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. b RODO (zgoda osoby, której dane dotyczą)

Termin usunięcia: po wycofaniu zgody przez innowatora

Rejestr, w którym należy odnotować proces: rejestr czynności przetwarzania danych

Dane innowatorów, które na podstawie ich zgody zostały przekazane podmiotowi prowadzącemu inkubator w celu upowszechniania innowacji, są przez niego przetwarzane w celach i w sposób przez niego ustalony. Oznacza to, że po otrzymaniu danych osobowych podmiot prowadzący inkubator z odbiorcy staje się administratorem tych danych i przetwarza je w celu upowszechniania innowacji społecznych. Ponieważ Instytucja Zarządzająca jest na tym etapie odbiorcą danych osobowych i może je wykorzystywać we własnych działaniach związanych z upowszechnianiem innowacji, należy w klauzuli informacyjnej przy pozyskiwaniu zgody na takie przetwarzanie poinformować o tym innowatora.

Podstawą prawną przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą, a samo przetwarzanie odbywa się na zasadach opisanych w części dotyczącej przetwarzania danych pomysłodawców innowacji społecznych. Oznacza to, że zgodę tę innowator może w dowolnym momencie wycofać, co dla podmiotu prowadzącego inkubator skutkuje brakiem możliwości dalszego przetwarzania danych w celu upowszechniania innowacji. Wycofanie zgody nie wpływa jednak na zgodność z prawem przetwarzania danych, którego podmiot prowadzący inkubator dokonał przed wycofaniem tej zgody, nie ma zatem obowiązku usuwać danych osobowych innowatorów z już wydanych lub opublikowanych przed wycofaniem tej zgody materiałów promujących innowacje.

5.4.2. Dane uczestników testowania wykorzystywane w ramach upowszechniania

Administrator: podmiot prowadzący inkubator

Procesor: podmiot, któremu inkubator powierzył przetwarzanie danych (jeśli dotyczy) – może to być np. zewnętrzny wobec niego podmiot wspierający upowszechnianie, a także podmiot świadczący usługi informatyczne dotyczące serwisów, w których dane uczestników innowacji są przetwarzane

Odbiorca: Instytucja Zarządzająca oraz każdy podmiot, którym inkubator udostępnił lub zamierza udostępnić dane uczestników testowania w celach dalszego upowszechniania innowacji (jeśli dotyczy)

Cel: upowszechnianie innowacji społecznej

Podstawa prawna: art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. b RODO (zgoda osoby, której dane dotyczą)

Termin usunięcia: po wycofaniu zgody przez uczestnika testowania innowacji

Rejestr, w którym należy odnotować proces: rejestr czynności przetwarzania danych

Dane uczestników testowania innowacji (w tym np. ich wizerunek), które na podstawie ich zgody przekazane zostały podmiotowi prowadzącemu inkubator, są przez niego przetwarzane na zasadach takich samych, jakie miały zastosowanie do omówionego wyżej przetwarzania danych innowatorów w celach związanych z upowszechnianiem innowacji.

Ponieważ upowszechnianie wiąże się często z publikowaniem wizerunku osób (innowatorów i osób uczestniczących w testowaniu innowacji), chcemy przy tej okazji przypomnieć, że wizerunek umożliwiający zidentyfikowanie osoby, którą przedstawia, jest sam w sobie daną osobową w rozumieniu RODO (nie muszą towarzyszyć mu żadne inne dane osobowe). W związku z tym, nawet jeśli publikujemy jedynie wizerunki osób, zobowiązani jesteśmy do wypełnienia wszystkich formalności związanych z przetwarzaniem danych osobowych. Przypominamy też, że publikacja wizerunku podlega przepisom Ustawy o prawie autorskim i prawach pokrewnych, wymaga więc nie tylko zgody osoby widniejącej na wizerunku, lecz także posiadania stosownych praw autorskich do samej fotografii.

6. Lista kontrolna dla inkubatora

W poradniku omówiliśmy obowiązki podmiotu prowadzącego inkubator wynikające z powszechnych przepisów i umowy o dofinansowanie projektu. Poniżej podsumowujemy je w formie listy kontrolnej, zachęcając do sprawdzenia z jej pomocą, jakie obszary ochrony danych wymagają jeszcze uwagi i dopracowania.

Namawiamy, aby traktować poniższą listę jak narzędzie wspierające proces wdrażania RODO w inkubatorach. Nie chcielibyśmy, by stała się straszakiem, który może sprawić jedynie, że perspektywa konieczności dostosowania się do obowiązków będzie jeszcze bardziej zniechęcająca.

Zadanie	**Status**	**Uwagi**
Inkubator prowadzi rejestr czynności przetwarzania danych dla danych, których jest administratorem	☐ tak ☐ nie	
Inkubator prowadzi rejestr kategorii czynności przetwarzania danych dla danych, których jest procesorem	☐ tak ☐ nie	
Przeprowadzono analizę procesów przetwarzania danych pod kątem obowiązku powołania inspektora ochrony danych	☐ tak ☐ nie ☐ nie dotyczy	
Przeprowadzono i udokumentowano analizę ryzyka związanego z przetwarzaniem danych osobowych	☐ tak ☐ nie	
Wprowadzono adekwatne do wyników analizy ryzyka zabezpieczenia danych	☐ tak ☐ nie	
Wobec każdej osoby, której dane są przetwarzane, spełniono obowiązek informacyjny	☐ tak ☐ nie	
Pozyskano zgody na wykorzystanie wizerunku innowatorów i uczestników testowania, jeśli mają być wykorzystane do upowszechniania	☐ tak ☐ nie ☐ nie dotyczy	

Zadanie	Status	Uwagi
Po zakończeniu rekrutacji pomysłodawców usunięto dane zbędne na dalszych etapach	☐ tak ☐ nie	
Opracowano politykę bezpieczeństwa danych lub inny wewnętrzny dokument porządkujący przetwarzanie danych	☐ tak ☐ nie	
Wyznaczono inspektora ochrony danych lub osobę odpowiedzialną za bezpieczeństwo danych	☐ tak ☐ nie ☐ nie dotyczy	
Każda osoba dopuszczona do przetwarzania danych posiada imienne upoważnienie do przetwarzania	☐ tak ☐ nie	
Każda osoba dopuszczona do przetwarzania danych podpisała oświadczenie o zachowaniu poufności	☐ tak ☐ nie	
Przeszkolono osoby odpowiedzialne za przetwarzanie danych lub poinstruowano je, jak właściwie postępować z danymi	☐ tak ☐ nie ☐ nie dotyczy	
Powierzenie przetwarzania danych odbywa się na podstawie pisemnej umowy powierzenia	☐ tak ☐ nie ☐ nie dotyczy	
Przekazano Instytucji Zarządzającej wykaz podmiotów, którym podpowierzono przetwarzanie	☐ tak ☐ nie ☐ nie dotyczy	
Instytucja Zarządzająca jest informowana z odpowiednim wyprzedzeniem o zamiarze powierzenia przetwarzania	☐ tak ☐ nie ☐ nie dotyczy	

7. Załączniki

1. Zgoda na przetwarzanie wizerunku do celów promocyjnych (1a dotyczy innowatorów, 1b – uczestników testowania innowacji)
2. Uchwała w sprawie niepowołania Inspektora Ochrony Danych
3. Wzór ewidencji upoważnień
4. Wzór umowy powierzenia przetwarzania danych
5. Lista kontrolna dla pomiotów, którym będzie powierzone przetwarzanie
6. Przykładowy arkusz analizy ryzyka
7. Notatka z przeprowadzenia analizy ryzyka
8. Przykładowy wyciąg z zasad przetwarzania danych
9. Wzór rejestru przetwarzania danych
10. Instrukcja prowadzenia rejestru przetwarzania danych
11. Wzór ewidencji naruszeń
12. Notatka z usunięcia danych osobowych
13. Wykaz podmiotów, którym powierzono przetwarzanie

Załączniki w wersji edytowalnej znajdują się na stronie:
https://innowacjespoleczne.pl/element_biblioteki/rady-na-rodo

www.innowacjespoleczne.pl