CZĘŚĆ I.
PODSTAWOWE INFORMACJE

Podstawa prawna

Podstawę prawną niniejszego dokumentu (dalej: Procedura) stanowią:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.Urz.UE.L. 119/1 [RODO],
- Ustawa z 10 maja 2018 r. o ochronie danych osobowych, Dz.U.2019.1781 z późn. zm. [ODO],
- Inne powszechnie obowiązujące przepisy prawa dotyczące ochrony danych osobowych lub bezpieczeństwa informacji, w tym przepisy sektorowe oraz regulacje z zakresu cyberbezpieczeństwa (takie jak rozporządzenie DORA czy dyrektywa NIS2, o ile znajdują zastosowanie).

Celem dokumentu jest:

- Wprowadzenie systemu ochrony danych osobowych,
- Inicjowanie działań podnoszących efektywność i sprawność w zakresie ochrony danych osobowych w Fundacji Edukacyjnej ODiTK w Gdańsku (dalej: Fundacja),
- Wskazanie działań, jakie należy wykonać oraz jakie ustanowić zasady i reguły postępowania, aby Administrator danych oraz jego pracownicy i współpracownicy mogli właściwie wykonywać zadania w zakresie ochrony danych osobowych.

Zakres zastosowania

Dokument dotyczy pracowników i współpracowników Fundacji przetwarzających dane osobowe, a także każdej osoby mającej dostęp do tychże danych osobowych. Dokument może obejmować również podmioty, które zawrą umowę z Fundacją, na podstawie której powierzone zostaną im dane osobowe do przetwarzania. Procedurę stosują wszystkie osoby i podmioty, które mają dostęp do danych osobowych w Fundacji. Obszar, w którym przetwarzane są dane osobowe, znajduje się w siedzibie Fundacji. Dane osobowe przetwarzane w sposób tradycyjny przetwarzane są na ww. obszarze. Z Procedurą niniejszą

należy zapoznać wszystkich pracowników oraz współpracowników mających dostęp do danych osobowych.

Podstawowe definicje

Poniżej zamieszczone są podstawowe definicje z zakresu ochrony danych osobowych. Są to pojęcia kluczowe do codziennej pracy z danymi osobowymi. Instytucje incydentalne zostaną wyjaśnione w dalszych częściach niniejszej Procedury.

- **Administrator danych** – Podmiot, który decyduje o celach i sposobach przetwarzania danych osobowych (np. pracodawca jest administratorem danych pracowników). Administrator danych osobowych może powołać Inspektora Ochrony Danych Osobowych.

- **Dane osobowe** – Informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

- **Przetwarzanie** – Operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

- **Pseudonimizacja** – Przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

- **Zbiór danych** – Uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

- **Zgoda** (osoby, której dane dotyczą) – Dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Obowiązki Administratora danych oraz schematy postępowania

1. **Wykaz obowiązków Administratora danych**

W świetle RODO przetwarzanie danych osobowych jest możliwe, gdy spełnione zostaną łącznie następujące warunki:

- Administrator danych uwzględnia zasady ochrony danych już w fazie planowania wdrożenia nowej usługi (**zasada privacy by design**) – zob. rozdział V,

- W przypadku, gdy planowany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, Administrator danych przed rozpoczęciem przetwarzania przeprowadza ocenę skutków dla ochrony danych osobowych (Data Protection Impact Assessment, DPIA) zgodnie z art. 35 RODO; jeśli wynik oceny wykaże wysokie ryzyko pomimo zastosowania środków zaradczych, Administrator przed rozpoczęciem przetwarzania konsultuje się z organem nadzorczym (art. 36 RODO).

- Do przetwarzania danych osobowych dopuszczone są wyłącznie osoby, które posiadają stosowne upoważnienie – zob. rozdział VI,

- Dane osobowe są przetwarzane zgodnie z prawem – istnieje przepis prawa zezwalający Administratorowi danych na ich przetwarzanie – zob. rozdziały VII–VIII,

- Administrator danych wykonuje obowiązek informacyjny względem osoby, której dane przetwarza – zob. rozdział IX,

- Dane osobowe powinny być przetwarzane jedynie w zakresie niezbędnym do realizacji celu, dla którego zostały zebrane oraz w czasie koniecznym do jego realizacji, **zgodnie z zasadą minimalizacji danych**. Nie należy zbierać dodatkowych danych osobowych niż jest to konieczne – zob. rozdział VII,

- W przypadku zmiany celu przetwarzania należy postąpić analogicznie jak przy pierwotnym zebraniu danych osobowych – tj. Administrator danych musi posiadać prawną podstawę ich przetwarzania, a o zmianie celu należy powiadomić osobę, której dane dotyczą (o ile uprzednio już tego nie uczyniono) – zob. rozdział VII,

- Administrator danych ma obowiązek respektować prawa osób, których dane osobowe przetwarza – zob. rozdział X (w tym pracowników i współpracowników – zob. rozdział XV),

- Administrator danych zobowiązany jest zapewnić bezpieczeństwo przetwarzanych danych osobowych – zob. rozdział XIII,

- Administrator danych prowadzi rejestr czynności przetwarzania danych – zob. rozdział XII,

- W przypadku powierzenia przetwarzania danych osobowych osobom trzecim, Administrator danych zapewnia zgodność powierzenia z prawem, w tym odpowiednią konstrukcję umowy powierzenia – zob. rozdział XI,

- Administrator danych dokumentuje wszelkie naruszenia ochrony danych osobowych, prowadzi rejestr naruszeń obejmujący okoliczności naruszenia, jego skutki oraz podjęte działania zaradcze (wymóg art. 33 ust. 5 RODO) – zob. rozdział XIV,

- W przypadku wykrycia naruszenia zasad przetwarzania danych osobowych Administrator danych zobowiązany jest do podjęcia odpowiednich działań – zob. rozdział XIV.

2. **Podstawowe schematy postępowania przez Administratora danych**

Schemat postępowania Administratora danych – zbieranie danych osobowych

- Uzyskanie zgody osoby, której dane są gromadzone, na ich przetwarzanie – zgoda może być zawarta w treści umowy, odrębnym oświadczeniu lub w opcji wyboru formularza na stronie internetowej (zob. rozdział VIII),

- Weryfikacja, czy wszystkie dane osobowe są niezbędne do realizacji celów Administratora danych; gdy zgromadzono dane zbędne, należy je usunąć (zob. rozdział VII),

- Wykonanie obowiązku informacyjnego względem tej osoby – wymagane informacje mogą być zawarte w treści umowy, w odrębnym dokumencie, w mailu lub na stronie internetowej (zob. rozdział IX),

- Przetwarzanie danych zgodnie z opisanymi w tym dokumencie zasadami,

- W przypadku, gdy dane osobowe stały się zbędne dla realizacji celu, dla którego je zebrano (np. umowa została wykonana i rozliczona), należy je usunąć albo zanonimizować, chyba że istnieje inna podstawa prawna ich dalszego przetwarzania.

Schemat postępowania na wypadek utraty ciągłości przetwarzania danych osobowych (np. awarii systemu lub wystąpienia innego incydentu):

- Niezwłoczne podjęcie działań mających na celu zapewnienie przywrócenia ciągłości przetwarzania danych,

- Weryfikacja zabezpieczeń danych osobowych pod kątem wykrycia ich naruszenia,
- Podjęcie działań mających na celu zapewnienie prawidłowego funkcjonowania środków zapewniających bezpieczeństwo danych osobowych,
- W przypadku zniszczenia albo uszkodzenia dokumentów lub plików zawierających dane osobowe – odtworzenie ich w oparciu o kopie zapasowe oraz inne posiadane materiały,
- W przypadku naruszenia zabezpieczeń: odtworzenie zabezpieczeń lub wprowadzenie zabezpieczeń dodatkowych. Do czasu przywrócenia pełnej funkcjonalności dotychczasowych zabezpieczeń należy wprowadzić zabezpieczenia tymczasowe, które zapewnią niezbędny stopień bezpieczeństwa danych osobowych (zob. rozdział XIII),
- Weryfikacja zakresu naruszenia,
- Ustalenie osób odpowiedzialnych za zaistniałe naruszenie,
- Zgłoszenie naruszenia właściwym organom, a także osobom, których dane osobowe zostały naruszone (zob. rozdział XIV),
- Jeżeli okaże się to konieczne, uzupełnienie procedur celem przeciwdziałania podobnym zdarzeniom w przyszłości.

Sposób wypełnienia wyżej wskazanych wymogów warunkujących zgodne z prawem przetwarzanie danych osobowych zostanie przedstawiony w dalszych częściach niniejszej Procedury. *Procedura przekazywania danych osobowych klientów do banku została uregulowana w odrębnym dokumencie pn. „Opis rozwiązań technicznych i organizacyjnych, zapewniających bezpieczne i prawidłowe wykonywanie przez przedsiębiorcę powierzonych czynności, w szczególności ochronę tajemnicy prawnie chronionej”.*

CZĘŚĆ II. INFORMACJE SZCZEGÓŁOWE

1. **Projektowanie ochrony danych osobowych**
   Administrator danych ma ogólny obowiązek uwzględniania zasad ochrony danych osobowych w procesie projektowania i wdrażania nowych usług. Administrator danych ma obowiązek uwzględnić i wdrożyć odpowiednie środki techniczne i organizacyjne zapewniające bezpieczeństwo przetwarzania danych osobowych – środki te zostały szczegółowo przedstawione w odrębnym punkcie Procedury. Ponadto, Administrator danych zapewnia domyślną ochronę danych osobowych (privacy by

default), tzn. systemy i usługi zostały skonfigurowane w sposób gwarantujący, że domyślnie przetwarzane są wyłącznie dane niezbędne do osiągnięcia określonych celów, a dostęp do danych osobowych mają tylko uprawnione osoby.

2. Upoważnienie do przetwarzania danych osobowych
Administrator danych albo podmiot przetwarzający (podmiot, z którym Administrator zawarł umowę o powierzenie przetwarzania danych osobowych) zobowiązani są do udzielenia upoważnień osobom dopuszczonym do przetwarzania danych osobowych. Niedozwolona jest praca z danymi osobowymi bez upoważnienia pochodzącego od jednego ze ww. podmiotów.

Przykładowe upoważnienie

Data nadania upoważnienia:

…….

Upoważnienie do przetwarzania danych osobowych

Upoważniam Panią/Pana ……
o numerze PESEL ……, zatrudnioną/-ego na stanowisku ……,
w ……

1.

do dostępu do następujących zbiorów danych osobowych w celu ich przetwarzania:
– ……
– ……
– ……

Identyfikator/Login: ……
Okres trwania upoważnienia: ……

Wystawił: ……

(podpis w imieniu Administratora Danych Osobowych)

Osoba upoważniona do przetwarzania danych objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia, oraz do zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej: ……

3. Legalność przetwarzania danych osobowych
O legalności przetwarzania danych osobowych decyduje nie tylko istnienie

podstawy w przepisach prawa, ale także zgodność tejże podstawy z zakresem przetwarzanych danych. Oznacza to, że Administrator może przetwarzać dane wyłącznie, gdy:

- Istnieje podstawa prawna uprawniająca Administratora danych do ich przetwarzania (patrz niżej),
- Dane osobowe przetwarzane są wyłącznie w celu wynikającym z danej podstawy prawnej oraz zakomunikowanym osobie, której dane dotyczą (np. w celu świadczenia oraz rozliczenia usługi),
- Dane osobowe są gromadzone tylko w zakresie i czasie niezbędnym do realizacji celu, o którym mowa w pkt 2 (po wykonaniu i rozliczeniu usługi należy je usunąć, chyba że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie danych w innym celu albo istnieje inna podstawa prawna ich przetwarzania – patrz ramka).

Zmiana celu przetwarzania – przykład

Klient wyraził zgodę na przetwarzanie danych osobowych w celu realizacji usługi. Klient nie wyrażał innych zgód.

Po wykonaniu i rozliczeniu umowy, Administrator danych zamierza w dalszym ciągu przetwarzać te dane osobowe, tylko że w celu marketingu bezpośredniego.

Aby było to możliwe, Administrator danych powinien powiadomić tę osobę o zmianie celu przetwarzania oraz przesłać jej stosowną informację (zob. rozdział IX). Dane osobowe mogą być dalej przetwarzane w celu marketingowym, chyba że osoba skorzysta z przysługujących jej uprawnień, które okażą się zasadne (zob. rozdział X).

RODO za legalne uznaje przetwarzanie danych osobowych, gdy wystąpiła co najmniej jedna z niżej wskazanych przesłanek. Oznacza to w szczególności, że Administrator danych nie musi każdorazowo dysponować zgodą osoby, której dane przetwarza – wystarczające jest spełnienie chociażby jednej z niższej wymienionych podstaw:

- osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów,
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze,
- przetwarzanie jest nezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,

- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi,

- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

W praktyce obrotu gospodarczego najczęściej występującymi przesłankami są:

- **odebranie zgody** od osoby, której dane mają być przetwarzane – należy pamiętać, że oświadczenie o wyrażeniu zgody musi spełniać ustawowe wymagania (wskazane dalej),

- **realizacja i zawarcie umowy** – brak odrębnej zgody klienta albo kontrahenta nie uniemożliwia przetwarzania danych osobowych, gdy bez tego procesu nie jest możliwe wykonanie umowy na jego rzecz (w tym utrzymywanie bieżącego kontaktu, wystawienie faktury albo rachunku, dochodzenie należności itp.). Przesłanka ta obejmuje również możliwość przetwarzania danych osobowych przed zawarciem umowy, jeżeli czynności te zmierzają do jej zawarcia lub wykonania (np. prowadzenie negocjacji w zakresie oferty lub treści umowy, przesłanie próbek, wzorów, referencji, podjęcie innych czynności na wyraźne żądanie klienta/kontrahenta zmierzających do wykonania przyszłej umowy, np. umówienie spotkania, przesłanie ofert itp.),

- **przetwarzanie danych w uzasadnionych celach administratora** (np. marketing bezpośredni własnych towarów i usług) – decydując się na tę przesłankę przetwarzania danych osobowych należy pamiętać o ochronie praw osoby, której dane dotyczą, w tym prawa do prywatności.

4. Klauzula zgody na przetwarzanie danych osobowych

Klauzula wyrażenia zgody na przetwarzanie danych osobowych musi spełniać niżej wskazane warunki:

- musi być wyrażona w sposób udokumentowany – nie musi przyjmować formy pisemnej, może być wyrażona drogą elektroniczną (np. wiadomość e-mail albo komunikat generowany przez skrypt formularza zamieszczonego na stronie internetowej), a także w każdej innej postaci, o ile Administrator danych jest w stanie, w każdym czasie i bez dodatkowych środków, wykazać fakt udzielenia zgody,

- nie może być łączona z treścią innych zgód, oświadczeń i klauzul odbieranych przez Administratora danych. Przykładowo, jeżeli Administrator danych prócz zgody na przetwarzanie odbiera także zgodę

na przesyłanie informacji handlowej, to obie klauzule powinny być odrębne – dana osoba może wyrazić zgodę na jedną z nich, obie albo żadną z nich,

- klauzula musi zawierać informację o możliwości odwołania zgody w każdym czasie oraz sposobie i skutkach jej odwołania,

- zgoda powinna być udzielona dobrowolnie, co znaczy, że od jej udzielenia nie może być uzależnione świadczenie przez Administratora danych usług, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

Przykład klauzuli zgody:

„Wyrażam zgodę na przetwarzanie moich danych osobowych w zakresie: imię, nazwisko, adres e-mail, numer telefonu przez …, w celu … . Przyjmuję do wiadomości, że w dowolnym momencie mogę odwołać udzieloną zgodę – pisemnie na adres Administratora danych lub mailowo na adres: …, a wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Mam świadomość, że wyrażenie niniejszej zgody jest dobrowolne, jednakże bez jej wyrażenia nie jest możliwe wykonanie na moją rzecz usług … .”

Jeżeli dane osobowe mają być przekazywane innym podmiotom bądź przetwarzane również w innych celach, klauzula niniejsza podlegać będzie dalszemu rozbudowaniu – o czym mowa niżej.

5. Obowiązek informacyjny

Jednym z podstawowych obowiązków Administratora danych jest wykonanie obowiązku informacyjnego względem osoby, której dane są zbierane. Zakres tego obowiązku zależny jest od tego, czy dane osobowe zbierane są bezpośrednio od tej osoby, czy też pozyskiwane od innych administratorów danych.

Obowiązek informacyjny może być wykonany w jeden z następujących sposobów – poprzez przekazanie osobie, której dane są zbierane:

- uprzednio przygotowanej informacji na piśmie,

- informacji drogą elektroniczną (np. jako załącznik do e-maila albo informacji wygenerowanych przez skrypt na stronie internetowej, po wysłaniu przez użytkownika formularza kontaktowego),

- ustnie – na żądanie tej osoby.

Obowiązek informacyjny przy zbieraniu danych osobowych bezpośrednio od osoby, której dane są zbierane, obejmuje:

- tożsamość i dane kontaktowe Administratora danych oraz – gdy ma to zastosowanie – tożsamość i dane kontaktowe przedstawiciela Administratora,
- dane kontaktowe inspektora ochrony danych (IOD) – gdy został powołany,
- cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania,
- prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią – jeżeli przetwarzanie odbywa się na tej podstawie,
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
- informacje o prawie do żądania od Administratora danych dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
- jeżeli przetwarzanie odbywa się na podstawie zgody – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
- informacje o prawie wniesienia skargi na Administratora danych 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, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Przykład informacji:

„W wykonaniu obowiązku informacyjnego, o którym mowa w art. 13 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) informujemy, że:

1. Administratorem Pani/Pana danych osobowych jest … (pełna nazwa, adres, dane kontaktowe Administratora);

2. Pani/Pana dane osobowe przetwarzane będą w celu … na podstawie … (podać podstawę prawną przetwarzania – np. art. 6 ust. 1 lit. b RODO – niezbędność do wykonania umowy) i nie będą udostępniane innym odbiorcom, poza … (ewentualnie podać kategorię odbiorców);

3. Pani/Pana dane osobowe będą przechowywane przez okres … / do czasu … (podać okres przechowywania lub kryteria jego ustalenia);

4. posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu;

5. ma Pani/Pan prawo wniesienia skargi do organu nadzorczego, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych narusza przepisy RODO;

6. podanie danych osobowych jest dobrowolne, jednakże odmowa podania danych może skutkować brakiem możliwości zawarcia umowy/realizacji usługi …;

7. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany i nie będą profilowane.”

(Dalsze elementy obowiązku informacyjnego wymagane przy pozyskiwaniu danych z innych źródeł – art. 14 RODO – zostały pominięte w przykładzie, ale Administrator powinien je uwzględnić, jeśli dotyczy.)

X. Prawa osób, których dane są przetwarzane

RODO przyznaje osobom, których dane dotyczą, szereg praw związanych z przetwarzaniem ich danych osobowych. Administrator danych ma obowiązek respektować te prawa i umożliwić ich realizację. Prawa te obejmują:

- **Prawo dostępu do danych** – osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora potwierdzenia, czy przetwarza on jej dane osobowe, a jeżeli ma to miejsce, do uzyskania dostępu do nich oraz informacji m.in. o celach przetwarzania, kategoriach danych, odbiorcach danych, okresie przechowywania danych, prawach przysługujących tej osobie, źródłach danych (gdy nie zebrano ich od osoby) oraz o zautomatyzowanym podejmowaniu decyzji (art. 15 RODO). Na żądanie osoby Administrator dostarcza kopię danych podlegających przetwarzaniu.

- **Prawo do sprostowania danych** – osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe, a także uzupełnienia niekompletnych danych (art. 16 RODO).

- **Prawo do usunięcia danych (“prawo do bycia zapomnianym”)** – osoba, której dane dotyczą, ma – co do zasady – prawo żądania od Administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a Administrator ma obowiązek bez zbędnej zwłoki dane usunąć, jeżeli zachodzi jedna z okoliczności wskazanych w art. 17 ust. 1 RODO (m.in. dane nie są już niezbędne do celów, w których zostały zebrane, lub osoba cofnęła zgodę, na której opiera się przetwarzanie, i brak innej podstawy prawnej przetwarzania). Prawo do usunięcia danych nie ma charakteru bezwzględnego – RODO przewiduje wyjątki (art. 17 ust. 3), np. gdy przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń.

- **Prawo do ograniczenia przetwarzania** – na mocy art. 18 RODO osoba może żądać od Administratora ograniczenia przetwarzania, jeżeli: kwestionuje prawidłowość danych (na okres pozwalający Administratorowi sprawdzić prawidłowość danych), przetwarzanie jest niezgodne z prawem, a osoba sprzeciwia się usunięciu danych żądając w zamian ich ograniczenia, Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie do ustalenia, dochodzenia lub obrony roszczeń, lub jeśli osoba wniosła sprzeciw – do czasu stwierdzenia, czy prawnie uzasadnione podstawy Administratora są nadrzędne wobec podstaw sprzeciwu osoby.

- **Prawo do przenoszenia danych** – osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła Administratorowi, oraz ma prawo przesłać te dane innemu administratorowi bez przeszkód ze strony Administratora, jeżeli przetwarzanie odbywa się na podstawie zgody lub umowy i w sposób zautomatyzowany (art. 20 RODO).

- **Prawo do sprzeciwu** – osoba, której dane dotyczą, ma prawo, z przyczyn związanych z jej szczególną sytuacją, w dowolnym momencie wnieść sprzeciw wobec przetwarzania jej danych osobowych, jeśli odbywa się ono na podstawie art. 6 ust. 1 lit. e lub f RODO (zadanie realizowane w interesie publicznym / prawnie uzasadniony interes administratora). W przypadku zgłoszenia sprzeciwu Administratorowi nie wolno już przetwarzać tych danych, chyba że wykaże on istnienie ważnych, prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń (art. 21 ust. 1 RODO). Jeżeli jednak dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba ma prawo w dowolnym momencie wnieść sprzeciw (bez dodatkowych warunków)

wobec przetwarzania jej danych w takim celu – wówczas Administrator nie może tych danych dalej przetwarzać do celów marketingu bezpośredniego (art. 21 ust. 2–3 RODO).

- **Prawo do niepodlegania zautomatyzowanemu podejmowaniu decyzji** – na mocy art. 22 RODO osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji opierającej się wyłącznie na zautomatyzowanym przetwarzaniu (w tym profilowaniu) i wywołującej wobec niej skutki prawne lub w podobny sposób na nią istotnie wpływającej. Wyjątki od tej zasady przewidziano m.in. gdy decyzja jest oparta na wyraźnej zgodzie osoby lub jest niezbędna do wykonania umowy. W takich przypadkach osoba ma prawo do uzyskania interwencji ludzkiej ze strony Administratora, do wyrażenia własnego stanowiska i do zakwestionowania takiej decyzji.

Administrator danych informuje osoby, których dane dotyczą, o przysługujących im prawach w momencie zbierania danych (obowiązek informacyjny – zob. rozdział IX). Realizacja praw przez osobę, której dane dotyczą, następuje na jej wniosek. Administrator danych powinien ułatwiać korzystanie z tych praw i odpowiadać na wnioski bez zbędnej zwłoki – co do zasady w terminie do miesiąca. Szczegółowe zasady realizacji praw (w tym możliwe odstępstwa i procedury weryfikacji tożsamości wnioskodawcy) określają przepisy RODO (art. 12–22).

XI. Powierzenie przetwarzania danych osobowych

Administrator danych może powierzyć przetwarzanie danych osobowych innemu podmiotowi (podmiot przetwarzający), ale musi to odbyć się na podstawie pisemnej umowy lub innego instrumentu prawnego zgodnie z art. 28 RODO. W umowie powierzenia należy w szczególności zawrzeć postanowienia dotyczące zakresu i celu przetwarzania, rodzaju danych, kategorii osób, obowiązków i praw Administratora oraz wymogów co do sposobu przetwarzania danych przez podmiot przetwarzający (zgodnie z art. 28 ust. 3 RODO).

Podmiot przetwarzający nie może wykorzystywać ani przetwarzać powierzonych danych w celach innych niż wskazane przez Administratora danych i wynikające z umowy. Po zakończeniu przetwarzania danych (np. po wykonaniu usługi dla Administratora) podmiot przetwarzający jest zobowiązany do zwrotu lub usunięcia danych – według wyboru Administratora.

Administrator danych powinien dokonać weryfikacji, czy podmiot, któremu zamierza powierzyć dane (np. firma zewnętrzna świadcząca usługi IT, księgowe, marketingowe itp.), zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą (art. 28 ust. 1 RODO).

Podmiot przetwarzający, któremu powierzono dane, ma obowiązek zapewnić ich przetwarzanie zgodnie z umową i przepisami prawa – w tym zapewnić poufność, integralność, dostępność danych oraz podporządkować się poleceniom Administratora. Osoby działające z upoważnienia podmiotu przetwarzającego także powinny zobowiązać się do zachowania danych w poufności.

XII. Rejestr czynności przetwarzania

RODO nie przewiduje obowiązku rejestracji zbiorów danych osobowych w krajowym organie administracji. Zamiast tego, każdy Administrator danych osobowych ma obowiązek prowadzenia wewnętrznego rejestru czynności przetwarzania w swojej jednostce organizacyjnej. Powyższe nie dotyczy jednak administratora lub podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa.

Rejestr może być prowadzony w formie pisemnej albo elektronicznej oraz powinien zawierać następujące informacje:

- imię i nazwisko lub nazwę oraz dane kontaktowe Administratora oraz wszelkich współadministratorów (gdy występują), a także – gdy ma to zastosowanie – przedstawiciela Administratora oraz inspektora ochrony danych (gdy zostali ustanowieni/powołani),
- cele przetwarzania,
- opis kategorii osób, których dane dotyczą (np. pracownicy, klienci, kontrahenci) oraz kategorii danych osobowych (np. imię, nazwisko, adres e-mail, telefon itp.),
- gdy ma to zastosowanie – kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
- gdy ma to zastosowanie – informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa lub organizacji, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
- jeżeli jest to możliwe – planowane terminy usunięcia poszczególnych kategorii danych,
- jeżeli jest to możliwe – ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Podmiot przetwarzający (procesor) działający na zlecenie Administratora również ma obowiązek prowadzenia rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu każdego administratora (art. 30 ust. 2 RODO).
W rejestrze tym powinny zostać zamieszczone m.in.: nazwa i dane kontaktowe procesora i Administratora, cele przetwarzania, kategorie przetwarzań dokonywanych w imieniu Administratora, informacje o przekazaniach danych do państw trzecich (jeśli mają miejsce) oraz ogólny opis stosowanych środków bezpieczeństwa.

Rejestr może być udostępniany organowi nadzorczemu na jego żądanie w celu weryfikacji przestrzegania przepisów.

XIII. Bezpieczeństwo przetwarzania danych osobowych

Administrator danych oraz podmiot przetwarzający zobowiązani są do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia danych osobowych. Dobór tych środków należy do ww. podmiotów. Powinny one mieć na względzie takie czynniki jak: stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz zróżnicowane prawdopodobieństwo i wagę ryzyka naruszenia praw lub wolności osób fizycznych. Środki te powinny zapewniać:

- pseudonimizację lub szyfrowanie danych osobowych,
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Środki zapewniające bezpieczeństwo przetwarzania danych osobowych – przykłady:

- pomieszczenia, w których przetwarzane są dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności osób upoważnionych do przetwarzania danych osobowych,
- stosuje się mechanizmy kontroli dostępu do danych (np. indywidualne loginy i hasła); w przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni, a hasło składa się z co najmniej 8 znaków,

- każdy z użytkowników posiada unikalny identyfikator (login) oraz hasło,
- system informatyczny posiada aktualne oprogramowanie antywirusowe oraz zaporę sieciową (firewall), a także wykonywane są automatyczne kopie zapasowe danych,
- urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe, przeznaczone do:
- likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się je w sposób uniemożliwiający odczytanie,
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie,
- naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawy dokonuje się pod nadzorem osoby upoważnionej przez Administratora danych,
- nośniki zawierające dane osobowe, wykorzystywane do celów operacyjnych, w czasie nieobecności w pomieszczeniu osoby upoważnionej, przechowuje się w zamykanych na klucz szafach lub sejfach. W przypadku, gdy zbiór danych osobowych był zapisany na nośniku w sposób trwały i nie będzie dalej wykorzystywany, należy go fizycznie zniszczyć po przeniesieniu danych na dysk serwera lub do innego docelowego systemu,
- komunikacja pomiędzy stacjami roboczymi i serwerami odbywa się w oparciu o bezpieczne protokoły transmisji danych; styk sieci lokalnej z siecią publiczną chroniony jest przez zastosowanie zapory sieciowej (firewall) oraz jej bieżący monitoring.

W przypadku przetwarzania danych osobowych podczas pracy zdalnej lub mobilnej, należy przestrzegać następujących zasad bezpieczeństwa:

- Należy korzystać wyłącznie ze sprzętu komputerowego oraz oprogramowania zatwierdzonego przez Administratora danych do celów pracy zdalnej. Urządzenia używane do pracy zdalnej powinny być odpowiednio zabezpieczone (posiadać aktualne oprogramowanie i aktualne poprawki systemowe, zainstalowane programy antywirusowe i firewalle) oraz chronione hasłem. Nie wolno instalować na nich nieautoryzowanego oprogramowania ani używać niezabezpieczonych prywatnych urządzeń do przetwarzania danych służbowych bez zgody Administratora.
- Połączenie internetowe wykorzystywane do pracy zdalnej powinno być bezpieczne. Zaleca się korzystanie z szyfrowanego połączenia (VPN)

podczas zdalnego dostępu do wewnętrznych systemów Fundacji. Należy unikać korzystania z publicznych, niezabezpieczonych sieci Wi-Fi do celów służbowych – chyba że zastosowano dodatkowe zabezpieczenia, takie jak wspomniane szyfrowane połączenie VPN.

- Podczas pracy zdalnej należy zapewnić, aby osoby postronne nie miały dostępu do ekranu komputera, dokumentów ani rozmów zawierających dane osobowe. Monitor powinien być tak ustawiony, by nie był widoczny dla osób nieupoważnionych, a w razie przerwy w pracy komputer należy zablokować. Dokumenty papierowe zawierające dane osobowe oraz przenośne nośniki danych należy przechowywać w sposób zabezpieczony (np. w zamykanej szafce) i nie pozostawiać ich bez nadzoru.

- Po zakończeniu pracy zdalnej lub w przypadku opuszczenia domowego stanowiska pracy, pracownik powinien wylogować się z wszelkich systemów służbowych i wyłączyć lub zablokować używane urządzenia. Urządzeń służbowych (laptopów, telefonów itp.) nie należy pozostawiać w miejscach publicznych bez nadzoru (np. w samochodzie bez odpowiedniego zabezpieczenia).

- Jeżeli praca zdalna wykonywana jest z wykorzystaniem prywatnego sprzętu komputerowego pracownika, sprzęt ten musi spełniać wymagania bezpieczeństwa określone przez Administratora danych (m.in. powinien mieć aktualny system operacyjny i oprogramowanie zabezpieczające, wskazane jest szyfrowanie dysku oraz silne hasło dostępu). Pracownik zobowiązany jest chronić dane przetwarzane na prywatnym urządzeniu z tą samą starannością, jak na sprzęcie służbowym.

- Wszelkie incydenty naruszenia bezpieczeństwa danych osobowych podczas pracy zdalnej (np. zagubienie lub kradzież urządzenia zawierającego dane, podejrzenie nieuprawnionego dostępu do danych, infekcja złośliwym oprogramowaniem itp.) należy niezwłocznie zgłaszać Administratorowi danych lub wyznaczonemu przez niego personelowi odpowiedzialnemu za bezpieczeństwo (np. Inspektorowi Ochrony Danych, o ile został powołany).

- Pracownik wykonujący pracę zdalną potwierdza zapoznanie się z niniejszymi zasadami ochrony danych osobowych i zobowiązuje się do ich przestrzegania, co powinno zostać udokumentowane (zgodnie z wymogiem art. 6726 §1–2 Kodeksu pracy dotyczącym zasad pracy zdalnej).

XIV. Zgłaszanie naruszeń

RODO wprowadza również – dotychczas nieznany – obowiązek raportowania o wykryciu naruszenia ochrony danych osobowych. Zakres tych obowiązków

zależy od tego, kto naruszenie wykrył, a także od skutków naruszenia – stosowne zestawienie przedstawia poniższa tabela.

Za naruszenie praw lub wolności osób fizycznych uznać można przykładowo naruszenie prawa do prywatności bądź ujawnienie danych osobowych osobie nieupoważnionej.

Procedurę postępowania w przypadku wykrycia naruszeń, wraz z podziałem na ich rodzaje, przedstawia poniższa tabela:

- **Naruszenie nieistotne** – nie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych.
- **Naruszenie skutkuje ryzykiem** naruszenia praw lub wolności osób fizycznych.
- **Naruszenie skutkuje wysokim ryzykiem** naruszenia praw lub wolności osób fizycznych.

Administrator danych: Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, **prowadzi rejestr naruszeń obejmujący** okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

- Przy naruszeniu **nieistotnym**: brak dodatkowych obowiązków poza wewnętrznym udokumentowaniem incydentu (jak wyżej).
- Przy naruszeniu **skutkującym ryzykiem**: zgłoszenie naruszenia organowi nadzorczemu (Prezesowi Urzędu Ochrony Danych Osobowych) w ciągu 72 godzin od stwierdzenia naruszenia.
- Przy naruszeniu **skutkującym wysokim ryzykiem**: zgłoszenie naruszenia organowi nadzorczemu **oraz** zawiadomienie osoby, której dane dotyczą, o naruszeniu (niezwłocznie, w przystępnej formie).

Podmiot przetwarzający (procesor):

- W każdym z powyższych przypadków procesor **niezwłocznie zgłasza** fakt naruszenia Administratorowi danych (który dalej postępuje jak wyżej).
- Zawiadomienie osoby, której dane dotyczą, nie jest wymagane w następujących przypadkach:
- administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,

- administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

- informowanie indywidualne wymagałoby niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

XV. Dane osobowe w zatrudnieniu

1. Zasady ogólne

Zgodnie z przepisami Kodeksu pracy (art. 221) pracodawca uprawniony jest do przetwarzania szeregu danych osobowych pracowników. Co ważne, pracodawca posiada także uprawnienie do żądania ujawnienia tych danych przez pracownika, a także przez osobę ubiegającą się o zatrudnienie (aplikującą o pracę u pracodawcy). Podstawę prawną żądania tych danych stanowi ww. przepis Kodeksu pracy.

Przedmiotowe uprawnienie obejmuje następujące dane osobowe osoby ubiegającej się o zatrudnienie:

- imię (imiona) i nazwisko,

- imiona rodziców,

- datę urodzenia,

- miejsce zamieszkania (adres do korespondencji),

- wykształcenie,

- przebieg dotychczasowego zatrudnienia.

W stosunku do pracownika pracodawca uprawniony jest natomiast do przetwarzania danych osobowych:

- wskazanych powyżej w punktach 1–6,

- innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy,

- numeru PESEL pracownika nadanego przez Rządowe Centrum Informatyczne Powszechnego Elektronicznego Systemu Ewidencji Ludności (RCI PESEL).

Pracodawca uprawniony jest także do żądania od ww. osób udokumentowania prawdziwości podanych informacji i danych osobowych.

Do danych osobowych ww. osób stosuje się zasady przetwarzania wynikające z RODO. Oznacza to, że:

- osoby te mogą rozpocząć przetwarzanie danych osobowych po udzieleniu im upoważnienia przez Administratora danych,
- dane osobowe ww. osób mogą być powierzone do przetwarzania innym podmiotom (np. biuro rachunkowe, kancelaria prawna) na mocy umowy powierzenia danych,
- osoby upoważnione do przetwarzania danych są zobowiązane do zachowania ich w poufności (również po ustaniu zatrudnienia),
- w pozostałym zakresie prawa i obowiązki związane z przetwarzaniem tych danych są analogiczne jak dla innych osób, których dane przetwarza Administrator.

2. **Dane szczególnych kategorii oraz inne wymogi**

Co do zasady, pracodawca nie żąda od kandydata do pracy ani od pracownika podania tzw. szczególnych kategorii danych osobowych (danych wrażliwych, o których mowa w art. 9 RODO, np. dotyczących zdrowia, przynależności religijnej czy orientacji seksualnej), ani danych osobowych dotyczących wyroków skazujących i naruszeń prawa (art. 10 RODO). Wyjątkiem mogą być sytuacje, gdy obowiązek lub uprawnienie do żądania takich danych wynika wprost z przepisów prawa (np. żądanie informacji o niekaralności na określonych stanowiskach, badań lekarskich itp.).

Przetwarzanie danych osobowych kandydatów i pracowników odbywa się przy zastosowaniu wszystkich opisanych w niniejszej Polityce zasad, w tym zabezpieczeń organizacyjnych i technicznych. Dostęp do danych pracowniczych mają wyłącznie osoby upoważnione (działy kadr, bezpośrednia kadra zarządzająca itp.), a ich udostępnianie na zewnątrz może nastąpić jedynie na podstawie przepisów prawa (np. do ZUS, US) lub umów powierzenia (np. biuru płacowemu).

Dane osobowe pracowników przetwarzane są przez okres wynikający z przepisów prawa (m.in. okres przechowywania akt osobowych, dokumentacji płacowej – zgodnie z ustawą o narodowym zasobie archiwalnym i archiwach oraz przepisami podatkowymi). Po upływie wymaganego okresu są usuwane lub archiwizowane zgodnie z przepisami.

XVI. Postanowienia końcowe

1. Wątpliwości dotyczące interpretacji lub zastosowania przepisów niniejszej Procedury wyjaśnia Administrator danych.

2. Tekst Procedury powinien zostać udostępniony użytkownikom w taki sposób, aby mogli się z nim zapoznać i wdrożyć w życie jej postanowienia. Jednocześnie tekst Procedury stanowi tajemnicę przedsiębiorstwa Administratora danych w rozumieniu ustawy z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji. (Pracownicy i inne osoby upoważnione do przetwarzania danych osobowych w Fundacji powinni podpisać zobowiązanie do zachowania niniejszej Polityki w poufności.)

3. Zmiana Procedury wymaga zatwierdzenia przez Administratora danych.

4. **Procedura została przyjęta uchwałą zarządu Administratora danych z dnia 2 stycznia 2024 roku oraz wchodzi w życie z dniem 2 stycznia 2024 roku.**

5. Procedura podlega regularnemu przeglądowi i aktualizacji. Administrator danych dokonuje przeglądu niniejszej Polityki co najmniej raz do roku oraz każdorazowo w razie istotnych zmian przepisów prawnych lub okoliczności wpływających na ochronę danych osobowych, tak aby zachować jej aktualność i zgodność z obowiązującymi wymogami. Wszelkie zmiany Procedury są dokumentowane w tabeli historii zmian na początku dokumentu i wchodzą w życie po ich zatwierdzeniu przez Administratora.

W zakresie nieuregulowanym w niniejszej Procedurze zastosowanie mają powszechnie obowiązujące przepisy prawa z zakresu ochrony danych osobowych oraz bezpieczeństwa informacji. Fundacja monitoruje zmiany w przepisach, w tym nowe regulacje dotyczące cyberbezpieczeństwa i w razie objęcia jej zakresem takich regulacji podejmuje działania zapewniające zgodność z tymi przepisami.