Політика захисту персональних даних у Представництві Фонду міжнародної солідарності в Україні

Дата останнього оновлення: 20220811

Мета і сфера дії документу

Мета розробки документу

Ця *Політика захисту персональних даних* Фонду міжнародної солідарності (далі: *Політика*) описує правила опрацювання персональних даних та їх захисту у Фонді міжнародної солідарності. Метою документа є визначення відповідних стандартів захисту персональних даних та забезпечення послідовності їх впровадження, а також забезпечення відповідності діяльності Фонду міжнародної солідарності чинному законодавству, зокрема Регламенту (ЄС) 2016/679 Європейського парламенту та Ради від 27 квітня 2016 р. про захист фізичних осіб щодо опрацювання персональних даних та про вільний рух таких даних, а також про скасування Директиви 95/46 /ЕС (Загальний регламент захисту даних (GDPR)).

Під забезпеченням захисту персональних даних розуміють гарантування конфіденційності, цілісності та доступності персональних даних, а також підзвітності дій, які здійснюються щодо персональних даних. Персональні дані Фонду міжнародної солідарності захищаються від внутрішніх і зовнішніх загроз, зокрема від доступу невповноважених осіб. *Політика* створена для виконання вимог та впровадження рішень, передбачених GDPR, відповідно до ст. 24 п. 2 GDPR.

Зв'язок із чинними нормативними актами та ієрархічне закріплення в документації Фонду

Політика є документом нижчого рівня відносно GDPR та інших правових положень, чинних у Європейському Союзі та країнах, де розташовані організаційні підрозділи Фонду. У разі суперечності між положеннями цього документа та положеннями, чинними в країні місцезнаходження даного організаційного підрозділу, цей підрозділ коригує Політику відповідно до вимог законодавства шляхом розробки Положення про опрацювання персональних даних, враховуючи ці розбіжності. У разі, якщо чинні правові норми представляють відмінний рівень захисту прав і свобод суб'єктів даних, застосовуються положення, які передбачають більший захист.

У Фонді міжнародної солідарності стандарти захисту інформації описані в документі «*Політика захисту даних*». Даний документ виконує роль деталізації положень «*Політики захисту даних*» (так званий lex specialis), стосовно предмета її регулювання, тобто персональних даних, їх опрацювання та захисту. У питаннях, не охоплених положеннями цього документа, застосовуються положення *Політики захисту даних*. У разі суперечності між *Політикою захисту даних* та положеннями цього документа щодо предмета цього документа застосовуються положення цього документу.

Цей документ зберігається, оновлюється та оприлюднюється відповідно до внутрішніх нормативних актів Фонду, зокрема інструкції з *Документи в ФМС*.

Документ адресований усім працівникам та співробітникам Фонду міжнародної солідарності. Описані правила поширюються на всіх співробітників, керівництво та суб'єктів, які співпрацюють з Фондом міжнародної солідарності на основі цивільно-правових договорів, котрі мають контакт із захищеними персональними даними.

Цей документ є головним документом щодо опрацювання та захисту персональних даних у Фонді міжнародної солідарності. Будь-які інші документи, котрі діють у Фонді міжнародної солідарності, у тому числі, положення про захист персональних даних в організаційних підрозділах Фонду міжнародної солідарності, повинні відповідати положенням цього документа та підпорядковуватися їм. У неврегульованих питаннях та у разі суперечності між положеннями даної *Політики* та положеннями додаткових документів і документів нижчого відносно цієї Політики рівня застосовуються положення цієї *Політики*. Положення документів нижчого рівня та додаткових до цієї *Політики* документів, які не відповідають положенням *Політики*, приводяться у відповідність до положень *Політики*.

Зміст

Визначення

Адміністратор персональних даних (АПД) – організаційний підрозділ, який приймає рішення про цілі та засоби опрацювання персональних даних.

Фонд – Фонд міжнародної солідарності.

Персональні дані – будь-яка інформація, котра стосується визначеної або ідентифікованої фізичної особи, яка дозволяє прямо чи опосередковано ідентифікувати фізичну особу. Ідентифікація повинна бути можливою без надмірної витрати часу чи надмірних зусиль.

Конфіденційні персональні дані – персональні дані певних категорій, тобто дані, які розкривають расове чи етнічне походження, політичні погляди, релігійні чи світоглядні переконання, членство в профспілці. Конфіденційні персональні дані також включають генетичні дані, біометричні дані для однозначної ідентифікації фізичної особи, дані щодо здоров'я, сексуальності чи сексуальної орієнтації або інші дані, розголошення яких може становити високий ризик для прав і свобод суб'єктів даних.

Інспектор із захисту персональних даних (ІЗПД) – працівник, відповідальний за захист персональних даних на рівні Фонду.

Керівник організаційного підрозділу – член Правління Фонду або особа, яка керує Головним офісом або відділенням Фонду від імені Правління Фонду.

Організаційний підрозділ – окремі організаційні підрозділи Фонду: Головний офіс у Польщі, зареєстровані філії та закордонні представництва Фонду.

Порушення захисту персональних даних – порушення безпеки, яке призводить до випадкового або незаконного знищення, втрати, модифікації, несанкціонованого розкриття або несанкціонованого доступу до персональних даних, які передаються, зберігаються або іншим чином опрацьовуються у Фонді.

Особа, вповноважена на опрацювання персональних даних – особа, якій надано право доступу до персональних даних.

Третя країна – країна за межами Європейської економічної зони.

Суб'єкт персональних даних – фізична особа, якої стосуються дані.

Оператор персональних даних – суб'єкт, якому адміністратор персональних даних доручає опрацювання персональних даних від свого імені.

Правові норми щодо персональних даних – норми GDPR, норми європейського права прямої дії та правові норми щодо персональних даних, прийняті в Польщі.

Опрацювання даних – операція або низка операцій з персональними даними або картотеками персональних даних з використанням автоматизованих засобів або без них, такі як збирання, реєстрація, організація, структурування, зберігання, адаптація чи зміна, завантаження, ознайомлення, використання, розкриття через передавання, розповсюдження чи надання іншим чином, упорядкування чи комбінування, обмеження, стирання чи знищення;

GDPR – Регламент (ЄС) 2016/679 Європейського парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування

Директиви 95/46 / ЕС (Загальний регламент про захист даних) (Вісник законів ЄС L 119, стор. 1, зі зміною, оприлюдненою в Віснику законів ЄС L 127 від 23.05.2018 р. та Віснику законів L 74 від 03.04.2021 р.);

Картотека персональних даних – будь-який структурований вміщений в IT-системі набір даних, який містить інформацію, котра дозволяє ідентифікувати дану особу, доступний користувачам відповідно до певних критеріїв.

У питаннях термінології, не врегульованих в цьому документі, застосовуються визначення, прийняті в *Політиці захисту даних* та GDPR.

Загальні положення

Правила перегляду, оновлення, зберігання Політики та розкриття її змісту

1. *Політика* переглядається періодично, не рідше одного разу на 5 років.
2. *Політика* оновлюється у разі внесення змін до положень щодо опрацювання персональних даних у сфері, яка впливає на положення цієї політики. Інспектор із захисту персональних даних відповідає за моніторинг змін у правових нормах.
3. Документ зберігається та оновлюється відповідно до внутрішніх нормативних актів Фонду, зокрема тих, які містяться в інструкції *Документи в ФМС*.
4. Інформація, яка міститься в цьому документі, є конфіденційною і не призначена для поширення за межами Фонду.
5. Зміст цього документу розкривається особам, яким необхідно надати повноваження з опрацювання персональних даних в Фонді міжнародної солідарності, з метою ознайомлення їх із чинними правилами та прийняття цих правил перед наданням дозволу на опрацювання персональних даних. Зміст документа також розкривається особам, уповноваженим на опрацювання персональних даних в Фонді міжнародної солідарності.
6. Зміст цього документа може бути розкритий третім особам та органу, який здійснює нагляд за опрацюванням персональних даних у Польщі, за згодою Правління Фонду міжнародної солідарності. Перед тим, як розкрити зміст цього документа зовнішньому суб'єкту, Правління Фонду міжнародної солідарності накладає на документ застереження «з обмеженим доступом».

1. Опрацювання персональних даних в Фонді

1.1. Фонд міжнародної солідарності опрацьовує персональні дані лише у зв’язку з місією та цілями, визначеними його статутом, тобто в рамках участі у співробітництві у сфері розвитку інших країн. Діяльність, яку здійснює Фонд, зосереджена на таких напрямках:

- підтримка демократії, принципів належного урядування та громадянського суспільства;
- підтримка місцевого розвитку;
- діяльність у сфері прав людини та допомоги репресованим;
- підтримка незалежних ЗМІ;
- спостереження за виборами та навчання спостерігачів;
- підтримка самоврядування та внутрішніх реформ на центральному та місцевому рівнях;
- гуманітарна допомога.

1.2. Фонд є неприбутковою організацією.

1.3. Фонд не опрацьовує дані для інших цілей, зокрема для комерційних або маркетингових цілей

2. Групи процесів з опрацювання персональних даних Фондом

2.1. Фонд в рамках реалізації процесів, зазначених у п. 1.1. вище, опрацьовує персональні дані, необхідні для реалізації статутних цілей та функціонування самої організації.

2.2 У рамках здійснення заходів, зазначених у п. 1.1. вище, Фонд визначив такі групи процесів, пов'язаних з опрацюванням персональних даних:

a) опрацювання персональних даних осіб, пов'язаних з проектами, які реалізуються Фондом (власна діяльність);
b) опрацювання персональних даних осіб, пов'язаних з проектами, які підтримуються Фондом (проекти, які реалізуються за грантовими конкурсами, партнерські проекти, прямі гранти та інституційні гранти);
c) опрацювання даних осіб, які звертаються до Фонду за підтримкою в різних формах;
d) опрацювання даних осіб, які беруть участь у заходах, організованих Фондом;
e) опрацювання персональних даних для цілей внутрішніх процесів фонду, необхідних для забезпечення його належного функціонування;
f) персональних даних, пов'язаних з управлінням людськими ресурсами;
g) опрацювання персональних даних, пов'язаних з процесом здійснення закупівель Фондом;
h) інші процеси, не зазначені вище, пов'язані зі статутною діяльністю Фонду.

2.3. У сфері, в якій організаційні підрозділи Фонду залишаються індивідуальними адміністраторами персональних даних, вони можуть здійснювати процеси, які не належать до груп процесів, зазначених у п. 2.2., на підставі Положення про опрацювання персональних даних в організаційних підрозділах. Включення та опис до Положення про опрацювання персональних даних в організаційних підрозділах процесів, які не належать до груп процесів, описаних у п. 2.2. вище, не є порушенням цієї Політики та відбувається на виключний ризик організаційного підрозділу як окремого адміністратора персональних даних.

3. Категорії персональних даних, які опрацьовуються Фондом

3.1 Фонд опрацьовує звичайні персональні дані, такі як: ім'я, прізвище, дата народження, адреса електронної пошти, дані про громадянство, дані паспорта (номер, термін дії, орган, що видав) та дані з інших документів, які посвідчують особу, приналежність до установи та посаду, освіту, номер телефону, адресні дані, реквізити банківського рахунку та інші відомості, необхідні для вчинення дій, зазначених в п. 1.1. цього документа та для забезпечення функціонування Фонду.

3.2. Фонд опрацьовує конфіденційні персональні дані, тобто персональні дані особливих категорій, які розкривають політичні погляди, світогляд та інші дані, розголошення яких може становити високу загрозу правам і свободам суб'єктів даних.

3.3. Фонд проводить інвентаризацію даних і, таким чином, ідентифікує ресурси даних, способи використання даних і залежності між картотеками. В інвентаризації виділяє випадки опрацювання даних особливої категорії.

3.4. Вищезазначена інвентаризація здійснюється Фондом у формі ведення реєстру заходів з опрацювання персональних даних.

3.5 Реєстр заходів з опрацювання персональних даних містить інформацію про адміністратора даних, вид процесу, у рамках якого опрацьовуються дані, категорію осіб, дані яких опрацьовуються, категорію персональних даних, які опрацьовуються, мету опрацювання, категорію одержувачів, яким персональні дані були або будуть розкриті, включаючи одержувачів у третіх країнах або в міжнародних організаціях, інформацію, яким країнам і міжнародним організаціям передаються дані, інформацію про правову основу опрацювання даних, джерело даних, інформацію про заплановану дату видалення даних та загальний опис технічних та організаційних заходів безпеки.

3.7 При здійсненні нових заходів з опрацювання персональних даних Фонд робить опис процесу здійснення нових заходів з опрацювання, аналізує пов'язані з цим ризики, визначає правові підстави для опрацювання, категорії зібраних даних та одержувачів даних, а також належним чином заповнює реєстр заходів з опрацювання персональних даних.

3.8. Фонд веде реєстр категорій заходів з опрацювання.

3.9. Реєстр заходів з опрацювання включає дані адміністратора, який доручає персональні дані для опрацювання, встановлений термін опрацювання, відомості про передачу персональних даних третій країні чи міжнародній організації, загальний опис технічних та організаційних заходів безпеки.

3.10. У сфері, у якій організаційні підрозділи Фонду залишаються індивідуальними адміністраторами персональних даних, вони можуть опрацьовувати персональні дані, відмінні від зазначених у п. 3.1 і 3.2. вище, на підставі Положення про опрацювання персональних даних в організаційних підрозділах. Організаційні підрозділи ведуть облік заходів з опрацювання персональних даних для реалізації принципів, зазначених у п. 3.3. вище, відповідно до принципів, зазначених у п. 3.5. вище. Включення та опис у Положенні про опрацювання персональних даних в організаційних підрозділах опрацювання персональних даних, відмінних від зазначених у п. 3.1. та 3.2. вище, не є порушенням цієї Політики та відбувається на виключний ризик організаційного підрозділу як окремого адміністратора персональних даних.

4. Принципи опрацювання персональних даних

4.1 Опрацювання персональних даних відбувається у Фонді:

a) на законній підставі та відповідно до законодавства (законність);
b) у чесний і прозорий для суб'єкта даних спосіб (справедливість);
c) для конкретних, чітко визначених цілей (доцільність);
d) лише в такому обсязі та з наданням лише такого доступу працівників до персональних даних, який необхідний, а не з запасом (мінімізація);
e) з забезпеченням правильності даних (коректність);
f) не довше, ніж потрібно (обмеженість у часі);

g) із забезпеченням захисту персональних даних від втрати, пошкодження чи знищення, несанкціонованої зміни, розголошення неуповноваженим особам (цілісність та конфіденційність);
h) із врахуванням принципів захисту персональних даних на етапі проектування процесів, тобто до збору даних;
i) у спосіб, що дозволяє особам, чиї дані Фонд опрацьовує, реалізувати свої права відповідно до чинного законодавства і в обсязі, у якому це можливо;
j) у спосіб, що забезпечує підзвітність Фонду.

5. Правові підстави опрацювання персональних даних

5.1. Персональні дані Фонд зазвичай опрацьовує як адміністратора даних, якщо опрацювання:
a) стосується діяльності/проектів, які ведуться Фондом, коли Фонд приймає рішення щодо мети та обсягу зібраних даних (власна діяльність);
b) стосується внутрішніх процесів, необхідних для функціонування Фонду;
c) стосується процесу здійснення закупівель Фондом;
d) стосується ситуації, коли дані були спочатку зібрані іншими адміністратора даних (одержувачами грантів та партнерами), які визначили мету та обсяг зібраних даних, а потім ці дані були надані Фонду для цілей моніторингу та звітності - це стосується конкурсних та партнерських проектів. У такій ситуації грантоотримувач/партнер несе відповідальність за збір та опрацювання даних, відповідно до GDPR, тобто інформування суб'єктів даних про їхні права, про повідомлення даних Фонду та за отримання відповідних видів згоди. На вимогу Фонду грантоотримувач/партнер зобов'язаний надати декларацію про виконання обов'язків у вищевказаній сфері.

5.2. Правовими підставами для опрацювання звичайних персональних даних Фондом у разі власних проектів/заходів, які здійснює Фонд, є таке:
a) згода, надана суб'єктом персональних даних;
b) якщо це необхідно для виконання договору, стороною якого є суб'єкт даних, або для вжиття заходів на вимогу суб'єкта даних перед укладенням договору;
c) якщо це необхідно через юридичні зобов'язання, покладені на Фонд;
d) якщо опрацювання необхідне для цілей законних інтересів, які реалізує Фонд, за винятком випадків, коли переважний характер відносно цих інтересів мають інтереси або базові права і свободи суб'єкта даних.

5.3. Підставою для опрацювання звичайних персональних даних Фондом у випадку проектів, які реалізуються в рамках грантового конкурсу та партнерських проектів, прямих грантів та інституційних грантів, є згода або законний інтерес адміністратора (тобто стаття 6 абзац 1 літера a) GDPR або ст. 6 абзац 1 літ. f) GDPR). Згода може бути дана у формі відповідної заяви або у формі дії, яка це явною підтверджує. Такою дією може бути, наприклад, участь у проекті.

5.4. Фонд опрацьовує конфіденційні дані як адміністратор даних, якщо опрацювання:

a) стосується даних, пов'язаних зі здоров'ям у сфері трудових відносин працівників та співпраці з іншими особами;
b) стосується даних осіб, які звертаються до Фонду щодо надання підтримки в різних формах;
c) стосується даних членів неприбуткової організації відповідно до ст. 9 абзац 2 літ. d) GDPR
d) застосовується до ситуації, коли дані спочатку були зібрані іншими адміністраторами даних (одержувачами грантів та партнерами), які визначили мету та обсяг збору даних, а потім дані надаються Фонду для цілей моніторингу та звітності - це стосується конкурсних та партнерських проектів. У такій ситуації грантоотримувач/партнер несе відповідальність за збір даних відповідно до GDPR, тобто інформування суб'єктів даних про їхні права, про передачу даних до Фонду та за отримання явної згоди на опрацювання даних, наданої суб'єктом даних для однієї або кількох конкретних цілей у ситуації, коли згода є необхідною.

5.5. Підстави опрацювання конфіденційних персональних даних Фондом:

a) опрацювання необхідне для виконання завдань адміністратора, як стосуються трудових відносин з працівниками та іншими особами, а обсяг опрацювання даних визначено в Законі;
b) на основі явної згоди на опрацювання, наданої суб'єктом даних для однієї або кількох конкретних цілей;

5.6. Підставою для опрацювання Фондом конфіденційних персональних даних у випадку проектів, які реалізуються в рамках грантового конкурсу та партнерських проектів, є чітка згода на опрацювання даних, наданих суб'єктом, для однієї або кількох конкретних цілей.

5.7. У тій мірі, в якій організаційні підрозділи Фонду залишаються індивідуальними адміністраторами персональних даних, вони можуть опрацьовувати персональні дані в іншому характері та обсязі, ніж зазначені в п. 6.1. та 6.4. вище, на підставах, відмінних від зазначених у п 6.2. та 6.5. вище, на підставі Положення щодо опрацювання персональних даних в організаційних підрозділах. Включення та опис до Положень щодо опрацювання персональних даних в організаційних підрозділах, зазначеного в попередньому реченні, не є порушенням цієї Політики та здійснюється на власний ризик організаційного підрозділу як окремого адміністратора персональних даних.

6. Права, якими користуються суб'єкти даних

Фонд надає суб'єктам персональних даних, які він опрацьовує, такі права:

a) *на вимогу суб'єкта даних* – право на відкликання згоди на опрацювання даних;
b) *на вимогу суб'єкта даних* - право на доступ до даних, тобто право на отримання інформації: чи опрацьовує Фонд дані даної особи; яка мета та обсяг опрацювання даних; скільки часу Фонд буде опрацьовувати дані

щодо нього; що є джерелом даних, інформація про одержувачів або категорії одержувачів, яким Фонд надав або має намір надати дані, інформацію про автоматизоване прийняття рішень, у тому числі профілювання, а також про істотні принципи прийняття рішень та про значення та очікувані наслідки такого опрацювання, інформація про право вимагати виправлення, видалення, обмеження опрацювання даних, право подати заперечення та право подати скаргу до контролюючого органу, а також право на отримання вмісту цих даних у загальнозрозумілій формі, з урахуванням обмежень, передбачених ст. 15 GDPR;

c) право бути інформованим - право отримати інформацію, в т.ч. про те, ким і як опрацьовуються дані та право на отримання копії даних;
d) *на вимогу суб'єкта даних* право виправляти дані, тобто право вимагати доповнення, оновлення та виправлення інформації про суб'єкта даних, які опрацьовуються Фондом;
e) *на вимогу суб'єкта даних* право обмежити опрацювання;
f) *на вимогу суб'єкта даних* право на видалення даних у ситуації, коли дані більше не потрібні для досягнення мети; закінчився термін опрацювання даних; дані були зібрані без правових підстав; суб'єкт даних відкликав згоду, на якій базується опрацювання, і немає іншої правової підстави для опрацювання даних; суб'єкт даних заперечує проти опрацювання, і не існує вищих законних підстав для опрацювання;
g) *на вимогу суб'єкта даних* право заперечувати проти опрацювання даних - за винятком випадків, коли опрацювання необхідне для виконання завдання, яке виконується заради публічних інтересів або у зв'язку з законними інтересами адміністратора, які переважають інтереси, права та свободи суб'єкта даних, або якщо опрацювання необхідне для встановлення, розслідування чи захисту від претензій. Фонд не опрацьовує дані для цілей прямого маркетингу, тому право на заперечення проти прямого маркетингу не поширюється на опрацьовувані дані;
h) *на вимогу суб'єкта даних* право на передачу даних: якщо підставою для опрацювання є згода або договір і опрацювання здійснюється в автоматизованому порядку, за запитом Фонд видає дані в структурованому, загальновживаному форматі, який можна розшифрувати машинним способом, або передає його іншому об'єкту, якщо це технічно можливо;
i) право не бути об'єктом автоматизованого прийняття рішень, у тому числі профілювання;
j) право на конфіденційність електронного зв'язку - електронне обладнання та IT-системи, які використовуються Фондом, забезпечують відповідний стандарт безпеки опрацювання даних та гарантують конфіденційність комунікацій. Фонд застосовує спеціальні запобіжні заходи під час спілкування та отримання даних від одержувачів грантів/партнерів із країн, де існують особливі політичні умови, які становлять загрозу правам і свободам суб'єктів даних.

6.2 Правами суб'єктів даних, які не реалізуються безпосередньо Фондом є:

k) право подати скаргу в наглядовий орган;
l) право звернутися до суду загальної юрисдикції;

7. Забезпечення прав суб'єктами персональних даних

7.1. Фонд гарантує суб'єктам персональних даних, які ним опрацьовуються, дотримання прав, описаних у пункті a) -i) та l) розділу 7 вище.

7.2. Інспектор із захисту персональних даних повідомляє до загального відома адресу електронної пошти, на яку потрібно надсилатися запити щодо персональних даних та всю кореспонденцію, пов'язану з реалізацією прав суб'єктів персональних даних.

7.3. Дотримання прав суб'єкта даних, зазначених в п. j) -k) розділу 7 вище, забезпечується відповідно до положень чинного законодавства із залученням наглядового органу або суду, до юрисдикції якого входить розгляд справ щодо прав та претензій суб'єктів даних.

7.4. Запити щодо прав суб'єктів персональних даних розглядаються без невиправданих затримок, у будь-якому випадку впродовж одного місяця з моменту отримання запиту. У разі необхідності цей термін може бути продовжений ще на два місяці через складність запиту або кількість запитів. Впродовж одного місяця з моменту отримання запиту Фонд повідомляє суб'єкта даних про таке продовження із зазначенням причин затримки. Якщо суб'єкт даних подав свій запит в електронному вигляді, інформація також у міру можливості передається в електронному вигляді, якщо суб'єкт даних не вимагає іншої форми.

7.5. Рішення з питань розгляду звернень щодо реалізації прав суб'єктів персональних даних приймається Правлінням Фонду після консультації з Інспектором із захисту персональних даних.

8. Технічні та організаційні засоби, які застосовуються Фондом, з метою забезпечення безпеки даних, які формують мінімальні стандарти безпеки

8.1. Фонд встановлює мінімальні стандарти безпеки опрацювання персональних даних.

8.2. Заходи безпеки, які забезпечують мінімальні стандарти безпеки, розроблені Фондом, включають:

a) методи, які застосовуються для захисту приміщень, в яких опрацьовуються персональні дані (фізична і технічна безпека);
b) розробку та оновлення Політики захисту даних, Політики захисту персональних даних та Інструкції з управління інформаційними системами - документів, які використовуються для управління процесом опрацювання даних в організації, у тому числі персональних даних (організаційно-правові гарантії);
c) призначення та нагляд інспектора із захисту персональних даних (організаційно-правова безпека);
d) застосування клаузули про дотримання конфіденційності персональних даних у трудових та цивільно-правових договорах (правові захисні заходи);
e) навчання у сфері захисту персональних даних (організаційні захисні заходи);

f) шифрування, псевдонімізація та анонімізація персональних даних (технічні та організаційні захисні заходи);
g) відповідні заходи безпеки даних в IT-системах (технічні та технологічні захисні заходи).

8.3. Для забезпечення безпеки опрацювання персональних даних організаційні підрозділи Фонду застосовують фізичні і технічні, технологічні, а також організаційно-правові заходи. Детальні рішення щодо застосування організаційних, технічних і технологічних засобів захисту даних описані в *Політиці захисту даних*.

9. Аналіз ризику й оцінка наслідків для захисту даних

9.1. Фонд аналізує ризики порушення прав і свобод фізичних осіб. Цей аналіз полягає у виявленні потенційних та реальних факторів, які негативно впливають на безпеку персональних даних, а також на безпеку та стабільність опрацювання персональних даних, враховуючи характер, обсяг, контекст та цілі опрацювання, ризик порушення прав чи свобод фізичних осіб. Детальний опис методології управління ризиками міститься в окремому документі *«Оцінка ризику опрацювання персональних даних»*.

9.2. Фонд здійснює відповідні технічні та організаційні заходи, необхідні для мінімізації рівня виявленого на основі аналізу ризику.

9.3. Якщо:

a) процес або процеси опрацювання персональних даних включають в себе:
   - опрацювання конфіденційних даних у великих масштабах;
   - проведення систематичної, комплексної оцінки персональних факторів фізичних осіб, яка базується на автоматизованому опрацюванні, у тому числі на профілюванні;
   - систематичний моніторинг у великих масштабах місць загального користування.

b) результат аналізу ризиків для процесу свідчить про наявність високого ризику порушення прав і свобод осіб, персональні дані яких підлягають опрацюванню;

c) процес або процеси, включені до переліку, наведеного в додатку до Повідомлення Голови Управління із захисту персональних даних щодо переліку видів операцій з опрацювання персональних даних, які потребують оцінки наслідків опрацювання для їх захисту;

Фонд проводить оцінку наслідків у сфері захисту даних. Детальний опис методології управління ризиками можна знайти в окремому документі «*Оцінка ризику опрацювання персональних даних*».

10. Адміністратор персональних даних (АПД)

10.1. Правління Фонду є підрозділом, який на рівні всього Фонду відповідає за безпеку даних та відповідність стандартам, передбаченим цією політикою. Правління Фонду виконує функції адміністратора персональних даних для Головного офісу Фонду

10.2. Адміністратор персональних даних призначає працівника, який виконує обов'язки Інспектора із захисту персональних даних у Головному офісі Фонду.

10.3. Інші організаційні підрозділи діють як окремі адміністратори персональних даних для даних, які вони опрацьовують. Керівники інших адміністративних підрозділів можуть призначати працівників для виконання обов'язків спеціалістів із захисту персональних даних. Якщо такий працівник не призначений, відповідальність за захист персональних даних несе керівник даного підрозділу.

11. Інспектор із захисту персональних даних (ІЗПД)

11.1. ІЗПД повинен мати професійну кваліфікацію, зокрема професійні знання у сфері законодавства та практики захисту персональних даних.

11.2. Інспектор із захисту персональних даних:

a) Підтримує адміністратора у веденні реєстру заходів з опрацювання персональних даних та у веденні реєстру категорій заходів з опрацювання персональних даних;
b) інформує адміністратора персональних даних та працівників, які опрацьовують персональні дані, про обов'язки, покладені на них, відповідно до норм про персональні дані;
c) здійснює контроль за дотриманням положень про персональні дані, а також внутрішніх політик і процедур щодо опрацювання та захисту персональних даних;
d) за запитом надає рекомендації щодо оцінки наслідків для захисту даних та контролює їх виконання, відповідно до ст. 35 GDPR;
e) співпрацює з Головою Управління захисту персональних даних;
f) виступає в якості контактної особи для Голови Управління захисту персональних даних;
g) виступає в якості контактної особи для суб'єктів даних у всіх питаннях, пов'язаних з опрацюванням їхніх персональних даних та реалізацією їхніх прав відповідно до GDPR.

11.3. ІЗПД виконує свої завдання, належним чином враховуючи ризики, пов'язані з операціями з опрацювання, беручи до уваги характер, обсяг, контекст та цілі опрацювання.

11.4. ІЗПД підпорядковується безпосередньо вищому керівництву. Він не отримує інструкцій щодо виконання своїх завдань, не може бути покараний чи знятий з посади за їх виконання.

12. Обов'язки осіб, які опрацьовують персональні дані у Фонді

12.1. Працівники та партнери Фонду опрацьовують персональні дані на підставі повноважень на опрацювання даних, наданих особою, яка представляє адміністратора персональних даних. Детальні правила надання повноважень на опрацювання даних в ІТ-системі описані в Посібнику з управління ІТ-системою.

12.2. Працівники та співробітники Фонду, які опрацьовують персональні дані, зобов'язані:

a) пройти навчання з основних принципів законодавства про захист персональних даних;
b) зберігати в таємниці опрацьовані персональні дані та способи їх опрацювання і способи їх захисту;
c) застосовувати процедури і засоби опрацювання та захисту даних, визначені в Політиці захисту даних й у цьому документі, зокрема щодо використання IT-сервісів та програм, а також методів опрацювання даних;
d) негайно реагувати у разі інцидентів безпеки та порушення персональних даних;
e) виконувати вказівки Правління Фонду, інспектора із захисту персональних даних та Головного спеціаліста з питань безпеки у сфері захисту даних Фонду.

13. Кваліфікація інцидентів

13.1. Інцидент безпеки – це ситуація, в якій не було, але могло статися порушення захисту персональних даних, наприклад:

a) викрадення службового комп'ютера, телефону або інших електронних носіїв даних за умови, що конфіденційність або доступність персональних даних, які зберігаються в пам'яті комп'ютера/телефону/носія, не було порушено внаслідок такої події,
b) проникнення до приміщень організаційних підрозділів Фонду, де зберігаються дані, але без порушення конфіденційності, цілісності чи доступності персональних даних;
c) відсутність належного захисту даних, яке не призвело до порушення захисту персональних даних;
d) втрата паперової документації, яка містить дані;
e) розкриття інформації про технічні та організаційні заходи, пов'язані з системою безпеки Фонду.

13.2. Порушенням персональних даних є ситуація, яка призводить до порушення конфіденційності, цілісності або доступу до опрацювання даних, зокрема

a) несанкціонований доступ до даних;
b) несанкціонована зміна або знищення даних;
c) обмін даними з неавторизованим суб'єктом;
d) незаконне розголошення даних;
e) отримання даних із нелегальних джерел.

14. Порядок дій у випадку викриття інциденту безпеки або порушення захисту персональних даних

14.1. Кожен працівник або співробітник Фонду, у разі отримання інформації про інцидент безпеки або порушення безпеки персональних даних, зобов'язаний негайно, але не пізніше 24 годин, подати заяву через форму повідомлення про інцидент, доступну всім працівникам Фонду. Якщо доступ до цього каналу зв'язку втрачено, зверніться електронною поштою або через

керівника/іншого працівника: спочатку до Головного Спеціаліста з Безпеки, а потім до інспектора із захисту персональних даних або спеціаліста із захисту персональних даних, призначеного в даному організаційному підрозділі.

14.2. Якщо неможливо повідомити зазначених вище осіб, необхідно повідомити безпосереднього керівника та відповідального за безпеку Директора ФМС.

14.3. Поки відповідні особи не взяли на себе контроль над справою, необхідно якомога швидше вжити заходів для припинення небажаних наслідків виниклого порушення – якнайшвидше відключити пристрій від Інтернету та вимкнути його. Не вмикати заражений пристрій і передати його до IT-відділу даного організаційного підрозділу.

14.4. Отримавши повідомлення про можливість виникнення порушення, головний спеціаліст з питань безпеки у співпраці з інспектором із захисту персональних даних перевіряє, чи дійсно мало місце порушення захисту даних, та складає звіт за зразком, який наведений у Додатку 4 до цієї Політики, який повинен включати, зокрема:

a) зазначення осіб, причетних до події;
b) опис часу та місця події;
c) опис супутніх обставин та виду інциденту;
d) опис ужитих заходів;
e) оцінку ризику, пов'язаного з інцидентом;
f) у разі порушення/розголошення даних: попередню оцінку причин та опис запланованих заходів зі з'ясування та відновлення.

14.5. Звіт подається адміністратору персональних даних та іншим особам, визначеним ними.

14.6. Будь-яке порушення захисту персональних даних має бути предметом детального аналізу. Аналіз повинен включати: комплексну оцінку порушення/розкриття захисту персональних даних; визначення відповідальних осіб або суб'єктів; висновки щодо можливих заходів: процедурних, організаційних, кадрових та технічних, які мають запобігти подібним порушенням/розкриттю у майбутньому.

14.7. Інциденти безпеки та порушення захисту персональних даних документуються та реєструються у внутрішніх системах відповідно до шаблону, наведеного в Додатку 5 до цієї Політики. Відповідальними за цю діяльність є інспектора із захисту персональних даних та головний спеціаліст із безпеки.

14.8. Оцінка серйозності порушення здійснюється інспектором із захисту персональних даних у співпраці з головним спеціалістом з питань безпеки відповідно до внутрішньо встановленої методики та затверджується адміністратором персональних даних.

15. Надання та доручення опрацювання Персональних даних

15.1. Як правило, Фонд не передає персональні дані іншим суб’єктам. Однак у деяких ситуаціях надання персональних даних може бути необхідним або потрібним для досягнення передбачуваних цілей опрацювання.

15.2. Суб'єкти, яким Фонд може надавати персональні дані, включають, зокрема:

a) партнерів фонду;
b) донорів;
c) зовнішніх юрисконсультів;
d) банки;
e) страхові компанії,
f) аудиторів.

15.3 Фонд також може надавати персональні дані для відповіді на запити, зроблені стосовно Фонду уповноваженими державними та судовими органами (наприклад, прокуратурою, судом, поліцією, державними установами), а також на запит суб'єктів, які співфінансують його діяльність та контролюють використання ним коштів.

15.4 Фонд може доручити опрацювання персональних даних (тобто доручити опрацювання персональних даних від свого імені) третім особам (операторам).

15.5 Суб'єкти, яким Фонд може доручити опрацювання персональних даних - це, зокрема:

a) компанії, які надають IT-послуги та обслуговують сервери,
b) компанії, які надають телекомунікаційні послуги.

15.6. Фонд доручає персональні дані лише перевіреним суб'єктам, щодо яких отримано гарантії впровадження відповідних організаційно-технічних заходів щодо забезпечення безпеки, реалізації прав особи та інших обов'язків із захисту даних.

15.7. Доручення опрацювання персональних даних операторам відбувається із дотриманням вимоги про підписання договору доручення або договору, який містить положення про доручення, які відповідають вимогам GDPR (типового договору про доручення – додаток № 1 до цієї Політики) або іншого правового інструменту у розумінні ст. 28 абзац 3 GDPR.

15.8. Договори доручення реєструються в реєстрі договорів доручення, зразок якого становить додаток № 6 до цієї Політики.

16. Передача персональних даних в треті країни

16.1 Передача персональних даних до третіх країн – це передача персональних даних поза межі безпечної, відповідно до положень GDPR, Європейської економічної зони (ЄЕЗ).

16.2. Фонд передає персональні дані третім країнам або організаціям, відносно яких рішенням Європейської Комісії підтверджено відповідний рівень захисту даних.

16.3. За відсутності рішення Європейської Комісії, яке підтверджує належний рівень захисту, Фонд передає персональні дані третім країнам на основі відповідних гарантій: зобов'язальних корпоративних правил, стандартних положень про захист даних, прийнятих Європейською Комісією, стандартних положень про захист даних, прийнятих польським наглядовим органом і затверджених Комісією, затвердженого кодексу дій або затвердженого механізму сертифікації.

16.4. У разі відсутності рішення про належний рівень захисту або відсутності відповідних гарантій дані можуть передаватися за межі ЄЕЗ також тоді, коли:

- суб'єкт персональних даних був поінформований про можливі ризики, пов'язані із запропонованою передачею даних, та дав на це згоду;
- передача необхідна для укладення або виконання договору, укладеного із суб'єктом даних, або передача здійснюється в інтересах суб'єкта даних або з метою захисту істотних інтересів суб'єкта даних;
- передача необхідна для обґрунтування, розслідування або захисту від претензій.

17. Відповідальність

17.1 Випадки невиправданого невиконання зобов'язань, передбачених Політикою, можуть розглядатися як серйозне порушення трудових обов'язків (а у випадку суб'єктів, які співпрацюють з КПД на підставі цивільно-правових договорів - як неналежне виконання цивільно-правового договору або невиконання цивільно-правового договору), зокрема особою, яка, виявивши порушення безпеки ІТ-системи або обґрунтований здогад про таке порушення, не повідомила про цей факт КПД.

17.2 Щодо особи, зазначеної у п. 18.1. вище відкривається з'ясувальне провадження.

17.3 Накладення стягнення на особу, яка ухиляється від виконання зобов'язань, передбачених Політикою, не виключає кримінальної відповідальності цієї особи відповідно до чинного законодавства та можливості подати проти неї цивільний позов про відшкодування завданих збитків.

17.4. Упровадження Політики, а також заходи з коригування та підтримання вживаються у формі ознайомлення працівників та партнерів (осіб, які працюють у ФМС на умовах, відмінних від трудового договору) зі змістом Політики та періодичного проведення навчання у сфері захисту персональних даних.

18. Чинність

18.1.Політика набирає чинності з дня її прийняття за рішенням Голови Фонду.

18.2. Ця політика замінює інші документи, які діють досі у Фонді (у сфері, яка регулюється цією політикою).

Додатки

1. Зразок договору доручення опрацювання персональних даних з додатками 1-2.
2. Зразок звіту про інцидент безпеки/порушення захисту персональних даних.
3. Зразок реєстру інцидентів безпеки/порушень персональних даних.
4. Зразок реєстру договорів доручення.

Додаток № 1

Зразок договору доручення

Договір доручення опрацювання персональних даних

(далі – «Договір»)

укладений XXXX в XXXX між:

XXXX, розташованого в XXXX (дані Оператора), номер реєстрації XXXX,

якого представляє

XXXXX

далі у тексті договору – «Оператор»

та

[дані організаційного підрозділу], якого представляє [дані представника]

далі у тексті договору – «Адміністратор даних» або

Визначення:

«Документ» – будь-який носій, традиційний або електронний, на якому зберігаються персональні дані.

«Норми про захист персональних даних» – чинні норми законодавства про захист персональних даних, які мають застосування до адміністратора даних та оператора даних, зокрема Регламент Європейського Парламенту та Ради (ЄС) 2016/679 від 2 квітня 2016 р.

«Регламент» – Регламент Європейського Парламенту та Ради (ЄС) 2016/679 від 2 квітня 2016 року.

«Основний договір» – XXXXXX

«Договір доручення» – даний договір про опрацювання персональних даних.

§ 1

Доручення опрацювання персональних даних

1. Адміністратор даних доручає Оператору, відповідно до ст. 28 Загального регламенту про захист даних від 27 квітня 2016 року (далі – «Регламент») персональні дані, які опрацьовуються на умовах та з метою, визначеними даним Договором та Основним договором.

2. Оператор опрацьовує довірені дані виключно за дорученням та інструкціями адміністратора. Оператор зобов'язується опрацьовувати довірені йому персональні дані у відповідності до даного Договору, Основного договору та положень чинного законодавства, які захищають права суб'єктів даних, зокрема Регламенту.

3. Оператор заявляє, що застосовує заходи безпеки, які відповідають вимогам Регламенту.

4. Характер опрацювання має циклічний / одноразовий / постійний характер * (* позначте відповідне).

§2

Обсяг і мета опрацювання даних

1. Оператор буде опрацьовувати довірені йому за договором звичайні дані / спеціальні дані (* вкажіть тип даних: звичайні дані або конфіденційні дані). Сфера опрацювання даних включає в себе:

Категорії осіб, яких стосуються дані	Категорії персональних даних

2. Персональні дані, довірені адміністратором, будуть опрацьовуватися оператором лише з метою XXXXX (*необхідно вказати мету опрацювання даних оператором, наприклад виконання договору ..... № ... ... у сфері готельних послуг).

§3

Обов'язки суб'єкта, який здійснює опрацювання

1. Оператор зобов'язується опрацьовувати довірені персональні дані, захищати їх шляхом застосування відповідних технічних та організаційних заходів, які забезпечують належний рівень безпеки, котрий відповідає ризику, пов'язаному з опрацюванням персональних даних, зазначених у ст. 32 Регламенту.

2. Оператор зобов'язується проявляти належну старанність при опрацюванні довірених персональних даних.

3. Оператор зобов'язується надати повноваження на опрацювання персональних даних усім особам, які будуть опрацьовувати довірені дані з метою виконання цього договору.

4. Оператор зобов'язується забезпечити конфіденційність (про яку йдеться в статті 28 п. 3 пп. b Регламенту) даних, які опрацьовуються особами, які уповноважені опрацьовувати персональні дані, з метою виконання даного договору, як під час їхніх трудових стосунків із Суб'єктом опрацювання, так і після їх припинення.

5. Після завершення надання послуг, пов'язаних з опрацюванням, оператор видаляє / повертає адміністратору даних усі персональні дані (потрібно вибрати, чи має оператор видалити чи повернути дані) та видаляє будь-які наявні їх копії, якщо тільки законодавство Європейського Союзу або законодавство країни-члена не вимагає зберігання персональних даних. Зразок Протоколу повернення/видалення персональних даних додається як Додаток 1 до цього Договору доручення.

6. У міру можливості, оператор допомагає адміністратору в необхідному обсязі виконати обов'язок із надання відповіді на запити суб'єкта даних та виконання обов'язків, визначених ст. 32-36 Регламенту.

7. Оператор, виявивши порушення захисту персональних даних, повідомляє про це адміністратора без зайвого зволікання, протягом 24 годин.

8. Повідомлення, зазначене в п. 7, повинно містити, зокрема: інформацію про дату і час порушення, тип і місце порушення, опис і перебіг порушення, причини порушення, його доконані та потенційні наслідки, а також про вжиті заходи з виправлення. Форма заяви додається як Додаток 2 до даного Договору доручення.

§4

Право перевірки

1. Адміністратор даних, відповідно до ст. 28 п. 3 пп. h) Регламенту, має право перевіряти, чи відповідають заходи, яких вживає оператор під час опрацювання та захисту довірених персональних даних, положенням договору.

3. Оператор зобов'язується усунути виявлені під час перевірки недоліки в термін, зазначений адміністратором даних, не довше, ніж за 3 дні.

4. Оператор надає адміністратору даних всю інформацію, необхідну для засвідчення виконання обов'язків, передбачених у ст. 28 Регламенту.

§5

Передоручення опрацювання даних

1. Оператор може довірити персональні дані, передбачені цим договором, для подальшого опрацювання субпідрядникам (субоператорам) лише з метою виконання договору після отримання попередньої письмової згоди адміністратора даних.

2. Передача довірених даних до третьої країни може здійснюватися лише за письмовим розпорядженням адміністратора даних, якщо такий обов'язок не покладено на оператора законодавством ЄС або законодавством держави-члена, якому він підпорядковується. У цьому випадку перед початком опрацювання оператор інформує адміністратора даних про цей передбачений правом обов'язок, якщо законодавство не забороняє надавати таку інформацію, з огляду на важливі суспільні інтереси.

3. Субоператор повинен забезпечувати ті самі гарантії та обов'язки, які були накладені на оператора в даному Договорі.

4. Оператор несе повну відповідальність перед адміністратором даних за невиконання субпідрядником обов'язків із захисту даних.

§ 6

Відповідальність суб'єкта, який здійснює опрацювання

1. Оператор несе відповідальність за надання або використання персональних даних, яке суперечать змісту договору, і зокрема за розголошення персональних даних, довірених для опрацювання неуповноваженим особам.

2. Оператор зобов'язується негайно інформувати адміністратора даних про будь-які провадження, зокрема адміністративні чи судові, щодо опрацювання оператором персональних даних, зазначених в договорі, будь-які адміністративні рішення або судову постанову щодо опрацювання таких даних, адресовані оператору, а також будь-які заплановані, якщо про це відомо, або триваючі перевірки та інспекції щодо опрацювання цих персональних даних оператором, зокрема, такі, що проводяться інспекторами, уповноваженими Управлінням із захисту персональних даних. Цей пункт застосовується лише щодо довірених адміністратором персональних даних.

§7

Термін дії договору

7.1 Даний Договір доручення укладається на термін дії Основного договору, укладеного між Сторонами.

7.2 Адміністратор даних може негайно припинити дію цього Договору, якщо оператор порушує положення Основного договору, зокрема, якщо оператор:

a) незважаючи на зобов'язання усунути виявлені під час перевірки недоліки, не усуне їх у встановлений термін;
b) опрацьовує персональні дані у спосіб, що не відповідає договору;
c) довірив опрацювання персональних даних іншому суб'єкту без згоди адміністратора даних;

або Норм про захист персональних даних, зокрема у разі розкриття персональних даних неуповноваженим особам, а також у разі, якщо контролюючий орган, відповідальний за нагляд за дотриманням положень про захист персональних даних, встановить, що оператор не дотримується цих Норм.

7.3 У разі припинення дії даного Договору з причин, зазначених у пункті 8 вище, Сторони зобов'язуються розпочати обговорення протягом трьох календарних днів з дати припинення дії цього Договору доручення, з метою визначення способу виконання Основного договору.

§8

Правила дотримання конфіденційності

1. Оператор зобов'язується зберігати в таємниці всю інформацію, дані, матеріали, документи та персональні дані, отримані від адміністратора даних та від осіб, які з ним співпрацюють, а також дані, отримані будь-яким

іншим способом, навмисно чи випадково, в усній, письмовій або електронній формі.

2. Оператор заявляє, що у зв'язку з зобов'язанням дотримуватися конфіденційності щодо даних конфіденційного характеру, вони не будуть використовуватися, розголошуватися або надаватися без письмової згоди адміністратора даних для будь-яких цілей, крім виконання Договору, за винятком випадків, коли необхідність оприлюднення інформації випливає з чинних норм законодавства або Договору.

§9

Прикінцеві положення

1. Договір складено у двох однакових примірниках для кожної зі сторін.

2. У питаннях, які не врегульовано, будуть застосовуватися положення Цивільного кодексу та Регламенту.

3. Судом, відповідним для вирішення спорів, котрі виникають з даного договору, є суд, відповідно до юрисдикції адміністратора даних.

_____ _____

Адміністратор даних Оператор

Додаток №1 до Договору про Доручення опрацювання персональних даних

Протокол

Повернення / видалення персональних даних з картотеки даних

(зразок)

.....

(реєстраційний номер)

.....

(місце і дата складання)

Комісія в складі:

1.

.....

.....

2.

.....

.....

3.

.....

.....

(дані членів комісії)

Призначена (ким) .....
(дата) ..... р.

(назва оператора даних чи вповноваженої ним особи)

На підставі .....

.....

(правова підстава видалення даних)

*видалила з картотеки даних **і повернула адміністраторові даних

(зазначте те, що правильне)

.....

.....

(назва картотеки даних)

Персональні дані

.....

.....

.....

.....

.....

.....

(опис видалених персональних даних)

(ким)

.....

.....

.....

.....

(перелік пошкоджених документів або IT-носіїв, що містять персональні дані, та спосіб знищення цих даних)

1. .....
2. .....
3. .....

Додаток №2 до Договору Доручення опрацювання персональних даних

Звіт про інцидент порушення персональних даних

(зразок)

Дата і час інциденту / порушення:	
Хто повідомляє про інцидент / порушення:	
Вид і місце інциденту / порушення:	
Опис перебігу інциденту / порушення:	
Причини інциденту / порушення:	
Наслідки інциденту / порушення:	
Вжиті заходи реагування:	

Додаток № 2

Звіт про інцидент безпеки / порушення захисту персональних даних

(зразок)

Дата і година інциденту / порушення:	
Хто повідомляє про інцидент / порушення:	
Вид і місце інциденту / порушення:	
Хто надає пояснення щодо інциденту / порушення:	
Опис перебігу інциденту / порушення:	
Причини інциденту / порушення:	
Наслідки інциденту / порушення:	
Вжиті заходи реагування:	

Додаток №3

Реєстр порушень захисту персональних даних

(Зразок)

№ п/п	Вид порушення	Обов'язок повідомити наглядовому органу ТАК / НІ	Обов'язок повідомити суб'єкт даних ТАК / НІ	Обставини порушення	Наслідки порушення	Вжиті заходи реагування

Додаток №4

Реєстр договорів доручення

(зразок)

№ п/п, рік	Дані ідентифікації суб'єкта опрацювання	Довірені дії		Дата укладення договору / додаткової угоди	Термін дії договору	Доступ до звичайних / особливих даних	Примітки
		сфера	Місце виконання				

Документ опрацювала

Анастасія Чорногорська, Заступниця Керівника Представника

Анастасія Чорногорська
Анастасія Чорногорська (8 черв. 2023 16:49 GMT+3)

Документ затвердив

Павел Кост, Керівник Представництва

Paweł Kost
Paweł Kost (12 черв. 2023 08:26 GMT+3)

SFPLinUA_Compliance_05_Personal_data_protection_policy

Підсумковий звіт «Аудит» 2023-06-12

Створено:	2023-06-08
Від:	Documents UA (documents_ua@solidarityfund.pl)
Стан:	Підписано
Код транзакції:	CBJCHBCAABAAcBUiDUONawV0WuU0hlZ1CoscUj82N21N

Історія "SFPLinUA_Compliance_05_Personal_data_protection_policy"

Користувач Documents UA (documents_ua@solidarityfund.pl) створив документ
2023-06-08 - 13:40:01 GMT

Користувач anastasiia.chornohorska@solidarityfund.pl надіслав документ електронною поштою для підписання
2023-06-08 - 13:43:52 GMT

Користувач anastasiia.chornohorska@solidarityfund.pl переглянув електронного листа
2023-06-08 - 13:48:36 GMT

Підписант anastasiia.chornohorska@solidarityfund.pl зазначив таке ім’я: Анастасія Чорногорська
2023-06-08 - 13:49:17 GMT

Користувач Анастасія Чорногорська (anastasiia.chornohorska@solidarityfund.pl) поставив електронний підпис на документ
Дата підписання: 2023-06-08 – 13:49:19 GMT – Джерело часу: сервер

Користувач pawel.kost@solidarityfund.pl надіслав документ електронною поштою для підписання
2023-06-08 - 13:49:21 GMT

Користувач pawel.kost@solidarityfund.pl переглянув електронного листа
2023-06-08 - 13:49:22 GMT

Підписант pawel.kost@solidarityfund.pl зазначив таке ім’я: Paweł Kost
2023-06-12 - 5:26:07 GMT

Користувач Paweł Kost (pawel.kost@solidarityfund.pl) поставив електронний підпис на документ
Дата підписання: 2023-06-12 – 5:26:09 GMT – Джерело часу: сервер

Підписання угоди завершено.

2023-06-12 - 5:26:09 GMT