Політика захисту даних у Представництві Фонду міжнародної солідарності в Україні

Дата останнього оновлення: 20230811

Предмет і мета документу

У цій Політиці описано принципи гарантування безпеки даних, обробка яких здійснюється як віртуально в інформаційних системах, так і на фізичних носіях, що обов'язкові для всіх організаційних підрозділів Фонду. Документ визначає також поділ відповідальності за цей процес у Фонді.

Мета документу — забезпечити уніфікований підхід до захисту даних, що обробляються в Фонді.

Додатком до «Політики» з технічного боку є «Інструкція з управління інформаційними системами», а також «Інструкція з архівування даних як віртуально, так і на фізичних носіях».

Захист персональних даних — це окрема частина процесу захисту даних і з огляду на специфічне правове регулювання в цій сфері він був прописаний у «Політиці захисту персональних даних», документі, уніфікованому з цією «Політикою».

Політика захисту даних

Пов'язані документи:

- Політика захисту персональних даних
- Інструкція з управління інформаційними системами
- Інструкція з архівування даних як віртуально, так і на фізичних носіях

Зміст

Дефініції

Головний спеціаліст з безпеки — працівник, відповідальний за захист даних на рівні всього Фонду, зокрема за захист інформаційних систем, а також за розробку стандартів, що стосуються IT-оснащення Фонду.

Дані — інформація, обробкою якої займається Фонд, пов'язана з самою організацією, а також із реалізованими нею процесами, зокрема інформація програмного, операційного, юридичного, фінансового й технічного характеру, не залежно від формату й способу її зберігання й поширення.

Доступність даних — забезпечення безперешкодного доступу до даних, які обробляє Фонд, для уповноважених користувачів.

Захист даних — забезпечення дотримання правил безпеки щодо способів обробки даних в організації.

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

Інформаційна система — низка пристроїв, програм, процедур обробки інформації та програмних інструментів, які взаємодіють між собою і використовуються з метою обробки даних.

Керівник організаційного підрозділу — член Правління Фонду чи особа, яка очолює Головний офіс або відділ Фонду за дорученням Правління Фонду.

Конфіденційність даних — ненадання даних неуповноваженим користувачам.

Користувач — особа, уповноважена Фондом для обробки даних.

Локальний спеціаліст із безпеки — працівник, відповідальний за захист даних на рівні організаційного підрозділу. Цю функцію виконує керівник організаційного підрозділу чи призначена ним особа.

Обробка даних — будь-які операції, що виконуються з даними, такі як: збирання, реєстрація, зберігання, впорядкування, зміна, надання доступу і видалення даних на фізичних носіях чи в інформаційних системах.

Організаційний підрозділ — окремі організаційні одиниці Фонду: Головний офіс у Польщі й зареєстровані відділи Фонду.

Порушення захисту даних — порушення безпеки, що призводить до випадкового чи протизаконного знищення, втрати, зміни, несанкціонованого оприлюднення чи несанкціонованого доступу до даних, які Фонд пересилає, зберігає чи обробляє.

Фонд міжнародної солідарності (далі — Фонд) — власник даних, обробку яких здійснює.

Цілісність даних — забезпечення точності, цілісності та актуальності даних.

Частина І. Загальні положення

1.1. Ця політика стосується гарантування безпеки даних, що обробляються в усіх організаційних підрозділах Фонду. Фонд обробляє дані передусім у віртуальному форматі в інформаційних системах, але деякі дані також обробляються на фізичних носіях на папері. Додатком до цієї політики, який містить уточнення технічного характеру, є «Інструкція з управління інформаційними системами».

1.2. Дії, що виконуються у зв'язку з обробкою і захистом даних у Фонді, мають узгоджуватися з іншими внутрішніми документами й відповідними нормами права, що діють у країні, в якій міститься конкретний організаційний підрозділ. У разі протиріч у законодавстві, першорядними є норми права тієї країни, де знаходиться дана організаційний підрозділ. Щодо персональних даних слід дотримуватися норм Загального регламенту про захист даних (GDPR), що стосуються забезпечення захисту персональних даних громадян і резидентів Європейського союзу, які надсилаються і обробляються за межами Європейської економічної зони.

1.3. Ця політика має вищість щодо окремих положень, інструкцій і інших документів, які приймаються в окремих організаційних підрозділах для захисту даних.

1.4. Захист персональних даних — це окрема частина процесу захисту даних і з огляду на специфічне правове регулювання він був прописаний у «Політиці захисту персональних даних», рівнозначному й узгодженому з цією політикою документі.

Принципи безпеки даних у ФМС — ієрархія

Рівень 1: відповідність до законодавства: GDPR й норми місцевого законодавства, якими керується конкретний організаційний підрозділ, зокрема норми, які стосуються захисту персональних даних

↓

Рівень 2 (уніфікований у межах усієї організації) «Політика захисту даних» Фонду + «Інструкція з управління інформаційними системами». Рівнозначний документ: «Політика захисту персональних даних»

↓

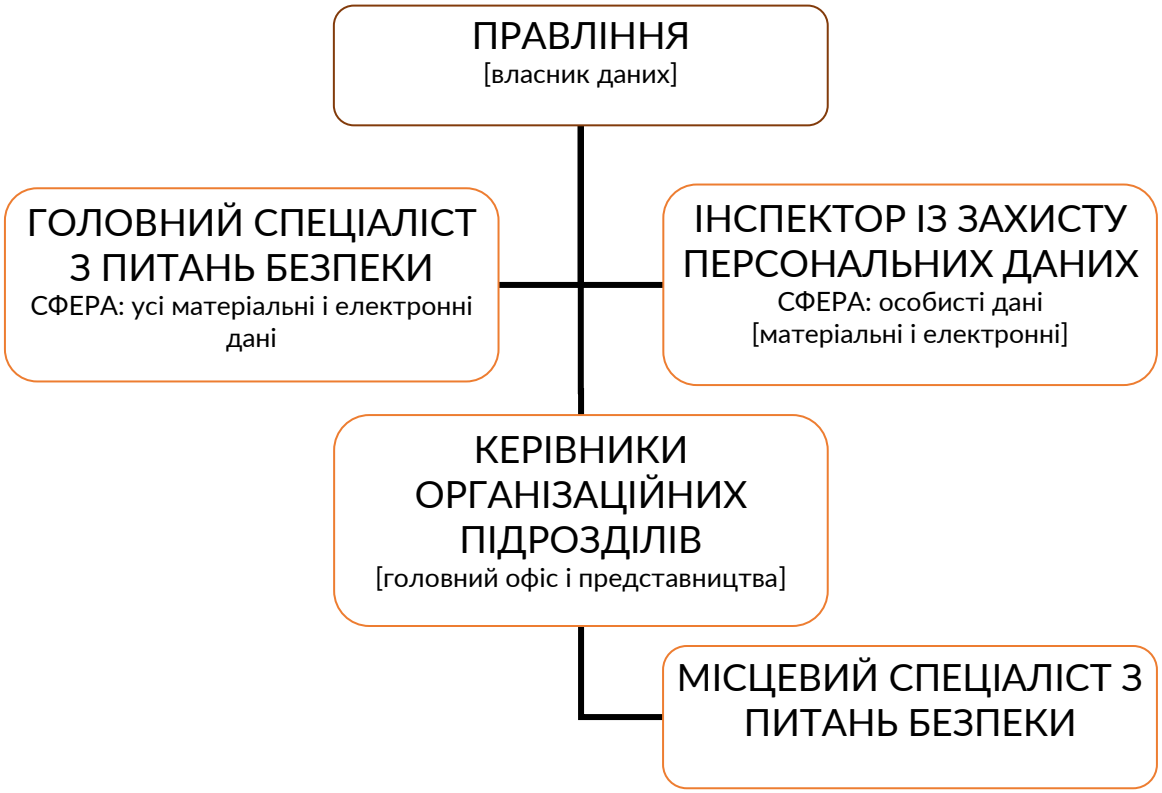
Рівень 3 організаційний підрозділ: місцеві положення захисту даних, а також інструкція з управління інформаційними системами + місцеві положення щодо захисту персональних даних

1.5. Правління доручає контроль над безпекою фізичних даних та інформаційних систем, у яких обробляються дані, а також відповідальність за визначення стандартів, які стосуються безпечних електронних пристроїв, які використовуються в Фонді, Головному спеціалісту з безпеки.

1.6. З огляду на особливе правове регулювання, а також їхню специфіку контроль над захистом персональних даних доручено Інспектору із захисту персональних даних, який тісно співпрацює з Головним спеціалістом із безпеки.

1.7. На рівні організаційного підрозділу за безпеку техніки, яка використовується локально, відповідальний керівник цього підрозділу.

Розподіл відповідальності за захист даних



1.8. Серед обов'язків Правління Фонду — забезпечити, щоб працівники й особи, з якими Фонд співпрацює, мали відповідні знання щодо безпечної обробки даних в інформаційних системах, а також безпечного використання техніки. Навчання співробітників з цієї теми покладається на Головного спеціаліста з безпеки.

Частина II. Безпека й захист даних у Фонді

1. Технічні засоби й організаційні ресурси, необхідні для забезпечення конфіденційності, цілісності й доступності даних у Фонді

1.1. Фонд використовує технічні засоби й організаційні ресурси, необхідні для забезпечення конфіденційності, цілісності й доступності даних, які обробляються в інформаційних системах, а також на фізичних носіях.

1.2. Контроль і нагляд за обробкою даних у Фонді передбачає:

a) захист даних засобами, відповідними до виявленого рівня ризику, зокрема окремий нагляд над обробкою й видаленням документації з конфіденційною інформацією, а також псевдонімізація та шифрування даних там, де це необхідно;

b) постійний моніторинг інформаційних систем, забезпечення запасних копій і виявлення пробілів;

c) надання доступу до даних лише уповноваженим особам;

d) захист від зовнішніх і внутрішніх атак;

e) реагування у випадку порушення безпеки даних;

f) обробку даних відповідно до законодавства

g) забезпечення відповідного захисту даних у випадку доручення обробки даних іншим особам, які займатимуться обробкою.

1.3. Усі Користувачі зобов'язані обробляти дані відповідно до чинних норм місцевого законодавства і відповідно до цієї політики, а також інших внутрішніх документів і процедур, пов'язаних із обробкою даних у Фонді. Усі особи зобов'язані зберігати конфіденційність даних, які вони обробляють.

2. Правила безпеки, що діють в офісах Фонду

2.1. З метою мінімізувати загрози, пов'язані з несанкціонованим доступом третіх осіб до даних, у всіх офісах організаційних підрозділів Фонду обов'язковим є:

a) обмежена кількість працівників, які мають власний ключ чи додаток для включення і виключення сигналізації/коду доступу (залежно від системи) до цього офісу;

b) графік роботи в офісі окремих працівників/осіб, які співпрацюють із Фондом;

c) принцип чистого столу, згідно з яким після закінчення роботи всі документи, що містять дані, ховають у стіл, де вони в відповідній безпеці;

d) принцип чистого екрану, згідно з яким під час відсутності Користувача біля комп'ютера, має погаснути екран, а повторний вхід в систему має вимагати вписування пароля Користувача чи використання біометрики;

e) заборона на записування паролів доступу й залишення їх на видноті;

f) обов'язкове використання програм шифрування для зберігання паролів.

2.2. В окремих організаційних підрозділах Фонду може бути обов'язковим відеонагляд. У випадку використання відеонагляду в офісі організаційного підрозділу, Фонд зобов'язаний детально поінформувати працівників про рамки застосованого рішення. Записувати можна лише зображення (без звуку).

2.3. В окремих організаційних підрозділах Фонду інформацією про ключових контрагентів і послуги (напр., інтернет, електроенергія, мобільний зв'язок, система моніторингу чи охорони будівлі тощо) володіє певне коло працівників, уповноважених керівником цього підрозділу контактувати з цими постачальниками.

3. Доступ до внутрішніх інформаційних систем та електронної пошти Фонду

3.1. Доступ до даних у інформаційній системі мають виключно Користувачі.

3.2. Профіль Користувача системи разом із правом доступу до окремих внутрішніх інформаційних систем Фонду, електронної пошти Фонду й до електронного архіву (архівізованих ресурсів) Фонду створюється спеціалістом з IT/локальним спеціалістм з IT після отримання згоди Дирекції ФМС чи керівника конкретної організаційного підрозділу. Так само надаються нові права доступу Користувачам.

3.3. Користувач інформаційної системи отримує доступ до даних, що обробляються в інформаційних системах Фонду, відповідно до рівня уповноваження.

3.4. Профіль Користувача системи захищений системою двофакторної автентифікації: паролем, який відповідає вимогам безпеки, описаним у документі «Управління інформаційною системою», а також додатковим захистом у вигляді ключа U2F чи додатку «Автентифікатор», який підходить для даного профілю. Заборонено розголошувати паролі до систем чи самовільно надавати доступ до інформаційної системи третім особам.

3.5. Профіль Користувача заморожується у день закінчення повноваження чи за зверненням керівника, а дані, зібрані Користувачем у системах, наданих Фондом, залишаються власністю Фонду. В окремих випадках керівник організаційного підрозділу чи директор Фонду може дати згоду на продовження повноваження Користувачеві.

3.6. У випадку довгої відсутності Користувача (напр., декретна відпустка, тривала хвороба), його профіль може бути заморожений або обмежений.

4. Правила користування Користувачами інформаційними системами, а також електронною поштою

4.1. Працівники/особи, з якими Фонд співпрацює, на звернення начальника/керівника проєкту отримують доступ до електронної пошти чи призначених для них ресурсів, доступних у інформаційних системах Фонду.

4.2. Дані, важливі для роботодавця/працівника, повинні зберігатися виключно в інформаційних системах, які надає Фонд.

4.3. Службова кореспонденція (внутрішня й зовнішня) має вестися за допомогою електронних засобів зв'язку, прийнятих у Фонді. Електронну пошту Фонду можна використовувати лише для цілей, пов'язаних із виконанням роботи.

4.4. Перед надсиланням/наданням доступу до даних, особливо персональних/чутливих даних, працівник/особа, з якою Фонд співпрацює, повинна перевірити вірогідність контактних даних партнерів і контрагентів.

4.5. З метою забезпечення організації роботи, що уможливлює повне використання робочого часу й належне використання наданих працівникові інструментів для роботи, передбачається ймовірність моніторингу електронної пошти, а також способу використання інформаційних систем Користувачем.

4.6. Роботодавець може ввійти у службовий профіль електронної пошти працівника чи в інформаційну систему Користувача лише з його згоди чи у випадку інформації про велику ймовірність порушення працівником законодавства чи положень Фонду. У випадку моніторингу без згоди працівника, моніторинг проводиться комісією у складі двох осіб, уповноважених Правлінням Фонду.

4.7. Моніторинг не може порушувати прав і гідності працівника.

5. Правила користування Користувачів телеінформаційною технікою

5.1. Телеінформаційна техніка (ноутбук, мобільний телефон, фотоапарат тощо) видається працівникам/особам, які співпрацюють з Фондом за протоколом, згідно з письмовим розпорядженням керівника організаційного підрозділу. Використання техніки й комп'ютерних програм роботодавця завжди мусить відбуватися відповідно до чинного законодавства і внутрішніх положень.

5.2. Не слід встановлювати жодної програми без згоди IT-спеціаліста чи використовувати додатки, доступні онлайн, яких немає у списку додатків, дозволених для використання IT-спеціалістом.

5.3. Забороняються будь-які зміни налаштувань комп'ютера роботодавця.

5.4. Працівники й особи, з якими Фонд співпрацює, не повинні використовувати зовнішніх носіїв на службових телеінформаційних пристроях. У випадку необхідності використання такого носія, слід повідомити про це й отримати згоду на таку дію від IT-спеціаліста.

5.5. Забороняється відкривати файли підозрілого походження. У разі сумнівів, слід звернутися за порадою до IT-спеціаліста.

5.6. Працівники/особи, з якими Фонд співпрацює, повинні користуватися ресурсами роботодавця і електронною поштою на службових телеінформаційних пристроях.

5.7. Коли ситуація вимагає використання підозрілого пристрою, слід використовувати приватний режим браузера, щоб бути впевненим, що дані будуть усунені з комп'ютера після закриття усіх віконець. Додатково в такій ситуації слід

обмежитися використанням тільки програм, які доступні в браузері онлайн. Слід утриматися від збереження будь-яких файлів на цей пристрій і якомога швидше змінити свій пароль/і доступу.

5.8. Працівники/особи, з якими Фонд співпрацює, під час робочих зустрічей, які відбуваються на території, куди не можна проносити телеінформаційні пристрої (напр., посольства іноземних держав), зобов'язані убезпечити службову техніку перед тим, як здати її на зберігання. Пристрої слід вимкнути і, якщо це можливо, убезпечити безпечним конвертом. З огляду на безпеку даних не рекомендується брати з собою службову техніку на такого типу зустрічі.

6. Правила користування Користувачів локальною мережею (LAN) та інтернетом в офісах Фонду

6.1. У локальній мережі в офісах Фонду слід користуватися виключно пристроями, які належать роботодавцю.

6.2. Особи, які відвідують офіс Фонду в Варшаві, не можуть користуватися інтернет-зв'язком організації, зокрема Wi-Fi. У відділеннях Фонду гості можуть користуватися окремою мережею для гостей.

6.3. Заборонено надавати паролі доступу до внутрішньої мережі особам, які не є працівниками/особами, з якими Фонд співпрацює.

6.4. Доступ до інтернету в офісах Фонду служить цілям, пов'язаним із виконанням роботи.

6.5. Активність в інтернеті повинна завжди відповідати чинному законодавству, а також не може порушувати хорошої репутації Фонду.

7. Правила безпеки даних під час роботи поза офісами Фонду

7.1. Працівники Фонду під час роботи поза офісами Фонду повинні користуватися виключно пристроями, які належать роботодавцю. Особи, які співпрацюють із Фондом, залежно від домовленостей, можуть користуватися власною технікою.

7.2. Під час роботи поза офісами Фонду слід користуватися надійними мережами/інтернет-зв'язками. Заборонено підключатися до інформаційних систем і пошти Фонду через відкриті незахищені мережі Wi-Fi.

7.3. Під час роботи з використанням конфіденційних даних поза офісами Фонду слід подбати про те, щоб не передавати ці дані третім особам і відповідно убезпечити пристрій під час перерв у роботі. Забороняється дистанційна робота з використанням цих у громадських місцях.

7.4. Заборонені подорожі зі службовою технікою, що містить службову інформацію, у країни з високим ризиком стеження. Перелік держав, про які йдеться вище, укладає й періодично актуалізує Головний спеціаліст із безпеки.

7.5. Заборонено заряджати телеінформаційну техніку загальнодоступними зарядними пристроями USB, USB-C, Lightning, які знаходяться у громадських місцях, напр., у торгових центрах, залізничних вокзалах, аеропортах, ресторанах.

7.6. Під час подорожі можливе заряджання шляхом використання надійних пристроїв, напр., павербанків і оригінальних зарядних пристроїв від техніки, наданих Фондом.

7.7. Не слід залишати телеінформаційні пристрої без нагляду.

7.8. У ситуації поїздки у особливо небезпечні місця, в місця з великою імовірністю крадіжки даних (чи конфіскації пристроїв), слід звернутися до IT-спеціаліста з проханням надати спеціальний пристрій для подорожі, який не містить даних. Такого типу пристрій слід сприймати як ненадійний і діяти відповідно до п. 5.7 цієї політики.

8. Доступ до даних Фонду на фізичних носіях

8.1. Дані на фізичних носіях належним чином захищені й не можуть бути доступні особам неуповноваженим.

8.2. Дані в паперовому вигляді й цифрові носії даних зберігаються в замкнутих приміщеннях і замкнутих шафах.

9. Архівування даних

9.1. Дані, які обробляє Фонд, підлягають архівуванню відповідно до законодавчих вимог і внутрішніх правил, затверджених у Фонді.

9.2. Архівовані дані збираються, зберігаються і захищаються від недозволених змін, несанкціонованого поширення, пошкодження чи знищення.

9.3. Документація може зберігатися на фізичних носіях (архів у паперовому форматі), а також у віртуальному вигляді (архів у інформаційних системах).

9.4. Проєктна документація підлягає архівуванню в обсязі, що вимагається донатором і відповідно до правових вимог і внутрішніх правил, затверджених у Фонді. Більшість документації зберігається у віртуальному форматі.

9.5. Доступ до заархівованої документації можна отримати після погодження відповідної заявки дирекцією ФМС і керівниками конкретної організаційного підрозділу. Дані надаються особами, які уповноважені управляти архівом.

10. Процедура сповіщення про інциденти

10.1. Інцидентом, якщо йдеться про обробку даних, є ситуація, що спричиняє загрозу втрати конфіденційності, цілісності чи доступу до оброблюваних даних, зокрема:

a) неавторизований доступ до даних,

b) неавторизовані зміни чи видалення даних,

c) надання доступу до даних неавторизованим суб'єктам,

d) нелегальне оприлюднення даних,

e) отримання даних із нелегальних джерел.

10.2. Кожен Користувач у випадку отримання інформації про інцидент чи у випадку підозри про інцидент, тобто:

a) крадіжки комп'ютера, телефонів, інших носіїв електронних даних;

b) виявлення слідів проникнення у приміщення, в яких зберігаються дані;

c) виявлення відсутності належного захисту даних;

d) підозри щодо отримання доступу до даних неуповноваженими особами (напр., дані, які стосуються історії хвороби чи заробітної плати працівника стають доступні неуповноваженим особам);

e) втрати паперової документації, що містить дані;

f) відсутності доступу до електронної скриньки, відсутності доступу в системі MS365;

g) виявлення залогінення з невідомого пристрою у електронну скриньку/у профіль в системі MS365;

h) виявлення невідомого пристрою, підключеного до месенджера (Whatsapp, Signal тощо)

зобов'язаний без зволікань сповістити про це шляхом заповнення «Формуляра інформування про інциденти», доступного всім працівника Фонду. Якщо Користувач втратив доступ до цього каналу комунікації, він мейлом чи за посередництвом керівника/іншого працівника контактує з: Локальним спеціалістом з безпеки (якщо такий був призначений), Головним спеціалістом із безпеки і Інспектором із захисту персональних даних.

10.3. У разі неможливості сповіщення вище перелічених осіб, слід повідомити безпосереднього керівника, а також Директора ФМС, відповідального за безпеку.

10.4. До передачі справи відповідним особам слід:

a) якнайшвидше вжити заходів для обмеження небажаних наслідків виявленого порушення — слід якнайшвидше відключити пристрій від інтернету й вимкнути його. Не вмикати інфікований пристрій і передати його в IT-відділ з описом ситуації;

b) спробувати з'ясувати причини чи винуватців порушення даних;

c) зупинити використання інфікованого пристрою — звернутися з проханнях про нову техніку;

d) задокументувати інцидент для аналізу.

11. Прикінцеві положення

11.1. Політика підлягає періодичній верифікації, не рідше, ніж раз на 3 роки. За моніторинг відповідальний Головний спеціаліст із безпеки.

11.2. Політика набуває чинності у день, вказаний у рішенні Правління Фодну.

11.3. Ця політика заміняє інші чинні до цього моменту в Фонді документи (що стосуються предмету цієї політики).

Документ опрацювала
Анастасія Чорногорська, Заступниця Керівника Представника

Анастасія Чорногорська
Анастасія Чорногорська (8 черв. 2023 16:50 GMT+3)

Документ затвердив
Павел Кост, Керівник Представництва

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

SFPLinUA_IT_01_Data_protection_policy

Підсумковий звіт «Аудит» 2023-06-12

Створено:	2023-06-08
Від:	Documents UA (documents_ua@solidarityfund.pl)
Стан:	Підписано
Код транзакції:	CBJCHBCAABAAQaR_4iseOi3mmeYIL-4xCt_aqxbXjxxZ

Історія "SFPLinUA_IT_01_Data_protection_policy"

Користувач Documents UA (documents_ua@solidarityfund.pl) створив документ
2023-06-08 - 13:44:18 GMT

Користувач anastasiia.chornohorska@solidarityfund.pl надіслав документ електронною поштою для підписання
2023-06-08 - 13:48:03 GMT

Користувач anastasiia.chornohorska@solidarityfund.pl переглянув електронного листа
2023-06-08 - 13:49:57 GMT

Підписант anastasiia.chornohorska@solidarityfund.pl зазначив таке ім'я: Анастасія Чорногорська
2023-06-08 - 13:50:21 GMT

Користувач Анастасія Чорногорська (anastasiia.chornohorska@solidarityfund.pl) поставив електронний підпис на документ
Дата підписання: 2023-06-08 – 13:50:23 GMT – Джерело часу: сервер

Користувач pawel.kost@solidarityfund.pl надіслав документ електронною поштою для підписання
2023-06-08 - 13:50:25 GMT

Користувач pawel.kost@solidarityfund.pl переглянув електронного листа
2023-06-08 - 13:50:27 GMT

Підписант pawel.kost@solidarityfund.pl зазначив таке ім'я: Paweł Kost
2023-06-12 - 5:26:57 GMT

Користувач Paweł Kost (pawel.kost@solidarityfund.pl) поставив електронний підпис на документ
Дата підписання: 2023-06-12 – 5:26:59 GMT – Джерело часу: сервер

Підписання угоди завершено.
2023-06-12 - 5:26:59 GMT