ЗАТВЕРДЖЕНО

Наказом Директора
ТОВ «КРЕДИТ 911»

від "13" серпня 2021 року №13082021/1-ПД

_____Радченко О.А.

ПОЛОЖЕННЯ

Про обробку і захист персональних даних

1. Призначення і область застосування

1.1. Положення про організацію та забезпечення захисту персональних даних у ТОВ «КРЕДИТ 911» призначене для організації та проведення заходів щодо забезпечення захисту персональних даних відповідно до вимог Закону України «Про захист персональних даних».

1.2. Положення визначає порядок організації робіт, вимог, правил і рекомендацій щодо забезпечення захисту персональних даних у ТОВ «КРЕДИТ 911».

1.3. Положення є локальним нормативним правовим актом ТОВ «КРЕДИТ 911» (надалі Товариство або Колекторська компанія). Вимоги Положення обов'язкові для виконання всіма працівниками, які допущені до обробки персональних даних.

2. Терміни та скорочення

ІСПДн	Інформаційна система персональних даних
ЛОС	Локальна обчислювальна мережа
НСД	Несанкціонований доступ
ПДн	Персональні дані
ПЗ	Програмне забезпечення
ЗЗІ	Засоби захисту інформації
СЗПДн	Система (підсистема) захисту персональних даних
ЗУ	Закон України

Автоматизована обробка персональних даних - обробка персональних даних за допомогою засобів обчислювальної техніки.

Блокування персональних даних - тимчасове припинення обробки персональних даних (за винятком випадків, якщо обробка необхідна для уточнення персональних даних).

Вірус (комп'ютерний, програмний) - програмний код, що виконується або інтерпретований набір інструкцій, що володіє властивостями несанкціонованого розповсюдження та самовідтворення. Створені дублікати комп'ютерного вірусу не завжди збігаються з оригіналом, але зберігають здатність до подальшого поширення та самовідтворення.

Шкідлива програма - програма, призначена для здійснення несанкціонованого доступу і (або) впливу на персональні дані або ресурси інформаційної системи персональних даних.

Доступ до інформації - можливість отримання інформації та її використання.

Інформація, що захищається - інформація, що є предметом власності та підлягає захисту, відповідно до вимог правових документів або вимог, встановлених власником інформації.

Ідентифікація - привласнення суб'єктам та об'єктам доступу ідентифікатора і (або) порівняння ідентифікатора, що пред'являється, з Переліком привласнених ідентифікаторів.

Інформація - відомості (повідомлення, дані) незалежно від форми їх подання.

Інформаційна система персональних даних - сукупність містяться в базах даних персональних даних та забезпечують їх обробку інформаційних технологій і технічних засобів.

Інформаційні технології - процеси, методи пошуку, збору, зберігання, обробки, надання, поширення інформації та способи здійснення таких процесів і методів.

Контрольована зона - простір (територія, будівля, частина будівлі, приміщення), в якому виключене неконтрольоване перебування сторонніх осіб, а також транспортних, технічних та інших матеріальних засобів.

Матеріальний носій персональних даних (далі матеріальний носій) - матеріальний об'єкт, що використовується для закріплення та зберігання інформації. В даному Положенні під матеріальним носієм розуміється паперовий документ, диск, дискета, флеш-карта і т.п.

Міжмережевий екран - локальний (однокомпонентний) або функціонально-розподілений програмний (програмно-апаратний) засіб (комплекс), що реалізує контроль за інформацією, що надходить в інформаційну систему персональних даних та (або) виходить з інформаційної системи.

Несанкціонований доступ (несанкціоновані дії) - доступ до інформації або дії з інформацією, що порушують правила розмежування доступу з використанням штатних засобів, що надаються інформаційними системами персональних даних.

Обробка персональних даних - будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем.

Технічні засоби інформаційної системи персональних даних - засоби обчислювальної техніки, інформаційно-обчислювальні комплекси та мережі, засоби та системи передачі, прийому та обробки ПДн (засоби та системи звукозапису, звукопідсилення, звуковідтворення, переговорні та телевізійні пристрої, засоби виготовлення, тиражування документів та інші технічні засоби обробки мовної, графічної, відео- і літеро-цифрової інформації), програмні засоби (операційні системи, системи управління базами даних тощо), засоби захисту інформації.

Персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Правила розмежування доступу - сукупність правил, що регламентують права доступу суб'єктів доступу до об'єктів доступу.

Програмне (програмно-математичне) вплив - несанкціонований вплив на ресурси інформаційної системи, що здійснюється з використанням шкідливих програм.

Ресурс інформаційної системи - іменований елемент системного прикладного або апаратного забезпечення функціонування інформаційної системи.

Засіб обчислювальної техніки - сукупність програмних і технічних елементів систем обробки даних, здатних функціонувати самостійно або в складі інших систем.

Суб'єкт доступу (суб'єкт) - особа або процес, дії якого регламентуються правилами розмежування доступу.

Знищення персональних даних - дії, в результаті яких стає неможливим відновити зміст персональних даних в інформаційній системі персональних даних та (або) в результаті яких знищуються матеріальні носії персональних даних.

Цілісність інформації - здатність засобу обчислювальної техніки або інформаційної системи забезпечувати незмінність інформації в умовах випадкового і / або навмисного викривлення (руйнування).

3. Загальні положення

3.1. Необхідність проведення заходів щодо захисту персональних даних в ТОВ «КРЕДИТ 911» визначається:

- Законом України від 01.06.2010 р № 2297-VI «Про захист персональних даних»;
- Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. № 1/02-14 «Про затвердження документів у сфері захисту персональних даних»;
- Конвенцією Ради Європи №108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних».

3.2. Метою захисту ПДн є запобігання можливого витоку інформації і (або) несанкціонованого та ненавмисної зміни або руйнування ПДн.

3.3. Виконання заходів щодо захисту ПДн дозволяє забезпечити захист прав і свобод людини та громадянина при обробці його персональних даних, у тому числі захист прав на недоторканність приватного життя, особисту та сімейну таємницю.

3.4. Захист ПДн досягається виконанням комплексу організаційних заходів та застосуванням засобів захисту інформації від несанкціонованого доступу, програмно-математичних впливів з метою порушення цілісності (модифікації, знищення) та доступності інформації в процесі її обробки, передачі та зберігання, а також працездатності технічних засобів.

3.5. Усі працівники, що обробляють ПДн і забезпечують захист ПДн, повинні бути ознайомлені з цим Положенням під підпис.

4. Персональні дані, що підлягають захисту

4.1. Персональні дані, що підлягають захисту, затверджуються наказом директора ТОВ «КРЕДИТ 911» у вигляді Переліку оброблюваних персональних даних.

4.2. Зміни, доповнення переліку персональних даних, що обробляються в ТОВ «КРЕДИТ 911», здійснюються на підставі інформації, що надається працівникам та керівниками підрозділів, які обробляють ПДн при виконанні посадових обов'язків.

4.3. Персональні дані, що підлягають захисту в ТОВ «КРЕДИТ 911», також надаються Кредитодавцем у вигляді Електронного реєстру боржників на підставі агентського договору між Кредитором та ТОВ «КРЕДИТ 911».

5. Організаційна система забезпечення безпеки ПДн

5.1. До складу організаційної системи забезпечення безпеки ПДн Товариства входять:

- Директор ТОВ «КРЕДИТ 911»
- особа, відповідальна за організацію обробки персональних даних;
- працівники Відділу інформаційних технологій;
- керівники підрозділів, працівникам яких надано доступ до ПДн;
- працівники, яким надано доступ до ПДн (ІСПДн користувачі).

5.2. Загальне керівництво організацією робіт із захисту ПДн здійснює Директор Товариства.

5.3. Особа, відповідальна за організацію обробки персональних даних, в межах забезпечення безпеки ПДн виконує такі функції:

- організовує процеси розробки, затвердження та коригування локальних правових актів щодо забезпечення безпеки ПДн;

- здійснює внутрішній контроль за дотриманням Товариства і його працівниками законодавства України про персональні дані, у тому числі вимог до захисту персональних даних;

• доводить до відома працівників Товариства положення законодавства України про захист ПДн, локальних актів з питань обробки ПДн, вимог до захисту ПДн.

5.4. З числа працівників Відділу інформаційних технологій призначаються адміністратори безпеки. Обов'язки адміністраторів безпеки, відповідальних за захист інформації, визначаються Інструкцією адміністраторам безпеки ІСПДн і включають:

• адміністрування, контроль працездатності і аналіз результатів роботи засобів захисту інформації ІСПДн;

• контроль діяльності структурних підрозділів Товариства по виконанню ними встановлених вимог забезпечення безпеки ПДн в ІСПДн Товариства.

• виявлення та розслідування спроб НСД, інформування керівництва про факти порушення встановленого порядку робіт і спробах НСД до інформаційних ресурсів;

• проведення періодичних перевірок захищеності ІСПДн;

• підготовка пропозицій щодо вдосконалення та реалізацію заходів щодо забезпечення безпеки ПДН в ІСПД.

5.5. Відділ інформаційних технологій в межах адміністрування ІСПДн здійснює:

• системне адміністрування серверів, мережевого обладнання;

• адміністрування прикладних систем ІСПДн, робочих станцій ІСПДн Товариства.

5.6. Відділ інформаційних технологій в межах забезпечення захисту ПДн здійснює такі функції:

• вносить зміни у список користувачів і здійснює відповідні налаштування загальносистемного ПЗ;

• здійснює адміністрування засобів антивірусного захисту;

• забезпечує підготовку пропозицій щодо вдосконалення та реалізації заходів щодо забезпечення безпеки ПДн в ІСПДн;

• здійснює взаємодію зі структурними підрозділами Товариства;

5.7. Керівники підрозділів, працівникам яких надано доступ до ПДн, узгоджують заявку на допуск користувачів до обробки ПДн в ІСПДн. Забезпечують безпеку ПДн і виконання заходів щодо захисту в підрозділах Товариства. Готують необхідні для виконання функцій підрозділу пропозиції щодо внесення змін до переліку персональних даних, що оброблюються, перелік працівників, допущених до обробки персональних даних.

5.8. Працівники, яким надано доступ до обробки ПДн в межах обробки без використання засобів автоматизації, безпосередньо реалізують організаційні заходи щодо забезпечення збереження носіїв ПДн і виконання процедур щодо дотримання вимог законодавства.

5.9. Працівники, яким надано доступ до обробки ПДН в ІСПДн (користувачі ІСПДн) безпосередньо реалізують вимоги безпеки інформації, прийняті для ІСПДн, виконують встановлені режими захисту ПДн, забезпечують суворе виконання запропонованих правил безпеки інформації.

6. Захист ПДн при обробці в інформаційних системах персональних даних

6.1. Заходи щодо забезпечення безпеки персональних даних при їх обробці в інформаційних системах включають в себе:

- визначення загроз безпеці персональних даних при їх обробці в ІСПДн, формування на їх основі моделі загроз;
- розробку моделі порушника при використанні криптографічних засобів для забезпечення безпеки персональних даних;
- визначення необхідного рівня захищеності ПДн при їх обробці в ІСПДн;
- розробку на основі моделі загроз і моделі порушника з урахуванням необхідного рівня захищеності ПДн, системи захисту персональних даних, що забезпечує нейтралізацію передбачуваних загроз;
- застосування процедур, що пройшли в установленому порядку оцінку відповідності засобів захисту інформації;
- опис системи захисту персональних даних;
- встановлення та введення в експлуатацію засобів захисту інформації, відповідно до експлуатаційної та технічно документації;
- навчання осіб, які використовують засоби захисту інформації, що застосовуються в інформаційних системах, правилам роботи з ними;
- оцінку ефективності вжитих заходів, щодо забезпечення безпеки персональних даних, до введення в експлуатацію інформаційної системи персональних даних;
- встановлення правил доступу до персональних даних, що оброблюються в інформаційній системі персональних даних, а також забезпеченням реєстрації та обліку всіх дій, вчинених з персональними даними в інформаційній системі персональних даних;
- облік засобів захисту інформації, експлуатаційної та технічної документації до них, машинних носіїв персональних даних, що застосовуються;
- облік осіб, допущених до обробки персональних даних в інформаційній системі;
- контроль за прийнятими заходами щодо забезпечення безпеки персональних даних та рівня захищеності інформаційних систем персональних даних, включаючи контроль за дотриманням умов використання засобів захисту інформації, передбачених експлуатаційною і технічною документацією;
- розгляд і складання висновків з фактами недотримання умов зберігання машинних носіїв персональних даних, використання засобів захисту інформації, дій можуть призвести до

порушення конфіденційності персональних даних або інших порушень, що призводить до зниження рівня захищеності персональних даних, розробку та вжиття заходів щодо запобігання можливих небезпечних наслідків подібних порушень;

- вжиття заходів, у разі виявлення фактів несанкціонованого доступу до персональних даних;

- відновлення персональних даних, модифікованих або знищених внаслідок несанкціонованого доступу до них.

6.2. Методи і способи захисту персональних даних включають в себе:

- реалізацію дозвільної системи допуску користувачів до інформаційних ресурсів, інформаційної системи та пов'язаним з її використанням роботами, документами;

- розмежування доступу користувачів до інформаційних ресурсів, програмним засобам обробки (передачі) та захисту інформації;

- реєстрацію дій користувачів, контроль несанкціонованого доступу та дій користувачів, сторонніх осіб;

- облік і зберігання змінних носіїв інформації, їх обіг, що виключає розкрадання, підміну та знищення;

- резервування технічних засобів, дублювання масивів і носіїв інформації;

- використання захищених каналів зв'язку;

- розміщення технічних засобів, що дозволяють здійснювати обробку персональних даних, тільки в межах території, що охороняється (робочі станції, сервери, комутаційне обладнання, мережеві принтери);

- організацію фізичного захисту приміщень і технічних засобів, що дозволяють здійснювати обробку персональних даних;

- запобігання впровадження в інформаційні системи шкідливих програм (програм-вірусів) і програмних закладок з використанням засобів антивірусного захисту.

6.3. Порядок розробки, введення в дію та експлуатації СЗПДн

6.3.1. Безпека ПДн при їх обробці в інформаційних системах забезпечується за допомогою системи захисту персональних даних (СЗПДн), що включає організаційні заходи та засоби захисту інформації, а також інформаційні технології, що використовуються в інформаційній системі.

6.3.2. Вимоги щодо захисту ПДн для кожної ІСПДн повинні формуватися у вигляді технічного завдання на створення СЗПДн в ІСПДн на етапі розробки (модернізації) ІСПДн.

6.4. Дозвільна система допуску користувачів до інформаційних ресурсів

6.4.1. Розмежування доступу до інформаційних ресурсів, що містять ПДн, повинно здійснюватися на підставі Переліку підрозділів та посадових осіб, допущених до обробки персональних даних у ТОВ «КРЕДИТ 911»

6.4.2. Деталізація повноважень користувачів по доступу до ресурсів ІСПДн документується в Матриці доступу, яка є експлуатаційним документом ІСПДн. Ведення матриці доступу та внесення відповідних змін в налаштування засобів розмежування прав доступу користувачів ІСПДн здійснюється працівниками відділу ІТ.

6.4.3. На періодичній основі або після кожної зміни в ІСПДн працівники відділу ІТ повинні проводити перевірку відповідності прав користувачів, визначених Переліком підрозділів та посадових осіб, допущених до обробки персональних даних у ТОВ «КРЕДИТ 911» з Матрицею доступу ІСПДн і діючими правами доступу до ІСПДн.

6.5. Реєстрація дій користувачів

6.5.1. Реєстрація дій користувачів, повинна здійснюватися засобами системного програмного забезпечення та ЗЗІ ІСПДн.

6.5.2. Підлягають обов'язковій реєстрації наступні операції, здійснювані в ІСПДн:

- реєстрація входу (виходу) користувачів в систему (з системи), або реєстрація завантаження та ініціалізації операційної системи і її програмного зупинення;

- реєстрація запуску (завершення) програм і процесів (завдань, задач), призначених для обробки персональних даних;

- реєстрація спроб доступу програмних засобів (програм, процесів, завдань, завдань) до файлів, що захищені;

- реєстрація спроб доступу програмних засобів, до додаткових захищених об'єктів доступу.

6.6. Резервування технічних засобів, дублювання масивів і носіїв інформації

6.6.1. Забезпечення цілісності та доступності ПДн, програмних і апаратних засобів ІСПДн, а також засобів захисту, при їх випадковій або навмисній модифікації, повинно здійснюватися за допомогою резервного копіювання (дублювання масивів і носіїв інформації) оброблюваних даних, резервування елементів ІСПДн.

6.6.2. Для забезпечення цілісності ІСПДн повинні виконуватися наступні заходи щодо резервування:

- резервні копії інформаційних ресурсів, що містять ПДн, повинні зберігатися у спеціально виділеному місці, територіально віддаленому від місця обробки самої інформації;

- для забезпечення збереження резервних копій повинен бути застосований комплекс організаційних і фізичних заходів захисту від НСД;

- носії, на які здійснюється резервне копіювання, повинні регулярно перевірятися на відсутність механічних пошкоджень, збоїв логічної структури, файлової системи;

- повинні проводитися регулярні перевірки процедур відновлення даних.

6.7. Фізичний захист приміщень і технічних засобів

6.7.1. Розміщення ІСПДн та охорона приміщень, в яких ведеться робота з персональними даними повинні забезпечувати збереження носіїв персональних даних і засобів захисту інформації, а також виключати можливість неконтрольованого проникнення або перебування в цих приміщеннях сторонніх осіб.

6.7.2. Виконання вимог щодо виключення можливості неконтрольованого проникнення або перебування в приміщеннях ІСПДн сторонніх осіб реалізується здійсненням організаційних і технічних заходів щодо створення контрольованої зони (КЗ) ТОВ «КРЕДИТ 911».

6.8. Використання засобів антивірусного захисту

6.8.1. Підсистема антивірусного захисту реалізується шляхом впровадження спеціального антивірусного програмного забезпечення на робочих станціях і серверах ІСПДн.

6.8.2. Засоби антивірусного захисту призначені для реалізації наступних функцій:

- антивірусне сканування;
- блокування шкідливих програм;
- автоматизоване оновлення антивірусних баз;
- обмеження прав користувача на зміну налаштувань антивірусного програмного забезпечення;
- автоматичний запуск одразу після завантаження операційної системи.

6.8.3. Про всі випадки збоїв антивірусного програмного забезпечення (появи повідомлень про помилки), користувач повинен негайно повідомляти фахівців Відділу інформаційних технологій.

7. Вживання заходів у разі виявлення фактів порушення вимог безпеки інформації, розгляд і складання висновків за фактами порушення вимог безпеки

7.1. Особа, яка виявила факт порушення вимог безпеки інформації, негайно повідомляє працівників Відділу ІТ про факт порушення.

7.2. У випадках виявлення порушень при обробці ПДн в ІСПДн необхідно:

- негайно припинити обробку ПДн в ІСПДн, де виявлені порушення та вжити заходи до їх усунення;
- організувати в установленому порядку розслідування причин і умов появи порушень з метою недопущення їх надалі та притягнення до відповідальності винних осіб.

7.3. Відновлення робіт дозволяється тільки після усунення порушень та перевірки достатності та ефективності вжитих заходів, відповідності їх вимогам нормативних документів щодо захисту ПДн.

7.4. Порядок проведення розслідування причин і умов виникнення порушення вимог (НСД до ПДн) визначається окремими локальними нормативними актами Товариства.

7.5. У випадки, якщо внаслідок НСД ПДн були модифіковані або знищені, здійснюється відновлення ПДн з резервної копії.

8. Вимоги до персоналу щодо забезпечення захисту ПДн

8.1. При вступі на посаду нового працівника, безпосередній керівник структурного підрозділу, до якого він надходить, зобов'язаний організувати його ознайомлення з посадовою інструкцією та необхідними документами, що регламентують вимоги щодо захисту ПДн. Працівники Відділу ІТ, навчають навичкам виконання процедур, необхідних для виконання вимог щодо захисту ПДн в ІСПДн.

8.2. Співробітники повинні дотримуватися, встановлених організаційно-розпорядчими документами, вимог по режиму обробки персональних даних, обліку, зберігання, передачі носіїв інформації та забезпечення безпеки ПДн.

9. Щодо обліку операцій, пов'язаних з обробкою персональних даних

9.1 З володільцем/розпорядником персональних даних зберігається інформація про:

– дату, час та джерело збирання персональних даних суб'єкта;

– зміну персональних даних;

– перегляд персональних даних;

– будь-яку передачу (копіювання) персональних даних суб'єкта;

– дату та час видалення або знищення персональних даних;

– працівника, який здійснив одну із указаних операцій;

– мету та підстави зміни, перегляду, передачі та видалення або знищення персональних даних.

9.2 Видалення або знищення персональних даних у разі:

1) закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом;

2) припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом;

3) видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого;

4) набрання законної сили рішенням суду щодо видалення або знищення персональних даних.

9.3 Про зміну, видалення чи знищення персональних даних або обмеження доступу до них володілець персональних даних протягом 10 робочих днів повідомляє суб'єкта

персональних даних, а також суб'єктів відносин, пов'язаних із персональними даними, яким ці дані було передано.

9.4 Обов'язкове зберігання всіх носіїв інформації, на яких зафіксовано взаємодію із споживачем, його близькими особами, представником, спадкоємцем, поручителем, майновим поручителем або третіми особами, взаємодія з якими передбачена договором про споживчий кредит та які надали згоду на таку взаємодію (у тому числі за допомогою технічних засобів), протягом трьох років після такої взаємодії.

10. «Припинення» обробки персональних даних

10.1 Якщо під час першої взаємодії колекторської компанії з такою третьою особою вона висловила заборону на здійснення обробки її персональних даних, колекторська компанія зобов'язана негайно припинити здійснення такої обробки.