Витяг із Політики конфіденційності, затвердженої Наказом ТОВ «СС ЛОУН» від 03.02.2021 р. № 0302-1

9. Захист персональних даних

Діяльність Товариства з обробки персональних даних в тому числі в інформаційних системах нерозривно пов'язана із захистом Товариством конфіденційності отриманої інформації, якщо це не суперечить чинному законодавству. Система захисту персональних даних включає в себе організаційні та (або) технічні заходи, визначені з урахуванням актуальних загроз безпеки персональних даних і інформаційних технологій, що використовуються в інформаційних системах. Товариство здійснює оновлення цих заходів з появою нових технологій в разі потреби.

Захист персональних даних передбачає заходи, спрямовані на запобігання їх випадкових втрати або знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

Організаційні заходи охоплюють:

- визначення порядку доступу до персональних даних працівників Товариства;
- визначення порядку ведення обліку операцій, пов’язаних з обробкою персональних даних суб’єкта та доступом до них;
- розробку плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;
- регулярне навчання співробітників, які працюють з персональними даними.

Товариство видає наказ, яким визначає коло працівників, які мають доступ до персональних даних суб'єктів та визначає рівень доступу зазначених працівників до персональних даних. Кожен із цих працівників користується доступом лише до тих персональних даних (їх частини) суб'єктів, які необхідні йому у зв'язку з виконанням своїх професійних чи службових або трудових обов'язків.

Усі інші працівники Товариства мають право на повну інформацію лише стосовно власних персональних даних.

Працівники, які мають доступ до персональних даних, дають письмове зобов'язання про нерозголошення персональних даних, які їм було довірено або які стали їм відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків.

Датою надання права доступу до персональних даних вважається дата надання зобов'язання відповідним працівником.

Датою позбавлення права доступу до персональних даних вважається дата звільнення працівника, дата переведення на посаду, виконання обов'язків на якій не пов'язане з обробкою персональних даних.

У разі звільнення працівника, який мав доступ до персональних даних, або переведення його на іншу посаду, що не передбачає роботу з персональними даними суб'єктів, вживаються заходи щодо унеможливлення доступу такої особи до персональних даних, а документи та інші носії, що містять персональні дані суб'єктів, передаються іншому працівнику.

Товариство веде облік операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них.

З цією метою Товариством 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.

Ця інформація зберігається Товариством упродовж одного року з моменту закінчення року, в якому було здійснено зазначені операції, якщо інше не передбачено законодавством України.

З метою забезпечення безпеки обробки персональних даних вживаються спеціальні технічні заходи захисту, у тому числі щодо виключення несанкціонованого доступу до персональних даних, що обробляються та роботі технічного та програмного комплексу, за допомогою якого здійснюється обробка персональних даних (Додаток 1). На випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій Товариством розроблено відповідний план дій працівників (Додаток 2).

Відповідальна особа організовує роботу, пов'язану із захистом персональних даних при їх обробці відповідно до законодавства. Відповідальна особа визначається наказом власника бази персональних даних.

Відповідальна особа виконує такі завдання:

- інформує та консультує працівників Товариства з питань додержання законодавства про захист персональних даних;
- взаємодіє з Уповноваженим Верховної Ради України з прав людини та визначеними ним посадовими особами його Секретаріату з питань запобігання та усунення порушень законодавства про захист персональних даних.

З метою виконання вказаних завдань відповідальна особа:

- забезпечує реалізацію прав суб'єктів персональних даних;

- користується доступом до будь-яких даних, які обробляються Товариством та до всіх приміщень Товариства, де здійснюється така обробка;

- у разі виявлення порушень законодавства про захист персональних даних та/або цієї Політики повідомляє про це директора Товариства з метою вжиття необхідних заходів;

- аналізує загрози безпеці персональних даних.

Обов'язками відповідального за організацію роботи, пов'язаної із обробкою та захистом персональних даних Товариства є:

- відповідальність за дотриманням законодавства України у сфері захисту персональних даних;

- захист персональних даних у базах персональних даних від незаконної обробки, а також від незаконного доступу до них;

- розробку, впровадження та забезпечення належного функціонування системи управління персональними даними;

- реєстрацію інцидентів в системі управління персональними даними.

Вимоги відповідальної особи до заходів щодо забезпечення безпеки обробки персональних даних є обов'язковими для всіх працівників, які здійснюють обробку персональних даних.

Факти порушень процесу обробки та захисту персональних даних повинні бути документально зафіксовані відповідальною особою, що організовує роботу, пов'язану із захистом персональних даних при їх обробці.

Політика конфіденційності стосовно захисту персональних даних при користуванні сайтом Товариства надана в Додатку 3.

Положення цієї Політики розповсюджуються на Політику конфіденційності стосовно захисту персональних даних при користуванні сайтом Товариства.

Додаток 1

ПРАВИЛА
користування послугами інформаційних технологій

ТОВ «СС ЛОУН», надалі – Товариство, в своїй діяльності активно використовує інформаційні технології (далі - ІТ). В інформаційних системах Товариства зберігається і обробляється інформація, віднесена до конфіденційної. Приватна власність, цілісність, постійна доступність такої інформації є обов'язковими умовами ефективної роботи Товариства, що накладає певні обмеження і обов'язки на працівників.

Відповідальними за забезпечення працівника телекомунікаційними засобами і забезпечення доступу працівника до них, є Відділ інформаційних технологій.

Кожна ІТ-послуга являє собою орієнтований на користувача інструмент, що забезпечує виконання працівником певного бізнес завдання. Для користування ІТ-послугами працівник забезпечується необхідними програмними і технічними засобами (далі - ІТ-ресурси) Товариства. До ІТ-ресурсів належать персональні комп'ютери, корпоративна мережа, файлові каталоги, інформаційні системи і програми, бази даних. Дотримання цих Правил сприяє ефективному виконанню працівниками функціональних обов'язків, забезпечення безпеки ІТ-ресурсів і підтримці високої репутації Товариства.

Дані Правила розглядають типове використання ІТ-ресурсів. Спеціальні питання можуть описуватися в додаткових регламенти та розпорядженнях, які також є обов'язковими для виконання.

1. Загальні положення

Відділ інформаційних технологій за заявкою, поданою працівником або його керівником, відповідно до встановлених в Товаристві правил, забезпечує працівника телекомунікаційними засобами (ІТ-ресурсами), необхідних для виконання ним своїх трудових обов'язків, і забезпечує доступ працівника до ІТ-ресурсів. ІТ-ресурси Товариства і дані, що в них знаходяться, є власністю Товариства. Окремі відомості підлягають захисту відповідно до законодавства України.

ІТ-ресурси Товариства надаються працівникам тільки для виконання ними бізнес завдань. Їх використання для вирішення інших завдань забороняється.

Забороняється працівникам:

- проводити несанкціоновані перевірки захисту систем і мережі, зокрема, шляхом обходу механізмів захисту, їх відключення або руйнування, а також будь-які спроби розтину паролів або інформації з управління доступом;

- навмисно піддавати системи будь-якому ризику, пов'язаному з порушенням їх працездатності, а також конфіденційності, цілісності та доступності інформації.

Товариство має право здійснювати обробку будь-яких повідомлень користувачів, спрямованих в процесі використання ІТ-ресурсів Товариства, в тому числі із застосуванням технічних засобів такої обробки. Отримана із застосуванням

технічних засобів інформація може служити підставою для проведення уповноваженими працівниками Товариства перевірок активності користувачів на предмет відповідності її цим Правилам. При цьому уповноважений працівник Товариства має право переглядати зміст будь-якого IT-ресурсу, в тому числі повідомлень електронної пошти та інших документів, спрямованих в процесі використання IT-ресурсів Товариства.

Товариство надає уповноваженому працівнику право проведення періодичних перевірок активності користувачів без їх повідомлення на предмет відповідності її цим Правилам, а також перегляду вмісту будь-якого IT-ресурсу, в тому числі повідомлень електронної пошти та інших документів. Використання працівниками засобів захисту інформації, що перешкоджають проведенню перевірок, заборонено. Діяльність працівників в даній сфері відносин регулюється Конституцією України, Кодексом законів про працю України, а також Кримінальним кодексом України, Кодексом України про адміністративні правопорушення та іншим застосовним Законодавством.

2. Захист конфіденційної інформації

Пароль є секретною персональною інформацією і не підлягає розголошенню. Працівник несе персональну відповідальність за збереження своїх паролів в таємниці від будь-яких інших осіб. Не рекомендується використовувати в паролі особисту інформацію або відомі фрази. Пароль повинен містити не менше 8 символів і змінюватися не рідше 1 разу на 3 місяці.

Забороняється працівникам:

- зберігати паролі в записаному вигляді, передавати свій пароль стороннім особам або використовувати паролі інших осіб. У разі компрометації або підозри на компрометацію пароля, він підлягає негайній зміні;

- розголошувати конфіденційну інформацію або вчиняти дії, які можуть привести до її розголошення;

- передавати інформацію обмеженого доступу будь-якими способами, в тому числі через Інтернет, по електронній пошті, флеш-носії або за допомогою комп'ютерних носіїв інформації (дискети, CD-ROM і ін.);

- допускати до роботи на комп'ютері сторонніх осіб і залишати включений комп'ютер без нагляду, не заблокувавши екран і клавіатуру.

3. Обладнання та програмне забезпечення (ПО)

Комп'ютерне та комунікаційне обладнання, надане працівникові Товариства, є власністю Товариства, і використовується працівником з метою ефективного виконання своїх трудових обов'язків. Працівник несе відповідальність за збереження цього обладнання в процесі використання його в своїй трудовій діяльності.

Склад ПО, встановленого на комп'ютері користувача, визначається IT Стандартами, уповноваженим підрозділом IT підтримки. Використання нестандартного ПО, в тому числі засобів захисту і операційних систем, має бути узгоджене з Відділом інформаційних технологій.

Забороняється працівникам:

- змінювати конфігурацію апаратних і програмних комп'ютерних засобів Товариства без узгодження з Відділом інформаційних технологій;

- переміщати і підключати стаціонарне обладнання без узгодження з Відділом інформаційних технологій;

- використовувати зовнішні накопичувачі в обхід узгоджених з Відділом інформаційних технологій. Зовнішні накопичувачі, що містять інформацію обмеженого доступу (дискети, CD диски, флеш-диски, знімні диски і т.ін.), а також документована інформація (паперові копії інформації, роздруківки) повинні зберігатися в місцях, що виключають доступ до них сторонніх осіб.

4. Електронна пошта та Інтернет

Електронна пошта призначена для обміну повідомленнями з внутрішніми адресатами Товариства. Слід регулярно очищати поштові скриньки від непотрібних повідомлень.

Забороняється працівникам:

- використання зовнішніх поштових серверів для розсилки з Товариства будь-якої інформації;

- зберігання та передача в Інтернет інформації з обмеженим доступом.

Товариство має право вводити обмеження на використання мережі Інтернет, наприклад, на з'єднання з певним протоколом, а також з певними вузлами, що не відносяться до службової діяльності або загрожують безпеці мережі. Товариство так само має право контролювати діяльність працівників в мережі Інтернет (обробляти Web-запити, або інформацію, що направляється в Інтернет за допомогою Web-форм) із застосуванням спеціальних програмно-технічних засобів для такої обробки.

5. Область застосування та відповідальність

Дані Правила стосуються всіх працівників - користувачів IT-послуг Товариства. Користувачам слід керуватися цими Правилами щодо всіх ресурсів, будь то ресурси корпоративної мережі або файли з інформацією, що належить Товариству, розташовані на особистому комп'ютері.

Порушення цих Правил може призвести до застосування дисциплінарних стягнень, звільнення і притягнення до кримінальної відповідальності за незаконні отримання та розголошення відомостей, що становлять комерційну або банківську таємницю, а також законодавства України, яким визначено заходи припинення неправомірного доступу до комп'ютерної інформації, створення, використання і поширення шкідливих програм для технічного обладнання.

Додаток 2

План
дій працівників Товариства на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій

1. При виявленні ознак несанкціонованого доступу до персональних даних суб'єктів Товариства таких як: несанкціоноване отримання логінів і паролів, підбір паролів та ключів, працівник, який виявив дані ознаки, зобов'язаний негайно:

- припинити обробку персональних даних;
- звернутися до адміністратора системи з метою блокування доступу до облікового запису;
- повідомити безпосереднього керівника та відповідальну особу, що організує роботу, пов'язану із захистом персональних даних при їхній обробці в Товаристві;
- змінити паролі доступу (за наявності технічної можливості);

2. При виявленні зараження програмного забезпечення та носіїв інформації комп'ютерними вірусами працівник зобов'язаний:

- негайно припинити обробку персональних даних;
- вимкнути комп'ютерну техніку від електроживлення;
- повідомити адміністратора системи;
- повідомити безпосереднього керівника та відповідальну особу.

3. При вчиненні випадкових та/або помилкових дій, що можуть призвести до втрати, зміни, поширення, розголошення персональних даних тощо, необхідно:

- припинити обробку персональних даних;
- про всі події та факти повідомити безпосереднього керівника та відповідальну особу.

4. При відмові та/або збої програмного забезпечення, за допомогою якого здійснюється обробка персональних даних, працівник зобов'язаний:

- припинити обробку персональних даних;
- повідомити адміністратора системи;
- повідомити безпосереднього керівника та відповідальну особу.

5. При виявленні пошкодження, втрати, викрадення документа або іншого носія персональних даних невідкладно повідомити безпосереднього керівника та відповідальну особу.

6. В разі виникнення надзвичайних ситуацій (пожежа, повінь, стихійні лиха тощо):

- вжити невідкладних заходів щодо оповіщення відповідних служб реагування;

- забезпечити збереження носіїв персональних даних осіб від втрати та пошкодження (за наявної можливості та у спосіб, що не загрожує життю та здоров'ю працівників);

- повідомити безпосереднього керівника та відповідальну особу.

7. Про всі випадки несанкціонованого доступу до персональних даних, передбачені пунктами 1-6 даного Плану, та/або інші випадки, що призвели до пошкодження, псування, несанкціонованого доступу, знищення, поширення тощо персональних даних, працівник, який виявив даний факт, та керівник відповідного підрозділу невідкладно письмово повідомляють про подію відповідальну особу.

8. Після отримання повідомлення відповідальна особа складає Акт про факт порушення процесу обробки та захисту персональних даних (далі – Акт).

Акт підписується відповідальною особою та працівником, яким виявлено (вчинено) дане порушення. Відмова від підпису працівника фіксується відповідно до вимог чинного законодавства.

Вимоги відповідальної особи до заходів щодо забезпечення безпеки обробки персональних даних є обов'язковими для всіх працівників, які здійснюють обробку персональних даних.

9. Підписаний Акт надається директору Товариства або, в разі його відсутності, – посадовій особі, на яку покладено виконання його повноважень для прийняття рішення про проведення службового розслідування, повідомлення правоохоронних органів про несанкціонований доступ до персональних даних та вжиття відповідних заходів реагування.

Додаток 3

Політика конфіденційності
стосовно захисту персональних даних при користуванні сайтом
ТОВ « СС ЛОУН»

1. Загальні положення

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «СС ЛОУН» код ЄДРПОУ – 40071779, місцезнаходження: 03066, м. Київ, Глосіївський район, вулиця Михайла Максимовича, будинок 8 (надалі по тексту – Товарство) цією Політикою конфіденційності (надалі по тексту – «Політика») встановлює принципи отримання персональних даних Користувачів сайту www.ccloan.ua (надалі по тексту – «Сайт»), а також види персональних даних, які збираються, використовуються, обробляються та захищаються Товариством.

Ця Політика діє відносно всієї інформації, яку Товариство може отримати про Користувачів під час використання ними Сайту. Використання Сайту, так само як і заповнення реєстраційних форм Сайту, створення облікового запису на Сайті, означає беззастережну згоду Користувача з цією Політикою і зазначеними в ній умовами збору і обробки персональних даних. В разі незгоди з цими умовами Користувач повинен утриматися від використання Сайту.

Товариство зберігає за собою право вносити зміни до цієї Політики в будь-який час та з будьякої причини.

Сайт Товариства призначений для користування виключно повнолітніми особами.

2. Визначення термінів

2.1. У цій Політиці використовуються такі терміни:

2.1.1. Адреса інтернет-протоколу (IP-адреса) - комбінація цифр, що автоматично надається комп’ютеру Користувача під час інтернет-сесії, коли він підключається до свого інтернетпровайдера через локальну мережу.

2.1.2. Інтернет-браузер - програмне забезпечення для комп'ютера або іншого електронного пристрою під'єднаного до Інтернету, що дає можливість Користувачеві взаємодіяти з текстом, малюнками або іншою інформацією на Сайті.

2.1.3. Користувач сайту - особа, яка має доступ до Сайту, за допомогою мережі Інтернет та використовує Сайт.

2.1.4. Кредитний договір – Договір про надання споживчого кредиту/Договір надання коштів у позику, в тому числі і на умовах фінансового кредиту, укладений між Товариством та Позичальником, в якому визначені основні умови, права та обов’язки Сторін щодо отримання та повернення Кредиту.

2.1.5. Особистий кабінет – частина Сайту, доступ до якої отримує Позичальник за умови реєстрації з використанням Логіну та Пароля Особистого кабінету. Доступ

до Особистого кабінету здійснюється Позичальником шляхом введення Логіна Особистого кабінету і Пароля Особистого кабінету на Сайті.

2.1.6. Позичальник – фізична особа, яка має намір укласти з Товариством Кредитний договір.

2.1.7. Сайт - www.ccloan.ua.

2.1.8. Cookie – текстовий файл невеликого розміру, що зберігається на жорстких дисках користувачів сервером Сайту.

3. Особливості інформації, яка обробляється

3.1. Товариство отримує знеособлену загальну інформацію за результатами підрахунку таких даних, як: загальна кількість відвідувань Сайту, час відгуку сторінки Сайту, помилки під час завантаження, тривалість перебування на певних сторінках та кількість відвідувань кожної сторінки Сайту, історію переходу з Сайту на інші веб-сайти (включаючи дату та час) тощо. Ця інформація використовується виключно з метою оцінки рейтингу Сайту, подальшого покращення його роботи та вдосконалення процесу надання фінансових послуг.

3.2. Товариство здійснює збір та обробку наступних даних Користувачів під час користування ними Сайтом:

3.2.1. даних, що надаються Користувачам як при заповненні реєстраційних форм Сайту, так і в процесі користування Сайтом;

3.2.2. файли cookie;

3.2.3. IP-адреси;

3.2.4. параметри та налаштування інтернет-браузерів.

3.3. Товариство включає дані Користувача до бази персональних даних інтернет користувачівз моменту, коли він уперше починає користуватися Сайтом, а також постійно увесь період, протягом якого користується послугами Товариства. Строк зберігання даних становить період, протягом якого Користувач користується послугами Товариства, а також п'ять наступних років після закриття аккаунту (Особистого кабінету) на Сайті та завершення користування послугами Товариства.

3.4. Товариство здійснює обробку персональних даних Користувача з метою належного надання Користувачу послуг (ідентифікація, аутентифікація, авторизація, відновлення паролю, надсилання інформаційних матеріалів за підпискою Користувача, відповідей на запити та листи Користувача, а також для інших дій, в яких з’являється необхідність для належного надання послуг).

3.5. Товариство використовує знеособлені дані для таргетингу рекламних та/або інформаційних матеріалів за віком, статтю, іншими даними; для проведення статистичних досліджень; будь-якими іншими способами.

3.6. Товариство має право передати персональні дані, базу персональних даних, до якої включені персональні дані Користувача, повністю або частково третім особам без повідомлення про це Користувачеві у наступних випадках: особам, у ведення, володіння або власність яких передано Сайт; особам, що є пов’язаними/афілійованими з Товариством; новому власнику Товариства для оброблення з метою, передбаченою цією Політикою; іншим користувачам Сайту (як

фізичним, так і юридичним особам), якщо на Сайті передбачено відповідний функціонал.

3.7. Під час користування Сайтом на його інтернет-сторінках можуть бути присутні коди інтернет-ресурсів третіх осіб, у результаті чого такі треті особи отримують дані, зазначені у пунктах 2.2, 2.3 та 2.4 цієї Політики. Такими інтернет-ресурсами третіх осіб є:

3.7.1. системи зі збору статистики відвідувань Сервісів (наприклад, лічильники LiveInternet, Google Analytics тощо);

3.7.2. соціальні-плагіни (блоки) соціальних мереж (наприклад, Facebook тощо);
3.7.3. системи банеропоказів (наприклад, AdRiver тощо);

3.7.4. інші ресурси.

3.8. Виключно з метою покращення функціонування Сайту Товариства може використовувати сервіси третіх осіб, які додатково дозволяють здійснювати збір та обробку наступних даних Користувачів під час користування ними Сайтом:

3.8.1. роздільна здатність екрану пристрою Користувача;

3.8.2. тип пристрою, операційної системи, інтернет-браузера Користувача;

3.8.3. геолокація Користувача (виключно країна);

3.8.4. мова відображення Сайту;

3.8.5. переміщення, кліки миші;

3.8.6. натискання клавіш клавіатури пристрою Користувача;

3.8.7. відвідувані сторінки Сайту, час та дата відвідування сторінок Сайту;

3.8.8. URL-адреса, домен. Зазначені дані не є персональними даними в розумінні Закону України «Про захист персональних даних».

4. Права Користувача

4.1. Користувач має усі права щодо захисту його персональних даних, які передбачено чинним законодавством України, зокрема, Законом України «Про захист персональних даних».

4.2. Оброблення персональних даних здійснюється у дата-центрах, де розміщується обладнання, що забезпечує функціонування Сайту. Товариство вживає всіх передбачених законодавством заходів для захисту персональних даних Користувача. Зокрема, оброблення даних здійснюється на обладнанні, розміщеному в захищених приміщеннях із обмеженим доступом.

5. Використання IP-адреси

5.1. Товариство та/або треті особи, що технічно обслуговують Сайт, можуть збирати IPадреси з метою системного адміністрування та аудиту використання Сайту. Товариство може використовувати IP-адресу для ідентифікації Користувачів Сайту у випадку, коли це необхідно для захисту процесу надання послуг, самого Сайту або інших Користувачів.

5.2. Фактом відвідання Сайту Користувач надає Товариству та/або третім особам, що технічно обслуговують Сайт, свою згоду на збирання та використання IPадреси з метою, зазначеною у цьому розділі.

6. Файли Cookie

6.1. У роботі Сайту використовується технологія Cookies.

6.2. Файли Cookie додають функціональності Сайту або допомагають ефективніше та чіткіше аналізувати використання Сайту. Наприклад, сервер може використовувати cookie для того щоб Користувачу не потрібно було вводити пароль (у випадках, коли це необхідно) більше ніж один раз, відвідуючи Сайт.

6.3. Фактом відвідання Сайту Користувач надає Товариству та третім особам, що технічно обслуговують Сайт, свою згоду на збирання, оброблення та використання даних у межах використання технології Cookies.

6.4. При цьому у Користувача є можливість обрати: використовувати технологію cookies або відмовитися від цього. Більшість інтернет-браузерів автоматично приймають cookies, але Користувач може змінити налаштування свого браузера та відмовитися від цієї технології. Детальнішу інформацію про такі можливості можна отримати, звернувшись до інструкції з використання інтернет-браузера.

7. Посилання на інші веб-сайти

7.1. Сайт Товариства може містити посилання на інші сайти, створені третіми сторонами, політика щодо захисту персональних даних та інформації яких відрізняється від Товариства щодо захисту конфіденційності, яка застосовується такими третіми сторонами.

7.2. Рекомендуємо ознайомитися з положенням про конфіденційність усіх сайтів третіх сторін, перш ніж використовувати такі сайти або надавати свої персональні дані чи будь-якуіншу інформацію таким сайтам або через них.

8. Інші умови

8.1. Ця Політика набирає чинності з моменту її публікації на Сайтіта діє до моменту внесення змін та/або доповнень до неї чи її викладення у новій редакції.

8.2. Товариство залишає за собою право у будь-який час внести зміни до цієї Політики, які набудуть чинності одразу після розміщення на Сайті.

8.3. Товариство рекомендує регулярно переглядати цю Політику.

8.4. Користувачі мають права згідно з чинним законодавством, що передбачають доступ до персональних даних, які опрацьовуються, право виправити, стерти або заблокувати такі персональні дані, а також право заборонити певні дії стосовно опрацювання цих даних. Дляреалізації таких прав слід направити письмовий запит, використовуючи наші контактні дані, вказані на Сайті.