ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «АЙ ЛОМБАРД»
(ТОВ «АЙ ЛОМБАРД»)

Код ЄДРПОУ 44916262

НАКАЗ

Київ

03.07.2023 № 13-0723 ЗП

Про затвердження Положення
про захист персональних даних

На виконання вимог Закону України «Про захист персональних даних», Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14,

НАКАЗУЮ:

1. Затвердити «Положення про захист персональних даних» у новій редакції, далі — Положення (додається).
2. Юридичному відділу Товариства забезпечити розсилку даного наказу у встановленому порядку.
3. Всім працівникам Товариства, ознайомитись з Положенням, затвердженим даним наказом та дотримуватись його вимог.
4. Відділу кадрів Товариства забезпечити підписання всіма працівниками, які мають доступ до персональних даних письмового зобов'язання про нерозголошення (за формою, згідно додатку 3 до Положення, затвердженого даним наказом).
5. Контроль за виконанням цього наказу залишаю за собою.
6. Наказ набирає чинності 03.07.2023.

Директор
ТОВ «Ай Ломбард» **Дмитро МОРОЗОВ**

ЗАТВЕРДЖЕНО
наказом директора
від 03.07.2023 № 03-0723 ЗП

ВИТЯГ З
ПОЛОЖЕННЯ
ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

ІІ. ПЕРСОНАЛЬНІ ДАНІ КЛІЄНТІВ ТОВАРИСТВА

1. Склад персональних даних клієнтів Товариства

1.1. На виконання вимог законодавства, в Товаристві функціонує обліково-реєструюча система, яка забезпечує облік споживачів послуг Товариства та здійснює реєстрацію їх операцій.

1.2. Персональні дані клієнта є сукупністю інформації про фізичну особу, що відповідно до чинного законодавства є необхідною для надання відповідних послуг та інформації про послуги, які клієнт отримував в Товаристві.

1.3. До складу персональних даних клієнтів, що зберігаються в реєстраційно-обліковій системі, входять:

1.3.1. інформація про особу:
- прізвище, ім'я, по батькові фізичної особи;
- дані паспорта (номер, серія, дата видачі, орган, що видав) або іншого документа, що посвідчує особу;
- місце проживання фізичної особи;
- контактний телефон (за умови надання клієнтом);
- РНОКПП (за умови надання клієнтом);

1.3.2. інформація про послуги, які клієнт отримував в Товаристві:
- дати та номери договорів;
- строки дії договорів;
- дати закінчення дії договорів;
- короткий опис предметів застави, що надавались клієнтом в якості забезпечення застави;
- дати надання послуг;
- вид послуг;
- суми послуг;
- дати звернення стягнення на предмети застави;
- суми до повернення Товариству;
- заборгованість за договорами.

2. Обробка персональних даних клієнтів

2.1. Під обробкою персональних даних клієнтів розуміється збирання, реєстрація зберігання, адаптування, зміна, поновлення, використання, поширення, передача, використання та будь-які інші дії Товариства.

2.2. Дотримання прав та свобод клієнта в частині захисту його персональних даних, забезпечується Товариством шляхом організації роботи з дотриманням наступних принципів:

2.2.1. Обробка персональних даних клієнтів Товариства здійснюється виключно з метою реалізації відносин у сфері надання фінансових послуг, обліку споживачів послуг Товариства та реєстрації їх операцій, а також реалізації відносин у сфері надання рекламно-інформаційних послуг.

2.2.2. Отримання персональних даних здійснюється шляхом надання клієнтом необхідної інформації та первинних документів при укладенні відповідних договорів.

2.3. До обробки, передачі та зберігання персональних даних клієнтів Товариства можуть мати доступ:
- оцінювачі-експерти Товариства та їх безпосередні керівники (керуючі /завідувачі відділенням), які належним чином пройшли навчання питанням здійснення фінансового моніторингу, ознайомлені із законодавством з питань фінансового моніторингу, внутрішньою Програмою та Правилами здійснення фінансового моніторингу в Товаристві та списком терористів;
- безпосередні керівники відокремлених підрозділів (керуючі / завідуючі), зокрема з метою отримання контактної інформації клієнта для його інформування про акційні пропозиції та реалізації відносин у сфері надання рекламних послуг;
- співробітники відділу інформаційно-технічного забезпечення (виключно з метою забезпечення належного функціонування обліково-реєструючої системи ломбарду, її захисту від несанкціонованого доступу та унеможливлення будь-яких змін щодо даних, зафіксованих після здійснення операцій);
- співробітники юридичної відділу Товариства (виключно для отримання інформації необхідної для надання відповіді на законні запити уповноважених на те державних органів або письмові запити особисто клієнта чи належним чином уповноважених клієнтом осіб);
- працівники контрольно-ревізійної відділу Товариства, в межах, що необхідні для проведення внутрішніх перевірок фінансово-господарської діяльності Товариства та/або відокремлених підрозділів Товариства;
- дирекція та інші працівники Товариства, в межах наданих їм повноважень.

2.4. Внесення персональних даних клієнта та реєстрація його операцій здійснюється виключно належним чином уповноваженою особою (оцінювач — експерт) в момент реєстрації відповідної операції. Інформація про уповноважену особу, яка здійснила реєстрацію відповідної операції в обов'язковому порядку фіксується в реєстраційно-обліковій системі.

2.5. Згода клієнта на включення його персональних даних до бази обліково-реєструючої системи отримується в письмовому вигляді, шляхом підписання клієнтом відповідних договорів, в яких зазначається згода клієнта на такі дії. Відмова клієнта від надання персональних даних є беззаперечною та достатньою підставою для відмови в наданні йому відповідних послуг.

2.6. Під час внесення персональних даних особи до бази обліково-реєструючої системи, уповноважена особа зобов'язана в повній мірі відобразити інформацію про особу (п. 1.3.1. цього Положення), яка отримується з наданих клієнтом оригіналів документів та має точно відповідати інформації, наведеній у таких документах.

2.7. Уточнення персональних даних особи, які внесено до обліково-реєструючої системи, можливе виключно на прохання клієнта при оформленні чергової операції та за обов'язкової умови надання оригіналів документів, що підтверджують необхідність таких уточнень.

2.8. Програмне забезпечення обліково-реєструючої системи унеможливлює внесення будь-яких змін щодо даних, зафіксованих після здійснення операцій, будь-ким із працівників Товариства так само, як і будь-якою третьою особою.

3. Передача персональних даних клієнтів

3.1. Використання персональних даних можливе виключно у відповідності з цілями, що визначають мету їх отримання.

3.2. Передача персональних даних можлива за умови отримання згоди клієнта або у випадках, прямо передбачених законодавством та здійснюється виключно після перевірки дотримання порядку та правил передачі персональних даних працівником юридичного відділу.

3.3. При передачі персональних даних клієнтів Товариства необхідно дотримуватись наступних вимог:

3.3.1. Передача персональних даних клієнтів без належних правових підстав категорично заборонена;

3.3.2. Передача клієнту його персональних даних можлива виключно в письмовому вигляді за умови письмового клопотання клієнта / уповноваженої особи, в якому має бути зазначено об'єм інформації, яку має намір отримати клієнт та адресу, на яку таку інформацію можна надіслати (при цьому до клопотання обов'язково має бути додано завірену підписом клієнта копію паспорта зі зразком його підпису), або клопотання про отримання такої інформації навмисно.

3.3.3. Третя особа, має право на отримання інформації про клієнта, виключно за умови пред'явлення письмового доручення про це, засвідченого у встановленому законодавством порядку, в якому має бути зазначено об'єм інформації, згоду на передачу якої третій особі надає клієнт, вичерпна інформація про уповноважену особу, що надає можливість її ідентифікувати, а також в інших випадках, передбачених законодавством.

3.3.4. Передача персональних даних клієнта представникам державних органів може здійснюватися виключно у випадках, передбачених чинним законодавством.

3.3.5. Будь-яка передача персональних даних клієнта без погодження таких дій з юридичним відділом Товариства категорично заборонена та у випадку вчинення таких дій кваліфікується як грубе порушення трудової дисципліни.

4. Доступ до персональних даних клієнтів

4.1. Внутрішній доступ (в межах Товариства):

4.1.1. Право доступу до персональних даних, що містяться в реєстраційно-обліковій системі, в межах Товариства мають виключно:

- оцінювачі-експерти та їх безпосередні керівники (керуючі / завідуючі), в межах, що необхідні для реєстрації відповідних операцій;
- безпосередні керівники, в межах, що необхідні для реалізації відносин в галузі надання рекламно інформаційних послуг;
- працівники відділу забезпечення інформаційної безпеки (в межах, що необхідні для забезпечення належного функціонування та захисту обліково-реєструючої системи ломбарду);
- працівники контрольно-ревізійного відділу Товариства, в межах, що необхідні для проведення внутрішніх перевірок фінансово-господарської діяльності Товариства та/або відокремлених підрозділів;
- працівники юридичного відділу, в межах, що необхідні для перевірки інформації та надання відповіді на письмові запити клієнта чи уповноважених ним осіб, а також на обґрунтовані запити державних органів, що видаються на підставі закону;
- дирекція та інші працівники Товариства, в межах наданих їм повноважень.

4.1.2. Працівники Товариства мають право на доступ до персональних даних клієнтів та наданих їм послуг, виключно у випадках та в межах, що необхідні для виконання ними своїх посадових обов'язків.

4.1.3. Контроль внутрішнього доступу до обліково-реєструючої системи здійснюється за допомогою відповідного програмного забезпечення, яке унеможливлює доступ до неї без введення персонального паролю та/або сканування унікального персонального штрихкоду.

4.1.4. Працівникам Товариства категорично заборонено розголошувати їх пароль та/або передавати видане їм службове посвідчення з унікальним персональним штрихкодом.

4.1.5. Після ідентифікації працівника Товариства (введення паролю або сканування унікального персонального штрихкоду) програмне забезпечення надає йому можливість роботи з реєстраційно обліковою системою виключно в тих межах, що необхідні йому для виконання своїх функціональних обов'язків.

4.2. Зовнішній доступ.

4.2.1. До числа установ, що відповідно до закону можуть вимагати отримання персональних даних клієнта без його згоди, відносяться відповідні державні органи, згідно чинного законодавства.

4.2.2. Державні органи мають право на отримання персональних даних клієнтів виключно на підставі закону та в межах, що необхідні для виконання покладених на них зобов'язань.

4.2.3. Відповідь на запит державних органів готується виключно працівником юридичного відділу, який при надходженні запиту перевіряє законність його видання та правильність оформлення.

4.2.4. Неналежним чином оформлений або незаконний запит державного органу підлягає обов'язковому відхиленню.

4.3. Недержавні установи мають право на отримання персональних даних клієнтів виключно у випадку наявності письмової згоди клієнта на передачу інформації таким установам.

4.4. Треті особи мають право на отримання персональних даних клієнта, виключно за умови наявності письмового доручення клієнта на передачу такої інформації з дотриманням вимог, встановлених пунктом 3.3.3. цього розділу Положення, а також в інших випадках, передбачених законодавством.

5. Захист персональних даних клієнтів

5.1. Під загрозою або небезпекою втрати персональних даних мається на увазі одинична або комплексна, реальна або потенційна, активна або пасивна поява злочинних можливостей для зовнішніх або внутрішніх джерел загрози створювати несприятливі події, вчиняти дестабілізуючий вплив на інформацію, що захищається.

5.2. Ризик загрози будь-яким інформаційним ресурсам створюють стихійні лиха, екстремальні ситуації, терористичні дії, аварії технічних засобів та ліній зв'язку, інші об'єктивні обставини, а також зацікавлені та незацікавлені у виникненні загрози особи.

5.3. Захист персональних даних є регламентованим технологічним процесом, що попереджає порушення доступності, цілісності, достовірності та конфіденційності персональних даних, що окрім іншого забезпечується резервним копіюванням бази персональних даних.

5.4. Внутрішній захист.

5.4.1. З метою захисту персональних даних клієнтів в Товаристві регламентовано доступ до бази персональних даних та встановлено правила обробки та передачі такої інформації.

5.4.2. Захист персональних даних клієнтів від несанкціонованої обробки та передачі забезпечується шляхом:

- встановлення переліку осіб, що мають доступ до бази;
- контрольованого доступу до бази та унеможливлення доступу до неї без ідентифікації уповноваженого працівника (введення паролю або сканування унікального персонального штрихкоду);
- обмеження кола осіб, які мають доступ до бази;
- включення до переліку осіб, що мають право доступу до бази, виключно тих працівників, посадові обов'язки яких містять зобов'язання щодо реєстрації, обробки та передачі персональних даних та забезпечення функціонування обліково-реєструючої системи;
- максимального звуження повноважень по роботі з базою, що обмежується виключно тими функціями, які необхідні уповноваженим працівникам для виконання своїх посадових обов'язків;
- раціонального розташування робочих місць працівників, що працюють з базою персональних даних, при якому унеможливлюється несанкціонований доступ до захищеної інформації;
- ознайомлення працівників з вимогами внутрішніх нормативних документів, які містять зобов'язання щодо захисту баз персональних даних, зокрема з цим Положенням;
- обмеження доступу сторонніх осіб та працівників Товариства, що не мають доступу до бази персональних даних клієнтів Товариства, до робочого місця працівника з якого існує можливість ознайомитись з персональними даними;
- поточного внутрішнього контролю за дотриманням уповноваженими працівниками вимог цього Положення;
- постійної інформаційно-роз'яснювальної роботи з працівниками, щодо вимог законодавства в частині захисту персональних даних.

5.5. Зовнішній захист.

5.5.1. Захист бази персональних даних клієнтів від знищення, несанкціонованої обробки чи пошкодження забезпечується шляхом її резервного копіювання;

5.5.2. Захист бази персональних даних від несанкціонованого проникнення в реєстраційно-облікову систему забезпечується сучасними та ефективними програмно-технічними комплексами, персональну відповідальність за впровадження та належне функціонування яких несе відповідальна особа відділу інформаційно-технічного забезпечення, призначена окремим розпорядженням директора Товариства.

5.5.3. При формуванні статистичних або звітних відомостей персональні дані, у випадку можливості, знеособлюються.

6. Права та обов'язки клієнта

6.1. Клієнт має право:
- знати про місцезнаходження бази персональних даних, яка містить його персональні дані, її призначення та найменування, місцезнаходження та/або місце проживання (перебування) володільця чи розпорядника цієї бази або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;
- отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані, що містяться у відповідній базі персональних даних;
- на доступ до своїх персональних даних, що містяться у відповідній базі персональних даних;
- отримувати не пізніш як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи зберігаються його персональні дані у відповідній базі персональних даних, а також отримувати зміст його персональних даних, які зберігаються;
- пред'являти вмотивовану вимогу із запереченням проти обробки своїх персональних даних органами державної влади, органами місцевого самоврядування при здійсненні їхніх повноважень, передбачених законом;
- пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником цієї бази, якщо ці дані обробляються незаконно чи є недостовірними;
- на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;
- звертатися з питань захисту своїх прав щодо персональних даних до органів державної влади, органів місцевого самоврядування, до повноважень яких належить здійснення захисту персональних даних;
- застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних.

6.2. Клієнт зобов’язаний:
- своєчасно та в повному об’ємі надавати достовірну інформацію, яка є необхідною для укладення відповідних договорів;
- повідомляти Товариство про зміну своїх персональних даних та надавати відповідні підтверджуючі документи з метою належного їх відображення в базі.

7. Відповідальність за незаконне використання, знищення, розповсюдження, зміну персональних даних

7.1. Використання персональних даних працівниками Товариства, пов'язаних з персональними даними клієнтів Товариства, повинно здійснюватися виключно відповідно до їхніх посадових обов’язків та мети збору й обробки.

7.2. Працівники, посадовими обов’язками яких передбачено доступ до бази персональних даних клієнтів Товариства, зобов'язані не допускати незаконне використання, знищення, розповсюдження, розголошення, зміну у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням посадових обов'язків. Таке зобов'язання чинне після припинення ними діяльності, пов'язаної з персональними даними, крім випадків, установлених законом.

7.3. Порушення Порядку захисту персональних даних клієнтів Товариства, є грубим порушенням трудової дисципліни, за вчинення якого винного працівника може бути притягнуто до дисциплінарної чи адміністративної відповідальності, а у випадку якщо в таких діях міститься склад злочину — до кримінальної відповідальності, встановленої законодавством.

7.4. Кожен працівник, який має доступ до бази персональних даних несе персональну відповідальність за дотримання порядку внесення, обробки та збереження персональних даних, а також за дотримання порядку їх передачі.

7.5. Відповідальна особа Департаменту інформаційно-технічного та комп'ютерного забезпечення несе персональну відповідальність за забезпечення функціонування системи контрольованого доступу до обліково-реєструючої системи, належний захист обліково-реєструючої системи від несанкціонованого доступу як третіх осіб, так і не уповноважених на те працівників Товариства, та належне її резервне копіювання.

7.6. Передача персональних даних здійснюється виключно після перевірки дотримання Порядку та правил передачі персональних даних, працівником юридичного відділу Товариства, та отримання його дозволу на таку передачу.