Витяг із Політики конфіденційності, затвердженої Наказом

ТОВ «МУЛЬТІКРЕДИТ» від 01.02.2022 р. № 0102-1

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.