ВИТЯГ

З ПОРЯДКУ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ У КРЕДИТНІЙ СПІЛЦІ «ТАЙСТРА»

5.8. Захист персональних даних

5.8.1. Кредитна спілка, як володілець персональних даних вживає заходи щодо забезпечення захисту персональних даних на всіх етапах їх обробки, у тому числі за допомогою організаційних та технічних заходів.

5.8.2. Володілець персональних даних самостійно визначає перелік і склад заходів, спрямованих на безпеку обробки персональних даних, з урахуванням вимог законодавства у сферах захисту персональних даних, інформаційної безпеки.

5.8.3. 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.

5.8.4. Організаційні заходи охоплюють:

– визначення порядку доступу до персональних даних працівників володільця;

– 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.

5.8.5. Володілець веде облік працівників, які мають доступ до персональних даних суб’єктів.

Володілець визначає рівень доступу зазначених працівників до персональних даних суб’єктів.

Доступ до автоматизованої системи (комплексної інформаційної системи) здійснюється в порядку передбаченому Регламентом доступу до комплексної інформаційної системи затвердженим наказом голови правління та лише тими працівниками, які включено до списку осіб, що мають доступ до комплексної інформаційної системи.

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.

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

5.8.7. 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.

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

5.8.9. 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.

5.8.10. 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.

5.8.11. Володілець веде облік операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них. З цією метою володільцем 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.

При оброці персональних даних суб'єктів за допомогою автоматизованої системи така система автоматично фіксує вказану інформацію. Ця інформація зберігається володільцем упродовж одного року з моменту закінчення року, в якому було здійснено зазначені операції, якщо інше не передбачено законодавством України.

Кредитна спілка зберігає інформації про операції, пов'язані з обробкою персональних даних суб'єкта та доступом до них в порядку передбаченому внутрішніми положеннями кредитної спілки для збереження інформації з обмеженим доступом.

При оброці персональних даних суб'єктів за допомогою не автоматизованої системи, облік операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них ведеться у Реєстрі обліку операцій, пов'язаних з обробкою персональних даних у кредитній спілці «Тайстра» та доступом до них.

5.8.12. Персональні дані залежно від способу їх зберігання (паперові, електронні носії) мають оброблятися у такий спосіб, щоб унеможливити доступ до них сторонніх осіб.

5.8.13. 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.

Картотеки зберігаються у приміщеннях (шафах, сейфах), захищених від несанкціонованого доступу. Двері у приміщеннях (шафах, сейфах) повинні бути обладнані замком або контролем доступу.

Приміщення, де стоять комп'ютери, на яких здійснюється обробка персональних даних, замикаються. Для отримання ключа необхідно поставити відмітку в журналі.

Комп'ютери, де містяться персональні дані, захищені паролем. Кожен працівник має особистий пароль.

5.8.14. У КС визначається відповідальна особа, яка організовує роботу, пов'язану із захистом персональних даних при їх обробці.

5.8.15. Факти порушень процесу обробки та захисту персональних даних повинні бути документально зафіксовані відповідальною особою.

Про факт порушення відповідальна особа складає Акт про порушення процесу обробки та захисту персональних даних.

5.8.16 Кредитною спілкою розроблено план дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій.

5.8.17. Всі співробітники кредитної спілки, які працюють з персональними даними проходять регулярне навчання згідно Програми навчання співробітників (працівників та членів органів управління) кредитної спілки «Тайстра», які працюють з персональними даними…