Витяг з Порядку
обробки персональних даних
у базах персональних даних кредитної спілки «Партнер»

3. Захист персональних даних

3.1. Володілець, розпорядник персональних даних вживають заходів щодо забезпечення захисту персональних даних на всіх етапах їх обробки, у тому числі за допомогою організаційних та технічних заходів.
3.2. Володілець, розпорядник персональних даних самостійно визначають перелік і склад заходів, спрямованих на безпеку обробки персональних даних, з урахуванням вимог законодавства у сферах захисту персональних даних, інформаційної безпеки.
3.3. 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.
3.4. Організаційні заходи охоплюють:
– визначення порядку доступу до персональних даних працівників володільця/розпорядника;
– 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.
3.5. Володілець/розпорядник веде облік працівників, які мають доступ до персональних даних суб'єктів. Володілець/розпорядник визначає рівень доступу зазначених працівників до персональних даних суб'єктів. 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.
3.6. Усі інші працівники володільця/розпорядника мають право на повну інформацію лише стосовно власних персональних даних.
3.7. Працівники, які мають доступ до персональних даних, дають письмове зобов'язання про нерозголошення персональних даних та іншої конфіденційної інформації, якіїм були довірені або які стали їм відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків.
3.8. Датою надання права доступу до персональних даних вважається дата надання зобов'язання відповідним працівником.
3.9. 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.
3.10. 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.
3.11. Володілець/розпорядник веде облік операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них. З цією метою володільцем/розпорядником 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.
Володілець/розпорядник персональних даних самостійно визначає процедуру збереження інформації про операції, пов'язані з обробкою персональних даних суб'єкта та доступом до них. У випадку обробки персональних даних суб'єктів за допомогою автоматизованої системи така система автоматично фіксує вказану інформацію. Ця інформація зберігається

володільцем/розпорядником упродовж одного року з моменту закінчення року, в якому було здійснено зазначені операції, якщо інше не передбачено законодавством України.
3.12 Вимоги щодо обліку та збереження інформації про перегляд персональних даних не поширюється на володільців/розпорядників, які здійснюють обробку персональних даних в реєстрі, який є відкритим для населення в цілому.
3.13. Персональні дані залежно від способу їх зберігання (паперові, електронні носії) мають оброблятися у такий спосіб, щоб унеможливити доступ до них сторонніх осіб.
3.14. 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.
3.15. В органах державної влади, органах місцевого самоврядування, а також у володільців чи розпорядників персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до Закону, створюється (визначається) структурний підрозділ або відповідальна особа, яка організовує роботу, пов'язану із захистом персональних даних при їх обробці.
3.16. Інформація про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, повідомляється Уповноваженому Верховної Ради України з прав людини відповідно до Закону.
3.17. Відповідальна особа/структурний підрозділ виконує такі завдання:
– інформує та консультує володільця або розпорядника персональних даних 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.
3.18. З метою виконання вказаних завдань відповідальна особа/структурний підрозділ:
– забезпечує реалізацію прав суб'єктів персональних даних;
– користується доступом до будь-яких даних, які обробляються володільцем/розпорядником та до всіх приміщень володільця/розпорядника, де здійснюється така обробка;
– у разі виявлення порушень законодавства про захист персональних даних та/або Порядку повідомляє про це керівника володільця/розпорядника з метою вжиття необхідних заходів;
– аналізує загрози безпеці персональних даних.
3.19. Вимоги відповідальної особи до заходів щодо забезпечення безпеки обробки персональних даних є обов'язковими для всіх працівників, які здійснюють обробку персональних даних.
3.20. Факти порушень процесу обробки та захисту персональних даних повинні бути документально зафіксовані відповідальною особою або структурним підрозділом, що організовує роботу, пов'язану із захистом персональних даних при їх обробці.
3.21. Взаємодія з Уповноваженим Верховної Ради України з прав людини здійснюється в порядку, визначеному Законом та Законом України «Про Уповноваженого Верховної Ради України з прав людини».
3.22. Організація роботи, пов'язаної із захистом персональних даних при їх обробці, тих володільців/розпорядників, на яких не поширюються вимоги частини другої статті 24 Закону, покладається безпосередньо на тих осіб, які здійснюють обробку персональних даних, або, у разі необхідності, – на окремі структурні підрозділи чи посадових осіб.

Голова правління кредитної спілки «Партнер» _____ / Герасимук М.В. /