АТ «СЕБ КОРПОРАТИВНИЙ БАНК»

Витяг з Порядку обробки АТ «СЕБ КОРПОРАТИВНИЙ БАНК» персональних даних у базах персональних даних	Дата версії 14.11.2023	Статус документа	Класифікація
	Чинний з: 20.11.2023 року	Затверджено Рішенням Правління №54.2 від 20.11.2023 року	Відкритий/1

ВИТЯГ з

ПОРЯДКУ ОБРОБКИ АТ «СЕБ КОРПОРАТИВНИЙ БАНК» ПЕРСОНАЛЬНИХ ДАНИХ

У БАЗАХ ПЕРСОНАЛЬНИХ ДАНИХ

I. Загальні положення

1.1. Порядок обробки АКЦІОНЕРНИМ ТОВАРИСТВОМ «СЕБ КОРПОРАТИВНИЙ БАНК» (надалі - Банк) персональних даних в базах персональних даних (далі – Порядок) розроблений на виконання Закону України «Про захист персональних даних» (далі – Закон), відповідно до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних, вчинену 28 січня 1981 року в м. Страсбурзі, та Додаткового протоколу неї, Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, Конституції України, Закону України «Про захист персональних даних», Цивільного кодексу України, Законів України «Про інформацію», «Про захист інформації в автоматизованих системах», інших нормативно-правових актів України.

1.2. Порядок визначає загальні правила та умови обробки Банком персональних даних, а саме: збирання, реєстрації, накопичення, зберігання, адаптування, зміни, поновлення, використання і поширення, знеособлення, знищення відомостей про фізичну особу і регламентує механізм виконання дій з обробки персональних даних з моменту їх отримання Банком до знищення чи передачі до архіву.

Мета Порядку – забезпечення впровадження Банком найбільш оптимальних та ефективних процедур, пов’язаних з обробкою персональних даних в базах персональних даних, належного захисту прав суб’єктів персональних даних при обробці персональних даних.

1.4. Обробка персональних даних здійснюється повністю або частково в електронній формі з використанням засобів інформаційної (автоматизованої) системи та/або у паперовій формі шляхом ведення картотек персональних даних.

II. Загальні правила та умови обробки персональних даних

2.1. До персональних даних належать свідчення про суб’єкта: відомості, що ідентифікують або дають змогу ідентифікувати особу, відомості про грошові зобов'язання суб'єкта інформації, документована інформація про особу з державних реєстрів, інших баз даних публічного користування, відкритих для загального користування джерел тощо.

Персональні дані, незалежно від природи, змісту, способів та форми обробки відомостей, застосування загальних чи особливих вимог обробки, а також незалежно від ступеню зв'язку з фізичною особою, повинні оброблятися відповідно до встановлених законодавством України принципів обробки персональних даних.
2.2. Принципами обробки персональних даних є:

Загальне
2.2.1. Персональні дані повінні оброблятись на законних підставах, добросовісно та прозоро.

Обмеження мети
2.2.2. Персональні дані повинні збиратися для точно визначених, явних і леґітимних цілей та не оброблятись у спосіб, що є несумісним з цими цілями.

Зберігання та видалення Персональних даних
2.2.3. Дані повинні зберігатись у формі, що дозволяє ідентифікацію суб'єкта персональних даних не довше, ніж це необхідно для цілей, в яких вони обробляються.

Точність та пропорційність
2.2.4. Дані повинні бути точними та, в разі потреби, оновлюватись відповідно до цілі їх обробки. Необхідно вжити всіх достатніх заходів для забезпечення того, щоб персональні дані, які є неточними з огляду на цілі, для яких вони обробляються, були негайно видалені або виправлені. Крім того, Персональні дані повинні бути адекватними, релевантними та обмеженими стосовно цілей, для яких вони збираються та/або обробляються. Крім того, Персональні дані повинні оброблятися лише у спосіб, який забезпечує належну безпеку, включаючи захист від несанкціонованої або незаконної обробки та від випадкової втрати, знищення або пошкодження з використанням відповідних технічних або організаційних заходів.

Критерії законності обробки даних
2.2.5. Загальними підставами виникнення права на обробку персональних даних є:
a) згода суб'єкта персональних даних на обробку його персональних даних.
b) укладення та виконання правочину, в якому однією із сторін якого є суб'єкт персональних даних;
c) виконання юридичного зобов'язання Банку.
d) захист життєво важливих інтересів суб'єкта персональних даних або іншої фізичної особи.
e) необхідність виконання обов'язків Банку в суспільних інтересах та/або не виключно, які виникали при виконанні Банком своїх обов'язків передбачених законодавством (в т.ч. Законом України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення") до часу, коли отримання згоди на обробку персональних даних від суб'єкта персональних даних стане можливим.
f) необхідність захисту законних інтересів Банку або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта персональних даних у зв'язку з обробкою його даних переважають такі інтереси, зокрема, якщо суб'єкт персональних даних є дитиною.
g) надане Банку, як володільцю бази персональних даних право (дозвіл) на обробку персональних даних відповідно до його прав та обов'язків, передбачених Законом України «Про Національний банк України», «Про банки та банківську діяльність», «Про платіжні

системи та переказ коштів в Україні», «Про організацію формування та обігу кредитних історій» та прийнятих у відповідності до них нормативно правових актів Національного банку України і виключно в інтересах економічного добробуту людини та суспільства і прав людини на отримання фінансових послуг.

Права Суб'єкта персональних даних

2.2.7. Суб'єкт персональних даних має право:

1) знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;

2) отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані;

3) на доступ до своїх персональних даних;

4) отримувати не пізніш як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних;

5) пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних;

6) пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;

7) 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;

8) звертатися із скаргами на обробку своїх персональних даних до Уповноважений або до суду;

9) застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;

10) вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;

11) відкликати згоду на обробку персональних даних;

12) знати механізм автоматичної обробки персональних даних;

13) на захист від автоматизованого рішення, яке має для нього правові наслідки.

Захист обробки

2.2.8. Банк вживає відповідні технічні та організаційні заходи для забезпечення рівня безпеки, відповідно до ризиків, включаючи, зокрема:

1) псевдонімізація та шифрування персональних даних;

2) здатність забезпечити постійну конфіденційність, цілісність, доступність і стійкість систем і сервісів обробки;

3) можливість своєчасного відновлення доступності та доступу до персональних даних у разі фізичного або технічного інциденту;

4) процес регулярного тестування та оцінки ефективності технічних та організаційних заходів для забезпечення безпеки обробки.

При оцінці належного рівня безпеки враховуються, зокрема, ризики, які представляє обробка, зокрема випадкове або незаконне знищення, втрата, зміна, несанкціоноване розкриття або доступ до персональних даних, що передаються, зберігаються або обробляються іншим чином.

2.5. Формами надання згоди суб’єкта персональних даних можуть бути:

а) документ на паперовому носії з реквізитами, що дає змогу ідентифікувати цей документ та фізичну особу. Добровільне волевиявлення суб’єкта персональних даних засвідчується його підписом;

б) електронний документ, включаючи обов’язкові реквізити документа, що дають змогу ідентифікувати цей документ та фізичну особу. Добровільне волевиявлення фізичної особи щодо надання дозволу на обробку її персональних даних засвідчується електронним підписом суб’єкта персональних даних;

в) відмітка на електронній сторінці документу чи у електронному файлі, що обробляється в інформаційній системі на основі документованих програмно-технічних рішень, які, в свою чергу:

- не дозволяють обробку персональних даних до того часу, поки суб'єкт персональних даних не виконає дії, що підтверджують надання ним відповідної згоди;

- забезпечують реєстрацію дій суб’єкта персональних даних та цілісність протоколів реєстрації таких дій.

г) інші форми, що не суперечать законодавству України та дозволяють виконувати типові банківські операції (обмін валют, переказ коштів без відкриття банківського рахунку тощо) в звичайний спосіб, в т.ч. усно або шляхом акцепту публічно доступної інформації про обробку персональних даних, доступного для кожного суб’єкта персональних даних, що здійснює типову банківську операцію.

Надана згода може включати всі або окремі цілі обробки персональних даних для яких вони будуть використовуватися, підтвердження, що суб'єкт персональних даних повідомлений Банком про включення його персональних даних до бази персональних даних, про доступ до персональних даних суб’єкта розпорядників та третіх осіб, про права суб'єкта персональних даних відповідно до Закону та може бути викладена як цілісний документ, в анкеті для укладення правочину, в тексті договору про укладення правочину або іншим прийнятним для сторін шляхом, згідно домовленості між ними.

2.6. Згода суб’єкта персональних даних на обробку його персональних даних повторно не надається, якщо Банк продовжує обробляти персональні дані суб’єкта, відповідно до правовідносин на основі вільного волевиявлення фізичної особи, які виникли до набрання чинності Законом.

2.7. Суб'єкт персональних даних має право при наданні згоди внести застереження стосовно обмеження права на обробку своїх персональних даних, а Банк – надавати послуги, якщо таке застереження суб’єкта дозволяє Банку виконувати вимоги Закону України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення ";

2.8. Банк має зберігати фактичні дані, що свідчять про згоду суб’єкта персональних даних на обробку даних протягом строку обробки персональних даних.

2.9. Обробка персональних даних Банком здійснюється у відповідності до Закону, Законів України «Про банки та банківську діяльність», «Про платіжні системи та переказ коштів в Україні», «Про організацію формування та обігу кредитних історій» та прийнятих у відповідності до них актів Національного банку України і включає право розпорядника та третіх осіб обробляти персональні дані із баз персональних даних, що належать Банку та право Банку, як розпорядника, обробляти персональні дані із баз персональних даних, що не належать Банку.

Банк має право у відповідності до Закону відстрочити або відмовити у доступі до персональних даних третім особам і не має права відстрочити або відмовити у доступі до персональних даних суб'єкту персональних даних.

Суб'єкти персональних даних та треті особи мають право оскаржувати відстрочення або відмову у доступі до персональних даних відповідно до Закону.

VII. Порядок захисту інформації від несанкціонованого доступу при обробці персональних даних у складі інформаційної (автоматизованої) системи

7.1. З метою належного захисту інформації від несанкціонованого доступу володільцям та розпорядникам бази персональних даних при обробці персональних даних рекомендується вживати наступних заходів:

7.1.1. забезпечити обробку персональних даних у такий спосіб, щоб початок обробки персональних даних був можливий лише після вчинення особою, яка допущена до такої обробки дій, спрямованих на її авторизацію та ідентифікацію в інформаційній (автоматизованій) системі, в рамках якої здійснюється така обробка.

Володілець або розпорядник самостійно визначають спосіб авторизації та ідентифікації цих осіб. При цьому способом авторизації та ідентифікації може бути присвоєння кожній відповідальній особі та особі, яка допущена до обробки персональних даних у базі персональних даних, унікального логіну та паролю. В особливих випадках за рішенням володільця або розпорядника для забезпечення ідентифікації цих осіб додатково до логіну та паролю доступу може використовуватися електронний цифровий підпис.

7.1.2. Володільцю або розпоряднику бази персональних даних рекомендовано забезпечувати антивірусний контроль інформаційної (автоматизованої) системи, у складі якої здійснюється обробка персональних даних.

7.1.3. Для профілактики інцидентів, пов'язаних з ненавмисними діями відповідальних осіб, що можуть призвести до розголошення (втрати) персональних даних, володільцю або розпоряднику бази персональних даних рекомендовано визначити порядок захисту персональних даних під час їх обробки в інформаційних (автоматизованих) системах, що має містити заходи щодо:

- планової та позапланової заміни паролю відповідальної особи;

- періодичності та порядку резервного копіювання даних;

- визначення дій відповідальних осіб при виявленні вірусної небезпеки та періодичність оновлення антивірусних баз.