ЗАТВЕРДЖЕНО

Рішенням Наглядової Ради

Протокол № 022/2019 від 18.12.2019 р.

Голова Наглядової Ради

_____ Поспєловскі Е.

ПОЛІТИКА ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В АТ АКБ «ЛЬВІВ»

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Політика щодо захисту персональних даних (надалі – Політика) визначає основні принципи обробки відомостей чи сукупності відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, в будь-яких напрямках діяльності Банку, а також завдання Банку щодо дотримання безпеки персональних даних та забезпечення прав суб'єктів персональних даних відповідно до вимог законодавства України, з врахуванням вимог Regulation (EU) 2016/679 «Загальний регламент про захист даних» (надалі – GDPR).

1.2. У цій Політиці терміни вживаються у такому значенні:

База персональних даних - іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних;

Банк – АТ АКБ «ЛЬВІВ».

Вимоги – вимоги, що повинні дотримуватися працівники Банку під час Обробки персональних даних згідно з законодавством України з питань захисту Персональних даних, а також цієї Політики.

Витяг – витяг про Персональні дані конкретного Суб'єкта, які обробляються Банком;

Володілець – володілець Персональних даних - фізична чи юридична особа, державний орган або будь-який інший орган, що, окремо чи разом з іншими, визначає цілі і засоби Обробки персональних даних.

Комплаєнс-ризик – імовірність виникнення збитків/санкцій, додаткових втрат або недоотримання запланованих доходів або втрати репутації внаслідок невиконання банком вимог законодавства, нормативно-правових актів, ринкових стандартів, правил добросовісної конкуренції, правил корпоративної етики, виникнення конфлікту інтересів, а також внутрішньобанківських документів банку;

Згода - згода Суб'єкта Персональних даних – добровільне волевиявлення Суб'єкта за умови його поінформованості щодо надання згоди на Обробку його персональних даних відповідно до сформульованої мети їх обробки (у письмовій формі або у формі, що дає змогу зробити висновок про надання Суб'єктом згоди, у т.ч. надана під час реєстрації в інформаційно-телекомунікаційних системах шляхом проставлення відповідної відмітки).

Обробка персональних даних - будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення Персональних даних Суб'єкта, у тому числі з використанням інформаційних (автоматизованих) систем.

Особливі категорії персональних даних – Персональні дані, обробка яких становить особливий ризик для прав і свобод Суб'єктів: про расове, етнічне, національне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та/або організаціях, професійних спілках, релігійних організаціях чи в громадських організаціях світоглядної спрямованості, притягнення до адміністративної чи кримінальної відповідальності, застосування щодо особи заходів в рамках досудового розслідування або заходів, передбачених Законом України «Про оперативно-розшукову діяльність», вчинення щодо Суб'єкта тих чи інших видів насильства, а також дані, що стосуються здоров'я, статевого життя, біометричних або генетичних даних, місцеперебування та/або шляхи пересування Суб'єкта.

Офіс GDPR–Служба комплаєнс, до завдань якої відноситься забезпечення організації контролю за захистом персональних даних відповідно до законодавства України.

Оцінка відповідності – оцінка впливу нових продуктів, проектів, ініціатив Банку на режим захисту Персональних даних, виявлення ризиків недотримання Вимог.

Операційний ризик – ризик втрат, що виникає через неадекватні або недосконалі внутрішні процеси, системи, дії персоналу або в результаті впливу зовнішніх подій. Це визначення включає юридичний ризик та не включає стратегічний та репутаційний ризики.

Подія операційного ризику – непередбачений результат бізнес-діяльності, спричинений неадекватними процесами або збоями у внутрішніх процесах/системах, людьми або зовнішніми подіями.

Персональні дані – відомості чи сукупність відомостей про Суб'єкт, який ідентифікований або може бути конкретно ідентифікований.

Уповноважений - Уповноважений Верховної Ради України з прав людини - є посадовою особою, статус якої визначається Конституцією України, Законом України «Про Уповноваженого Верховної Ради України з прав людини» та іншими законами України, яка здійснює парламентський контроль за додержанням конституційних прав і свобод людини і громадянина та захист прав кожного на території України і в межах її юрисдикції на постійній основі.

Реєстр - перелік процесів Банку з Обробки персональних даних.

Розпорядник – фізична чи юридична особа, якій Банк надав право на Обробку персональних даних від імені Банку (на підставі укладеного з Банком договору).

Суб'єкт – фізична особа, персональні дані якої обробляються Банком.

Data protection Officer - відповідальна особа з питань захисту Персональних даних – Начальник Служби комплаєнс, який відповідає за дотримання Банком належного рівня захисту Персональних даних.

1.3. Метою Політики є створення безпечного середовища для Обробки персональних даних Суб'єктів, Володільцем або розпорядником яких є Банк, забезпечення адекватного та послідовного управління ризиками, що виникають при Обробці Банком персональних даних Суб'єктів.

1.4. Банк прагне дотримуватися вимог *GDPR*, зокрема, у відносинах, що безпосередньо входять в сферу його регулювання, за умови безумовного дотримання вимог законодавства України з питань захисту Персональних даних та забезпечує організацію контролю за захистом Персональних даних з врахуванням функціонування системи управління Комплаєнс-ризиком.

1.5. Політика визначає основні засади та правила Обробки Банком персональних даних фізичних осіб будь-якої категорії – працівників, контрагентів, клієнтів, акціонерів, пов'язаних з ними осіб, тощо.

1.6. Вимоги Політики поширюються на діяльність всіх відокремлених та структурних підрозділів Банку. Політика є обов'язковою для виконання і дотримання усіма працівниками Банку та Розпорядниками, які здійснюють Обробку персональних даних на підставі укладених з Банком договорів.

1.7. Політика застосовується до Персональних даних Суб'єктів, що існують в електронній або паперовій формі, та обробляються як в інформаційних системах/автоматизованими засобами, так і іншими способами (без використання автоматизованих засобів), наприклад в паперовій формі.

1.8. Порядок розкриття Персональних даних третім особам та Розпорядникам (надання доступу до Персональних даних) без отримання Згоди Суб'єкта Персональних даних здійснюється в порядку, що визначається нормативними документами Банку з питань захисту банківської таємниці та іншої інформації з обмеженим доступом.

1.9. Будь-які виключення/відхилення від вимог Політики застосовуються виключно на підставі рішення Правління Банку.

2. ПРИНЦИПИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Під час Обробки персональних даних Суб'єктів Банк повинен забезпечити дотримання наступних принципів:

2.1. Законність Обробки персональних даних

2.1.1.Обробка Банком персональних даних вважається законною за умови:

- отримання Згоди Суб'єкта на обробку персональних даних
- отримання Банком дозволу на Обробку персональних даних відповідно до законодавства України виключно для здійснення Банком своїх повноважень;
- укладення та виконання правочину, однією із сторін якого є Суб'єкт або який укладено на користь Суб'єкта або для здійснення переддоговірних заходів на вимогу Суб'єкта;
- дотримання принципу захисту життєво важливих інтересів Суб'єкта;
- виконання Банком вимог, установлених законодавством України;
- дотримання принципу захисту законних інтересів Банку або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту основоположних прав і свобод Суб'єкта у зв'язку з Обробкою його персональних даних переважають такі інтереси.

Банк повинен забезпечити здійснення Обробки персональних даних виключно за наявності однієї з вище зазначених умов. Обробка Банком Особливих категорій персональних даних дозволяється тільки за наявності спеціальних правових підстав, визначених законодавством України, зокрема:

- за умови надання Суб'єктом однозначної Згоди на обробку таких даних;
- обробка таких даних необхідна для здійснення прав та виконання обов'язків Банку у сфері трудових правовідносин відповідно до законодавства України із забезпеченням відповідного захисту даних Суб'єкта;
- обробка таких даних необхідна для захисту життєво важливих інтересів Суб'єкта або іншої особи у разі недієздатності або обмеження цивільної дієздатності Суб'єкта;
- обробка таких даних необхідна для обґрунтування, задоволення або захисту правової вимоги;
- обробка стосується даних, які були явно оприлюднені Суб'єктом.

2.1.2. Згода Суб'єкта на Обробку персональних даних повинна відповідати наступним критеріям:

- зрозумілість: формулювання, які використовує Банк для отримання Згоди повинні бути лаконічними та зрозумілими. Порядок відкликання Згоди також повинен бути зрозумілий та доступний для Суб'єкта;
- структурованість: якщо Згода є частиною договору, така згода повинна бути логічно та змістовно відокремлена від інших розділів договору;
- добровільність: виконання договору, в тому числі, надання послуг, не повинно залежати від отримання Згоди, якщо така згода не є необхідною для цілей цього договору;
- форма: Згода Суб'єкта повинна бути надана у письмовій формі або в іншій формі, що відповідає законодавству України, за умови застосовування до Банку;
- відкликання: Суб'єкт має право відкликати Згоду (визначено в п. 3.4. цієї Політики).

Згода на Обробку персональних даних малолітніх осіб, та, у випадках, передбачених нормативними документами Банку, неповнолітніх осіб надається Банку їх законними представниками.

2.1.3. Обробка персональних даних без Згоди Суб'єкта допускається виключно в інтересах національної безпеки, економічного добробуту та прав людини.

2.1.4. Обробка Банком Персональних даних, які оприлюднені як публічна інформація та\або надаються на запит у формі відкритих даних відповідно до законодавства України, не потребує одержання Згоди Суб'єкта Персональних даних (згідно зі ст. 10 ЗУ «Про доступ до публічної інформації»). Така інформація може Банком вільно копіюватись, поширюватись та використовуватись іншим чином, в тому числі в комерційних цілях, у поєднанні з іншою інформацією або шляхом включення до власного продукту Банку, з обов'язковим посиланням на джерело отримання цієї інформації.

2.2. Прозорість та відкритість Обробки персональних даних

Банк повинен забезпечити відкриту і прозору Обробку персональних даних із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки. З цією метою Банк забезпечує надання Суб'єкту повідомлення із вичерпною інформацією про Обробку його персональних даних, яке повинне містити:

- ідентифікаційні та контактні дані Банку;
- контактні дані Data protection Officer;
- склад та зміст зібраних Персональних даних Суб'єкта;
- цілі обробки, для яких було зібрано Персональні дані, та правові підстави для їх обробки;
- одержувачі або категорії одержувачів Персональних даних;
- інформація про передачу Персональних даних одержувачам у третіх країнах або міжнародним організаціям;
- строк зберігання Персональних даних або критерії, що використовуються для визначення цього строку;
- інформацію про права Суб'єктів Персональних даних;
- інформацію про те, чи є Обробка персональних даних вимогою законодавства України/ ЄС, за умови застосовування до Банку або договору, укладеного з Банком, або є необхідною для укладення договору, а також щодо того, чи зобов'язаний Суб'єкт надавати Персональні дані та можливі наслідки відмови у наданні таких даних;
- у випадку використання автоматизованої Обробки персональних даних для прийняття рішень щодо Суб'єкта (в т.ч. профайлінг): інформацію про логіку використання даних, а також вплив такої обробки на Суб'єкта;
- інформацію про здійснення подальшої Обробки персональних даних для інших цілей, якщо така обробка буде відбуватись;
- використання Банком інших джерел для збору Персональних даних про Суб'єкта.

Інформація про Обробку персональних даних надається Суб'єктам безкоштовно, до завершення збору Персональних даних, якщо вони збираються у Суб'єкта, а в інших випадках – не пізніше 30 днів з дня отримання Персональних даних.

Банк також надає Суб'єктам інформацію про порядок Обробки ним персональних даних шляхом розміщення її в електронній формі на офіційному веб-сайті Банку (www.banklviv.com) (надалі – Повідомлення). Суб'єкти мають змогу в будь-який час самостійно ознайомитися із Повідомленням.

Факт звернення Суб'єкта за послугою Банку, що не передбачає укладання договору, підтверджує самостійне ознайомлення Суб'єкта з Повідомленням. За необхідності, Повідомлення може використовувати різні засоби візуалізації інформації, зокрема, якщо його призначено для надання неповнолітнім особам.

Банк може отримувати Персональні дані Суб'єкта від третьої особи за умови надання третьою особою письмових гарантій, що:

- така передача здійснюється з дотриманням вимог законодавства України і не порушує права Суб'єкта, Персональні дані якого передаються;

- Суб'єкт, Персональні дані якого передаються, проінформований про склад та зміст переданих Персональних даних, про мету їх збору та про осіб, яким передаються його Персональні дані, а також про порядок реалізації ним прав, визначених Законом України «Про захист персональних даних».

2.3. Обмеження мети Обробки персональних даних

Банк здійснює Обробку персональних даних для конкретних і законних цілей. Мета Обробки персональних даних повинна бути чітко сформульована Банком та роз'яснена Суб'єкту.

Цілі, для яких Банк здійснює збір та Обробку персональних даних, містяться у Статуті Банку, нормативних документах Банку, Повідомленні, договорах, що укладаються між Банком та Суб'єктом.

Склад та зміст Персональних даних повинні бути відповідними, адекватними та не надмірними стосовно визначеної мети їх обробки.

У разі зміни визначеної мети Обробки персональних даних, у випадку, коли нова мета є несумісною з попередньою, подальша Обробка персональних даних Банком можлива за умови наявності Згоди Суб'єкта на Обробку його персональних даних відповідно до зміненої мети або якщо така обробка передбачена законодавством України.

Прийняття Банком рішення про сумісність нової мети Обробки персональних даних з попередньою здійснюється на підставі аналізу:

- зв'язку між цілями, для яких були зібрані Персональні дані, і цілями їх подальшої обробки;

- контексту, в рамках якого були зібрані Персональні дані, зокрема - в залежності від характеру правовідносини між Суб'єктом та Банком;

- характеру Персональних даних, зокрема, чи обробляються Особливі категорії персональних даних;

- можливі наслідки подальшої Обробки персональних даних для Суб'єктів;

- наявність відповідних гарантій, в.т.ч. шифрування даних або псевдонімізація.

Обробка персональних даних з метою надання інформації/пропозиції про послуги Банку, чи з метою зберігання Персональних даних в цілях виконання вимог законодавства України щодо порядку зберігання документів, не вважається несумісною обробкою та здійснюється Банком за умови забезпечення належного захисту Персональних даних.

2.4. Обмеження строку Обробки персональних даних

Персональні дані повинні оброблятися Банком у формі, що допускає ідентифікацію Суб'єкта, якого вони стосуються, не довше, ніж це необхідно для законних цілей, для яких вони збиралися або надалі оброблялися.

Банк повинен зберігати (обробляти) Персональні дані до закінчення строків зберігання відповідних документів/інформації, визначених умовами укладених договорів, Згодою, законодавством України. Якщо строки зберігання не визначені умовами укладених договорів чи Згодою, чи законодавством України, Банк має право самостійно визначити такі строки у нормативних документах Банку, керуючись принципами, викладеними в цій Політиці.

Строки зберігання повинні бути не меншими, аніж строки зберігання документів/інформації, визначені законодавством України. Строки зберігання Персональних даних не можуть бути меншими, ніж строки позовної давності у відповідних правовідносинах, визначені законодавством України. Якщо у певних правовідносинах законодавством визначено, що строки позовної давності не застосовуються, пов'язані з такими відносинами Персональні дані зберігаються Банком без обмеження строку.

Після закінчення строків зберігання, Персональні дані підлягають видаленню/знищенню або анонімізаціїї, в т.ч. в автоматичному порядку.

2.5. Мінімізація Персональних даних

При здійсненні Обробки персональних даних Банк зобов'язаний обмежуватись мінімально необхідним обсягом даних, який буде достатнім для досягнення цілей Обробки персональних даних.

2.5.1. Захист Персональних даних за призначенням (by design)

Зважаючи на об'єктивні обставини, витрати на реалізацію, специфіку, обсяг, контекст і цілі Обробки персональних даних, а також ймовірні ризики для прав і свобод Суб'єктів, які може спричинити обробка, Банк повинен, у момент визначення засобів Обробки персональних даних та в момент власне їх обробки, вжити необхідних технічних і організаційних заходів, призначених для результативної реалізації принципів захисту Персональних даних, зокрема, їх мінімізації.

2.5.2. Захист даних за замовчуванням (by default)

Банк повинен вживати відповідні технічні та організаційні заходи спрямовані на встановлення такого режиму захисту Персональних даних, що за замовчуванням не дозволятимуть надмірну Обробку персональних даних.

Для дотримання принципу мінімізації Персональних даних, Банк повинен ці дані:

- обробляти тільки для досягнення конкретної мети, з якою вони були зібрані,
- зберігати не довше, ніж це необхідно для досягнення мети їх збору,
- обробляти у тому обсязі, який обумовлений метою їх збору.

2.6. Точність Персональних даних

Банк повинен забезпечити точність та достовірність Персональних даних, які ним обробляються та оновлювати їх за потреби/у строки, визначені метою їх обробки.

Первинними джерелами відомостей про Суб'єкт є відомості, які він надає до Банку про себе, видані на його ім'я документи, підписані ним документи. Банк має право перевіряти надану Суб'єктом інформацію про себе в публічних джерелах офіційної інформації, та на підставі його Згоди – в третіх осіб.

Помилки, допущені в Персональних даних Суб'єкта, підлягають виправленню за його зверненням або з ініціативи Банку.

2.7. Цілісність та конфіденційність Персональних даних

Банк вживає організаційні та технічні заходи захисту інформації для забезпечення належного рівня безпеки Персональних даних (захист від несанкціонованої або незаконної Обробки персональних даних, від випадкової втрати, знищення або пошкодження даних)

Детальні вимоги щодо інформаційної безпеки даних визначаються Політикою інформаційної безпеки АТ АКБ «ЛЬВІВ».

2.8. Підзвітність

Банк повинен мати змогу продемонструвати відповідність застосованого в Банку режиму захисту Персональних даних принципам, визначеним у розділі 2 цієї Політики .

З цією метою Банк повинен запровадити процеси та процедури, що передбачатимуть:

- ведення обліку процесів з Обробки персональних даних, що здійснюються Банком, шляхом ведення Реєстру (визначено в розділі 6 цієї Політики);

- перевірку та Оцінку відповідності Офісом GDPR із залученням Відповідальних менеджерів при будь-яких змінах в існуючих програмних рішеннях/продуктах/процесах Обробки персональних даних;

- регулярну перевірку Офісом GDPR із залученням Відповідальних менеджерів всіх існуючих процесів Обробки персональних даних на відповідність вимогам Політики не рідше ніж один раз на два роки.

3. ПРАВА СУБ'ЄКТІВ ПЕРСОНАЛЬНИХ ДАНИХ

3.1. Доступ до Персональних даних

Суб'єкт має право:

- знати про джерела збирання, місцезнаходження своїх Персональних даних, мету їх обробки Банком, місцезнаходження або місце реєстрації Банку чи Розпорядника, що здійснюють Обробку його персональних даних, або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законодавством України, за умови застосовування до Банку;

- отримувати інформацію про умови надання Банком доступу до його Персональних даних, зокрема інформацію про третіх осіб, яким Банком передаються його Персональні дані;

- на доступ до своїх Персональних даних, які обробляються Банком;

- отримувати не пізніш як за тридцять календарних днів з дня надходження до Банку запиту, крім випадків, передбачених законодавством України, відповідь про те, чи обробляються Банком його Персональні дані, а також отримувати зміст таких Персональних даних;

- знати механізм автоматичної Обробки своїх персональних даних.

Суб'єкт має право на одержання від Банку будь-яких відомостей про себе за умови можливості ідентифікації Банком Суб'єкта цього запиту.

Якщо Банк здійснює Обробку персональних даних конкретного Суб'єкта, його запит щодо отримання доступу до своїх Персональних даних задовольняється протягом тридцяти календарних днів з дня його надходження, якщо інше не передбачено законодавством України. Відстрочення доступу Суб'єкта до своїх Персональних даних не допускається.

Копія Персональних даних, що обробляються Банком, надається Суб'єкту у формі Витягу, порядок складання якого визначається Банком самостійно.

Доступ Суб’єкта до його Персональних даних (у т.ч. надання Витягу) здійснюється Банком безоплатно.

3.2. Зміна та видалення Персональних даних

Суб’єкт має право пред’являти Банку вмотивовану вимогу щодо зміни або знищення своїх Персональних даних Банком та Розпорядником, якщо ці дані обробляються незаконно чи є недостовірними.

3.2.1. Банк зобов'язаний вносити зміни до Персональних даних на підставі вмотивованої письмової вимоги Суб'єкта, а також у разі виявлення неточності або помилки у Персональних даних.

Зміна Персональних даних, які не відповідають дійсності, проводиться невідкладно з моменту встановлення невідповідності.

Зміни до Персональних даних Суб’єкта, що є клієнтом чи контрагентом Банку за укладеним з Банком договором, вносяться за зверненням Суб’єкта з наданням Банку документів, що підтверджують такі зміни. Банк зобов’язаний вносити зміни до Персональних даних також за зверненням інших суб’єктів відносин у випадках, визначених законодавством України.

3.2.2. Суб’єкт має право подати Банку заяву про видалення/знищення його Персональних даних («право бути забутим»).

Персональні дані підлягають видаленню або знищенню у разі:

- закінчення строку зберігання даних, визначеного Згодою Суб'єкта на обробку цих даних або законодавством України;

- припинення правовідносин між Суб'єктом Персональних даних та Банком, якщо інше не передбачено законодавством України;

- видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого Верховної Ради України з прав людини;

- набрання законної сили рішення суду щодо видалення або знищення Персональних даних;

- якщо Персональні дані було зібрано Банком незаконно.

- якщо Суб’єкт відкликав Згоду (і у Банку немає інших правових підстав для здійснення Обробки персональних даних);

- суб’єкт заперечує проти Обробки персональних даних, якщо обробка ґрунтується виключно на законних інтересах Банку (і Банк не може обґрунтовано довести достатність свого законного інтересу для продовження Обробки персональних даних);

- якщо Персональні дані більше не є необхідними для досягнення цілей, для яких вони обробляються або були зібрані, та сплили строки позовної давності у таких відносинах, а також строки зберігання документів/інформації;

- якщо Персональні дані підлягають видаленню відповідно до вимог законодавства України;

Для знищення Персональних даних в інформаційних системах Банку, замість їх видалення, Банк може використовувати спосіб анонімізації цих даних. Процедура анонімізації передбачає заміну існуючих персональних даних, які дозволяють ідентифікувати Суб’єкта , на знаки/символи тощо, наприклад: заміна ПІБ клієнта на XXXXXXXXXX.

Банк не видаляє та не знищує Персональні дані, якщо Обробка персональних даних здійснюється, зокрема, для:

- реалізації права на свободу слова та інформації;

- дотримання зобов'язань, які передбачають Обробку персональних даних відповідно до законодавства України або ЄС, для виконання дій в інтересах суспільства або для здійснення офіційних повноважень Банку;

- подання, реалізації або супроводження судових позовів.

Банк повинен повідомляти про зміну та видалення Персональних даних Суб'єкта та кожного одержувача, якому було передано Персональні дані Суб'єкта, за умови, що це є технічно можливим.

3.3. Обмеження Обробки персональних даних

Суб'єкт має право вносити Банку застереження стосовно обмеження права на Обробку своїх персональних даних. Суб'єкт має право подати Банку заяву про встановлення режиму обмеження Обробки його персональних даних:

- на час, протягом якого Банк перевіряє точність та правильність Персональних даних;

- у випадку, якщо Обробка персональних даних здійснюється без належних правових підстав (але Суб'єкт не вимагає їх видалення);

- якщо строки Обробки персональних даних вже пройшли, але ці дані потрібні Суб'єкту для подання, реалізації або супроводження судових позовів;

- у разі подання Суб'єктом даних заяви про заперечення проти Обробки його персональних даних - на час, протягом якого здійснюється перевірка того, чи не переважають законні інтереси Банку над правами Суб'єкта.

При обмеженні Обробки персональних даних Банк має право лише здійснювати зберігання Персональних даних Суб'єкта (за відсутності інших підстав для Обробки персональних даних). Для здійснення всіх інших видів Обробки персональних даних необхідно отримати Згоду Суб'єкта.

Банк повинен повідомляти про обмеження Обробки персональних даних Суб'єкта та кожного одержувача, якому було передано Персональні дані Суб'єкта, за умови, що це є технічно можливим і не потребує непропорційних зусиль.

Після скасування режиму обмеження Обробки персональних даних, Банк повинен повідомити про це Суб'єкта.

Обробка персональних даних не підлягає обмеженню, якщо обробка здійснюється Банком:

- відповідно до вимог законодавства України;

- для захисту законних інтересів Банку з метою подання, реалізації або супроводження судових позовів;

- для захисту прав іншої фізичної або юридичної особи;

- з інших причин, що мають важливе суспільне значення.

3.4. Відкликання Згоди та заперечення проти Обробки персональних даних

Суб'єкт має право у будь-який час подати Банку заяву про відкликання Згоди, а також пред'являти вмотивовану вимогу із запереченням проти Обробки своїх персональних даних.

У разі відкликання суб'єктом даних Згоди без виконання процедур, необхідних для припинення договірних або інших відносин з Банком, Банк продовжуватиме Обробку персональних даних в межах та обсягах, обумовлених реалізацією існуючих правовідносин та законодавством України, у тому числі для захисту Банком своїх прав та законних інтересів за договорами.

Окрім того, Суб'єкт має право заперечувати проти здійснення Банком Обробки його персональних даних у наступних випадках:

- Обробка персональних даних здійснюється виключно на підставі законного інтересу Банку, і Банк не має інших обґрунтованих законних підстав для продовження Обробки персональних даних, які превалюють над інтересами, правами та свободами Суб'єкта (не застосовується до Обробки персональних даних з метою подання, реалізації або супроводження судових позовів);

- Обробка персональних даних (в т.ч. профайлінг) здійснюється у рекламних цілях;

- Персональні дані обробляються для статистичних, наукових або історичних цілей і їх обробка не є необхідною з точки зору публічного інтересу.

Заперечення щодо Обробки персональних даних, необхідних Банку для виконання своїх зобов'язань, у тому числі відкликання суб'єктом даних Згоди, можуть стати підставою для припинення виконання Банком умов укладених договорів.

3.5. Захист від автоматизованої Обробки персональних даних

Суб'єкт Персональних даних має право знати механізм автоматичної Обробки персональних даних, а також має право на захист від автоматизованого рішення, яке має для нього правові наслідки.

Суб'єкт має право заперечувати проти того, щоб Банк приймав рішення щодо нього виключно на основі автоматизованої Обробки його персональних даних, у тому числі профайлінгу, у випадках, коли це створює правові наслідки для Суб'єкта.

Це право не застосовується, якщо таке рішення:

- необхідне для укладання або виконання договору між Суб'єктом та Володільцем Персональних даних;

- приймається на виконання законодавства України і передбачає відповідні заходи захисту прав, свобод та законних інтересів Суб'єкта даних;

або

- здійснюється на підставі Згоди Суб'єкта.

У випадку, якщо автоматизована Обробка персональних даних здійснюється згідно з підпунктами 1 і 3 цього пункту, Банк повинен вжити заходів для захисту прав та законних інтересів Суб'єкта даних та забезпечити право Суб'єкта на індивідуальний розгляд його заяви при прийнятті рішень щодо нього («людський фактор»), право висловити свою точку зору та право на оскарження таких рішень.

Якщо автоматизована Обробка персональних даних передбачає обробку Особливих категорій персональних даних, можуть застосовуватись додаткові обмеження.

3.6. Мобільність Персональних даних

У випадках, коли Обробка персональних даних здійснюється Банком автоматизованими системами обробки інформації та за Згодою Суб'єкта /на підставі договору, Суб'єкт має право:

- одержувати Персональні дані, які він надавав Банку, у структурованому, зрозумілому форматі;

- вимагати передачі Банком своїх Персональних даних напряму до іншого Володільця, якщо у Банку наявна технічна можливість для цього.

Використання цього права не обмежує право Суб'єкта вимагати видалення його Персональних даних. Це право не стосується такої Обробки персональних даних, яка здійснюється Банком в суспільних інтересах або для виконання вимог законодавства України. Крім того, реалізація права Суб'єкта на мобільність Персональних даних не повинна негативно впливати на права та інтереси інших осіб.

4. МІНІМАЛЬНІ ТЕХНІЧНІ ВИМОГИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

4.1. З метою дотримання прав Суб'єктів, визначених у п. 3 цієї Політики, Банк прагне забезпечити реалізацію в інформаційних системах Банку мінімальних технічних вимог:

- можливість автоматизованого формування Витягу: в інформаційних системах Банку, які містять Персональні дані, що підлягають включенню до Витягу, повинні бути реалізовані технічні рішення для створення консолідованого Витягу про Персональні дані конкретного Суб'єкта;

- реєстрація Згоди: Банк повинен реєструвати та зберігати в інформаційних системах Банку факт, дату та спосіб отримання Згоди Суб'єкта на Обробку персональних даних, а також дані про її відкликання чи обмеження;

- видалення та/або анонімізація даних: інформаційні системи Банку, в яких здійснюється Обробка персональних даних, повинні мати можливість видаляти або анонімізувати наявні в них Персональні дані;

- можливість формувати звіт про закінчення строків зберігання даних: закінченні по закінченню строків Обробки персональних даних, установлених законодавством або нормативними документами Банку, інформаційні системи Банку повинні формувати звіт про ті Персональні дані, які підлягають видаленню або анонімізації.

4.2. Наявні та нові інформаційні системи Банку, в яких здійснюється або буде здійснюватись Обробка персональних даних, повинні відповідати зазначеним вище мінімальним технічним вимогам.

5. ПОШИРЕННЯ/ПЕРЕДАЧА ПЕРСОНАЛЬНИХ ДАНИХ ТРЕТІМ ОСОБАМ

5.1. Поширення Персональних даних передбачає дії щодо їх передачі третім особам, в т.ч. Розпорядникам за Згодою Суб'єкта, а без Згоди – у випадках, визначених законодавством України, за умови застосовування до Банку, та виключно в інтересах національної безпеки, економічного добробуту та прав людини (якщо це необхідно).

5.2. Про передачу Персональних даних третім особам в т.ч. Розпорядникам Банк протягом десяти робочих днів повинен повідомити Суб'єкта, якщо цього вимагають умови його Згоди або якщо інше не передбачено законодавством України.

5.3. Зокрема, Банк не здійснює такого повідомлення у випадках, коли Суб'єкт в тексті Згоди прямо надав Банку відмову від отримання повідомлень про передачу Персональних даних третім особам, в т.ч. Розпорядникам та/або Суб'єкт проінформований про умови Обробки Банком його персональних даних при наданні Згоди/підписанні договору з Банком відповідно до п. 2.2 цієї Політики.

5.4. При передачі Персональних даних Розпорядникам/третім особам Банк повинен дотримуватися наступних вимог:

– Банк може доручити Обробку персональних даних тільки тим Розпорядникам/третім особам, які надають достатні гарантії захисту цих даних для забезпечення відповідності Обробки персональних даних вимогам законодавства України, та забезпечують відповідний захист прав Суб'єкта;

– Обробка персональних даних від імені Банку може здійснюватися Розпорядником/третім особам на підставі письмового договору, що визначає предмет, тривалість, характер та ціль Обробки персональних даних, тип та обсяг Персональних даних і категорій Суб'єктів, а також взаємні зобов'язання та права Банка і Розпорядника.

5.5. Розпорядник та будь-яка особа, що діє від імені Банку або Розпорядника і має доступ до Персональних даних Суб'єктів, володільцем або розпорядником яких є Банк, повинна обробляти такі дані відповідно до вказівок Банку, якщо інше не передбачено законодавством України.

6. ПОШИРЕННЯ/ПЕРЕДАЧА ПЕРСОНАЛЬНИХ ДАНИХ ДО ТРЕТІХ КРАЇН АБО МІЖНАРОДНИХ ОРГАНІЗАЦІЙ

6.1. Передача Персональних даних іноземним суб'єктам відносин, пов'язаних із Персональними даними, здійснюється Банком лише за умови забезпечення відповідною державою належного захисту Персональних даних у випадках, встановлених законодавством або міжнародним договором України з цією державою.

6.2. Держави - учасниці Європейського економічного простору, а також держави, які підписали Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою Обробкою персональних даних, визнаються такими, що забезпечують належний рівень захисту Персональних даних. Кабінет Міністрів України визначає перелік держав, які забезпечують належний захист Персональних даних.

6.3. Персональні дані не можуть поширюватися з іншою метою, ніж та, з якою вони були зібрані.

6.4. Персональні дані можуть передаватися Банком іноземним суб'єктам відносин, пов'язаних з Персональними даними, також у разі:

- надання Суб'єктом однозначної Згоди на таку передачу;
- необхідності укладення чи виконання правочину між Банком та третьою особою - Суб'єктом на користь Суб'єкта;
- необхідності захисту життєво важливих інтересів Суб'єктів;
- необхідності захисту суспільного інтересу, встановлення, виконання та забезпечення правової вимоги;
- надання Банком відповідних гарантій щодо невтручання в особисте і сімейне життя Суб'єкта.

6.5. Банк повинен запровадити необхідні процедури щодо дотримання структурними підрозділами Банку правил поширення\передачі Банком Персональних даних третім особам\Розпорядникам та забезпечує виконання контролю щодо їх дотримання з боку Служби комплаєнс.

7. ЗАХОДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

7.1. Банк зобов'язаний забезпечити захист Персональних даних від випадкових втрати чи знищення, від незаконної Обробки персональних даних, у т.ч. від незаконного знищення чи доступу до Персональних даних.

7.2. Банк вживає організаційні та технічні заходи для належного захисту Персональних даних, які обробляються Банком самостійно або передаються Розпорядникам для подальшої Обробки персональних даних.

7.3. Для забезпечення належного рівня безпеки даних Банк та Розпорядник повинні, за можливості, впроваджувати такі технічні заходи захисту, які відповідають ступеню ризику Обробки персональних даних, включаючи, зокрема:

- псевдонімізацію та шифрування Персональних даних;
- конфіденційність, цілісність, доступність та стійкість систем та процесів з Обробки персональних даних;
- можливість своєчасного відновлення доступу до Персональних даних у разі фізичного або технічного інциденту безпеки;
- регулярне тестування та оцінку ефективності технічних та організаційних заходів для забезпечення безпеки Обробки персональних даних;
- інші вимоги стосовно заходів захисту, передбачені законодавством України.

7.4. При визначенні рівня захисту Персональних даних слід враховувати поточний технічний стан інформаційних систем, витрати на імплементацію заходів захисту, характер Обробки персональних даних та ризики для прав та свобод Суб'єктів.

7.5. Вимоги щодо інформаційної безпеки Персональних даних повинні бути реалізовані відповідно до нормативних документів Банку у сфері інформаційної безпеки.

7.6. З метою забезпечення контролю ефективності процесу організації захисту у ПД в Банку Служба комплаєнсу може проводити вибірковий моніторинг дотримання вимог цієї Політики структурними підрозділами Банку.

8. БАЗИ ПЕРСОНАЛЬНИХ ДАНИХ, ВОЛОДІЛЬЦЕМ ЯКОЇ Є АТ АКБ "ЛЬВІВ"

2.1. АТ АКБ "Львів" є володільцем:

- бази персональних даних «АБС Б2», а саме: системи обліку клієнтів, контрагентів АТ АКБ "Львів" в електронній формі;
- бази персональних даних «Працівники», а саме: системи кадрового обліку АТ АКБ "Львів" в електронній формі та у формі картотек персональних даних.
- бази персональних даних "Зберігач", а саме: системи депозитарного обліку АТ АКБ "Львів" в електронній формі.

9. РЕЄСТР

9.1. Банк забезпечує ведення єдиного централізованого Реєстру. Кожен структурний підрозділ Банку зобов'язаний надавати Службі комплаєнс інформацію про всі внутрішні процеси, що передбачать роботу з Персональними даними та знаходяться в зоні відповідальності такого структурного підрозділу, для внесення в Реєстр.

9.2. Доступ до Реєстру надається відповідальним працівниками Служби комплаєнс.

9.3. Інформація, що міститься в Реєстрі, повинна бути точною та актуальною. Раз на рік здійснюється актуалізація процесів в Реєстрі з внесенням відповідних змін, якщо:

- існуючий процес з Обробки персональних даних зазнав змін чи завершився,

або

- в Банку створено новий процес з Обробки персональних даних.

9.4. Служба комплаєнс регулярно перевіряє якість даних, занесених в Реєстр. При виявлені неповноти або неточності інформації, або за потреби внесення додаткової інформації до Реєстру, Служба комплаєнс вносить відповідні виправлення в Реєстр.

9.5. Інформація, занесена в Реєстр, є конфіденційною інформацією Банку. Інформація з Реєстру може бути надана уповноваженим органам України, які здійснюють контроль за додержанням законодавства про захист Персональних даних.

10. ОЦІНКА ВІДПОВІДНОСТІ ВИМОГАМ ТА ВПЛИВУ НА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

10.1. Перед запуском будь-якого нового проекту, ініціативи, процесу або продукту структурний підрозділ - ініціатор зобов'язаний ініціювати проведення Оцінки відповідності.

10.2. Служба комплаєнс надає висновок щодо відповідності процесу Обробки персональних даних вимогам цієї Політики та, за необхідності, рекомендації щодо запровадження організаційних або технічних заходів для забезпечення такої відповідності.

10.3. Якщо згідно з висновком Служби комплаєнс Обробка персональних даних може призвести до порушення прав Суб'єктів, Банк, до здійснення Обробки персональних даних, повинен провести оцінювання впливу передбачених операцій щодо такої обробки на захист Персональних даних.

11. ПОРУШЕННЯ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

11.1. Порушення у сфері захисту Персональних даних (надалі – Порушення захисту ПД) означає порушення організаційних або технічних заходів безпеки з боку сторонніх осіб або працівників Банку, що призвело до випадкового або умисного видалення, несанкціонованого розголошення, втрати, зміни Персональних даних або неавторизованого доступу до них (наприклад, хакерська атака, втрата незашифрованих ноутбуків, USB-носіїв чи паперових документів, помилково зазначені одержувачі електронної пошти у розсилці).

11.2. Банк повинен своєчасно виявляти та реагувати на Порушення захисту ПД. Працівники структурних підрозділів Банку зобов'язані негайно інформувати Службу комплаєнс про всі Порушення захисту ПД, виявлені у їх поточній діяльності, або ризик виникнення таких порушень шляхом направлення електронних повідомлень засобами електронної пошти Банку на функціональну поштову скриньку compliance@banklviv.com .

11.3. Вимоги та порядок дій Розпорядника у разі виявлення Порушення захисту ПД, які передані Банком на обробку, повинні бути передбачені в договорі, укладеному між Банком та Розпорядником.

11.4. Реагування на Порушення захисту ПД передбачає виконання комплексу заходів, спрямованих на локалізацію негативних наслідків від такого порушення, з'ясування та документування обставин його вчинення, відшкодування збитків, притягнення винних до відповідальності, усунення причин та умов, що сприяли Порушенню захисту ПД, удосконалення контролів для попередження подібних порушень у майбутньому.

11.5. Керівник структурного підрозділу, у якому відбулося Порушення захисту ПД забезпечує проведення перевірки за фактом такого порушення. Результати перевірки повинні бути відповідним чином задокументовані та містити, щонайменше, наступну інформацію:

- характер порушення, в т.ч. категорії та приблизну кількість Суб'єктів, а також категорії та приблизну кількість категорій Персональних даних;
- обставини вчинення Порушення захисту ПД;
- ймовірні наслідки Порушення захисту ПД;
- заходи, вжиті або запропоновані з метою усунення Порушення захисту ПД, в т.ч. заходи для мінімізації можливих негативних наслідків.

11.6. Data protection Officer контролює своєчасність та якість проведення перевірки Порушення захисту ПД, вивчає результати таких перевірок, контролює діяльність структурних підрозділів –

власників процесів, структурних підрозділів, де сталося порушення, проводить перевірки щодо вжиття заходів з удосконалення контролів для попередження подібних порушень у майбутньому.

11.7. Якщо Порушення захисту ПД має масовий характер, Банк зобов'язаний додатково проінформувати про допущене порушення Суб'єктів. Повідомлення Суб'єктів може бути здійснено в індивідуальному порядку або шляхом розміщення інформації про порушення на офіційному веб-сайті Банку.

11.8. Банк звільняється від обов'язку інформувати Суб'єктів про Порушення захисту ПД а умови, якщо Банк:

- вжив належних технічних та організаційних заходів захисту інформації, що унеможливлюють розкриття або доступ до Персональних даних неуповноваженими особами;

- прийняв своєчасні, ефективні та послідовні заходи мінімізації наслідків порушення.

11.9. Управління порушеннями, що становлять інциденти інформаційної безпеки, здійснюється відповідно до вимог інформаційної безпеки.

11.10. Якщо порушення у сфері захисту персональних даних є подією операційного ризику, у тому числі подією, або містить ознаки шахрайства, інформування про таку подію та подальші заходи реагування здійснюються відповідно до нормативних документів Банку з питань управління операційними ризиками.

12. DATA PROTECTION OFFICER

12.1. З метою організації роботи, підтримки та контролю за діяльністю самостійних структурних підрозділів Банку щодо виконання завдань, пов'язаних із захистом Персональних даних в Банку призначено Data protection Officer .

12.2. Завдання Data protection Officer:

- надання працівникам Банку методичні роз'яснення та консультації щодо порядку виконання вимог про захист Персональних даних;

- контроль за дотриманням в Банку Вимог;

- проведення оцінки поточних та потенційних ризиків режиму захисту Персональних даних в Банку;

- взаємодія з Уповноваженим Верховною Радою України з прав людини та визначеними ним посадовими особами його секретаріату ЄС та Суб'єктами з питань захисту Персональних даних в діяльності Банку.

12.3. Data protection Officer повинен бути залученим до всіх питань та процедур, що стосуються захисту Персональних даних в Банку. Працівники Банку повинні сприяти Data protection Officer у виконанні ним його завдань, надавати йому необхідну інформацію, ресурси, доступ до Персональних даних та процесів з Обробки персональних даних.

12.4. Контакті дані Data protection Officer є відкритими і розміщуються на офіційному веб-сайті Банку. Суб'єкти можуть звертатися до Data protection Officer щодо всіх питань, пов'язаних з Обробкою їх персональних даних.

12.5. Інформація про діяльність у сфері захисту Персональних даних, яку здійснює Data protection Officer в межах власної компетенції, є конфіденційною. Data protection Officer має право виконувати додаткові функції за посадою, тільки у разі, якщо це не призводить до виникнення конфлікту інтересів.

13. НАВЧАННЯ

13.1. Працівники Банку повинні знати та дотримуватись Вимог та вимог нормативних документів Банку щодо захисту Персональних даних.

13.2. З цією метою для всіх працівників Банку з ініціативи Служби комплаєнс повинні проводитися регулярні навчання, щонайменше, раз на два роки. За потреби, можуть бути організовані позачергові навчання для певних категорій посад або для виконання певних робіт.

13.3. Навчання проводиться у формі електронного курсу або в інший спосіб, рекомендований Службою комплаєнс.

14. ВІДПОВІДАЛЬНІСТЬ

14.1. Працівники Банку несуть персональну відповідальність за збереження конфіденційної інформації Банку та забезпечення захисту Персональних даних, які обробляються ними під час виконання їх посадових обов'язків, згідно з вимогами відповідних нормативних документів Банку.

14.2. Керівники самостійних структурних підрозділів за посадою відповідають за забезпечення в їх структурних підрозділах захисту Персональних даних згідно з вимогами відповідних нормативних документів Банку .