



ЗАТВЕРДЖЕНО
рішенням Правління ПАТ «АП БАНК»
від 30.11.2018 р.
Протокол №43
реєстр.№1785 від 30.11.2018

ПОЛОЖЕННЯ
про обробку та захист персональних даних
ПАТ «АП БАНК»

м.Київ, 2018

1. Загальні положення

- 1.1. Положення про обробку та захист персональних даних ПАТ «АП БАНК» (далі — Положення) визначає комплекс організаційних та технічних заходів з обробки та захисту персональних даних суб'єктів персональних даних ПАТ «АП БАНК» (далі — Банк) від несанкціонованого доступу, витоку інформації, неправомірного використання або втрати під час обробки.
- 1.2. Положення розроблено на підставі Закону України «Про захист персональних даних» від 01.06.2010 № 2297-VI (далі — Закон №2297) та Типового порядку обробки персональних даних у базах персональних даних, затвердженого наказом уповноваженого Верховної ради України з прав Людини від 08.01.2014 № 1/02-14 «Про затвердження документів у сфері захисту персональних даних» (далі — Типовий порядок).
- 1.3. Положення є обов'язковим для виконання працівниками Банку, які мають доступ до персональних даних та обробляють персональні дані.
- 1.4. Усі терміни у цьому Положенні визначаються відповідно до Закону №2297 та Типового порядку.
- 1.5. Персональні дані фізичних осіб, які обробляються Банком, є конфіденційною інформацією.

2. Терміни та скорочення

В Положенні використовуються такі терміни та скорочення:

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

володілець персональних даних - фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом / Положенням;

згода суб'єкта персональних даних - добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. У сфері електронної комерції згода суб'єкта персональних даних може бути надана під час реєстрації в інформаційно-телекомунікаційній системі суб'єкта електронної комерції шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки, за умови, що така система не створює можливостей для обробки персональних даних до моменту проставлення відмітки;

знеособлення персональних даних - вилучення відомостей, які дають змогу прямо чи опосередковано ідентифікувати особу;

картотека - будь-які структуровані персональні дані, доступні за визначеними критеріями, незалежно від того, чи такі дані централізовані, децентралізовані або розділені за функціональними чи географічними принципами;

обробка персональних даних - будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання й поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, зокрема з використанням інформаційних (автоматизованих) систем;

одержувач - фізична чи юридична особа, якій надаються персональні дані, зокрема третя особа;

персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;

розпорядник персональних даних - фізична чи юридична особа, якій володільцем персональних даних або законом / Положенням надано право обробляти ці дані від імені володільця;

суб'єкт персональних даних - фізична особа, персональні дані якої обробляються;

третя особа - будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого Верховної Ради України з прав людини, якій володільцем чи розпорядником персональних даних здійснюється передача персональних даних.

3. Бази персональних даних, володільцем яких є Банк

3.1. База персональних даних працівників Банку:

- 3.1.1. Персональні дані працівників Банку обробляються у «Базі персональних даних працівників», володільцем якої є Банк.

- 3.1.2. Обробка персональних даних у «Базі персональних даних працівників» проводиться з метою забезпечення реалізації трудових, соціально-трудових відносин, відносин у сфері управління персоналом (відповідно до Кодексу законів про працю України, Статуту Банку, внутрішніх нормативних документів щодо підбору та прийому персоналу в Банку, норм кадрової політики Банку; адміністративно-правових відносин (відповідно до Господарського кодексу України, Цивільного кодексу України), відносин у сфері бухгалтерського та податкового обліку (відповідно до Податкового кодексу України, Законів України «Про бухгалтерський облік та фінансову звітність в Україні», «Про оплату праці»).
- 3.1.3. У Базі персональних даних працівників Банку обробляються ідентифікаційні дані (прізвище, ім'я та по батькові, адреса, телефон тощо); паспортні дані; реєстраційний номер облікової картки платника податків; особисті відомості (вік, стать, освіта, наявність наукового ступеню чи звання; родинний стан, склад сім'ї тощо); відношення до військової служби; професія; життєві інтереси та захоплення; запис фотозображень.
- 3.1.4. Для Баз персональних даних працівників Банку розпорядники відсутні. Працівники Банку не є розпорядниками зазначеної бази персональних даних.
- 3.1.5. Персональні дані у Базі персональних даних працівників Банку обробляються у вигляді картотеки особових карток, особових справ та за допомогою інформаційної системи «HRM».
- 3.1.6. База персональних даних працівників Банку розміщена в приміщеннях головного офісу Банку, Україна, 04119, м. Київ, вул. Дегтярівська, буд. 27-т (літера А) та серверах Банку.
- 3.1.7. В управлінні заробітної плати і кадрового адміністрування персональні дані працівників обробляються у картотеках (на паперових носіях – особові картки форма № П-2, особових справах, в інших документах, що містять персональні дані працівників, у тому числі трудові книжки, організаційно-розпорядчі документи, звітні та облікові форми) та в інформаційній системі «HRM».
- 3.1.8. Для бази персональних даних працівників Банку третіми особами у контексті Закону № 2297 є:
- державні органи, яким персональні дані працівників передаються відповідно до законодавства України (Пенсійний фонд, податкова інспекція, військові комісаріати, центри зайнятості тощо);
 - інші юридичні та фізичні особи, яким персональні дані працівників передаються відповідно до законодавства України, а також в рамках виконання господарських та інших відносин, та які можуть звертатись із запитом щодо доступу до персональних даних працівників згідно з чинним законодавством України.

3.2. База персональних даних клієнтів Банку:

- 3.2.1. Персональні дані клієнтів Банку обробляються у «Базі персональних даних клієнтів», володільцем якої є Банк.
- 3.2.2. У Базі персональних даних клієнтів Банку обробляються ідентифікаційні дані (прізвище, ім'я та по батькові, адреса, дата та місце народження, громадянство, місце проживання тощо) та дані, що належать до банківської таємниці (відомості про банківські рахунки клієнтів, операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди, фінансово-економічний стан клієнтів).
- 3.2.3. Для Баз персональних даних клієнтів Банку розпорядники відсутні. Працівники Банку не є розпорядниками зазначеної бази персональних даних.
- 3.2.4. Персональні дані у Базі персональних даних клієнтів Банку обробляються у вигляді картотеки справ та за допомогою інформаційних систем («АБС Б2», тощо) з метою: забезпечення реалізації відносин у сфері економічних, фінансових послуг, відповідно до:

1	статті 6 Закону України «Про захист персональних даних»
2	Закону України «Про банки та банківську діяльність»
3	Положення про організацію бухгалтерського обліку, бухгалтерського контролю під час здійснення операційної діяльності в банках України, що затверджене постановою Правління Національного банку України від 04.07.2018 р. №75
4	Інструкції про порядок відкриття, використання і закриття рахунків у національній та іноземних валютах, що затверджена постановою Правління Національного банку України від 12.11.2003 р. № 492
5	Інструкції про порядок організації та здійснення валютно-обмінних операцій на території України, що затверджена постановою Правління Національного банку України від 12.12.2002 р. №502
6	Правил зберігання, захисту, використання та розкриття банківської таємниці, що затверджені постановою Правління Національного банку України від 14.07.2006 р.

	№267
7	Статуту Банку
8	Положення про операційну діяльність Банку
9	чинних Стандарти банківських продуктів Банку
10	Положення про банківську, комерційну таємницю і конфіденційну інформацію Банку

3.2.5.База персональних даних клієнтів Банку розміщена в приміщеннях головного офісу Банку, Україна, 04119, м. Київ, вул. Дегтярівська, буд. 27-т (літера А) та серверах Банку. Відділення Банку зберігають персональні дані клієнтів в паперовому вигляді в клієнтських справах.

3.2.6.Для бази персональних даних клієнтів Банку третіми особами у контексті Закону № 2297 є:

- державні органи, яким персональні дані клієнтів Банку передаються відповідно до законодавства України;
- інші юридичні та фізичні особи, яким персональні дані клієнтів передаються відповідно до законодавства України, а також в рамках виконання відносин у сфері економічних, фінансових послуг, та які можуть звертатись із запитом щодо доступу до персональних даних клієнтів згідно з чинним законодавством України.

3.3.У Банку не обробляються відомості про расове або етнічне походження суб'єктів персональних даних, їх політичні, релігійні або світоглядні переконання, членство в політичних партіях, відомості, що стосуються статевого життя.

4. Обов'язки та права особи, відповідальної за організацію роботи, пов'язаної із захистом персональних даних у Банку

4.1.З урахуванням вимог статті 24 Закону № 2297 наказом голови Правління Банку призначається особа, відповідальна за організацію роботи, пов'язаної із захистом персональних даних у Банку (далі — Відповідальна особа). Наказ доводиться до відома Відповідальної особи під підпис.

4.2. Відповідальна особа:

4.2.1.Забезпечує:

- організацію необхідних заходів щодо захисту персональних даних у Банку та контроль виконання положень даного документу;
- подання заяв про державну реєстрацію баз персональних даних, про обробку персональних даних, що становлять особливий ризик для прав і свобод суб'єктів персональних даних (за необхідності);
- ознайомлення керівників структурних підрозділів та працівників Банку з вимогами законодавства про захист персональних даних та змінами до нього, зокрема щодо зобов'язання не допускати розголошення у будь-який спосіб персональних даних, які було довірено або які стали відомі у зв'язку з виконанням посадових обов'язків.

4.2.2.Бере участь:

- у проведенні аналізу процесів обробки персональних даних відповідно до основних завдань та функцій Банку, зокрема визначення мети, з якою обробляються персональні дані, правових підстав для обробки персональних даних, відповідність та не надмірність персональних даних згідно з визначеною метою їх обробки, визначення третіх осіб, та приведення переліку персональних даних у відповідність до визначеної мети та правових підстав їх обробки;
- у визначенні персональних даних, що становлять особливий ризик для прав і свобод суб'єктів персональних даних;
- в процедурах обробки запитів третіх осіб щодо доступу до персональних даних (спільно з юридичним управлінням Банку).

4.2.3.Сприяє доступу суб'єктів персональних даних до власних персональних даних.

4.2.4.За необхідності готує проекти змін та доповнень до цього Положення.

4.2.5. Може погоджувати проекти положень про структурні підрозділи, працівниками яких обробляються персональні дані, та посадових інструкцій працівників, які обробляють персональні дані або мають доступ до них, за необхідності ініціює внесення необхідних змін та доповнень до положень про структурні підрозділи та посадових інструкцій.

4.2.6.Інформує голову Правління Банку про заходи, яких необхідно вжити для приведення складу персональних даних та процедур їх обробки у відповідність до чинного законодавства.

4.2.7.Інформує голову Правління Банку про порушення встановлених процедур обробки персональних даних.

4.2.8.Фіксує факти порушень режиму захисту персональних даних у порядку, визначеному розділом 7 цього Положення.

4.3. Відповідальна особа має право:

- 4.3.1.Перевіряти стан дотримання працівниками Банку законодавства у сфері захисту персональних даних та виконання вимог цього Положення, брати участь у службових розслідуваннях з питань порушень порядку обробки та захисту персональних даних.
- 4.3.2.Вносити пропозиції про розмежування режиму доступу працівників до обробки персональних даних відповідно до їх посадових обов'язків.
- 4.3.3.Розглядати вимоги працівників та клієнтів Банку щодо заперечення проти обробки їх персональних даних.

5. Права та обов'язки фізичної особи як суб'єкта персональних даних

Відповідно до Закону № 2297 фізична особа (працівник, клієнт Банку), персональні дані якої обробляються:

5.1. Є суб'єктом персональних даних.

5.2. Має право:

- знати про місцезнаходження та призначення відповідної бази персональних даних, мету обробки даних у відповідній базі персональних даних (працівників, клієнтів);
- отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються персональні дані, що містяться у базі персональних даних;
- на доступ до своїх персональних даних, що містяться у відповідній базі персональних даних, відповідно до статті 16 «Порядок доступу до персональних даних» Закону № 2297;
- отримувати не пізніше як за 30 календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи зберігаються його персональні дані у відповідній базі персональних даних, а також отримувати зміст його персональних даних, які зберігаються;
- пред'являти вмотивовану вимогу із запереченням проти обробки своїх персональних даних органами державної влади, органами місцевого самоврядування при здійсненні їхніх повноважень, передбачених законом;
- пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних Банком, якщо ці дані обробляються незаконно чи є недостовірними;
- 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;
- звертатися з питань захисту своїх прав щодо персональних даних до органів державної влади, органів місцевого самоврядування, до повноважень яких належить здійснення захисту персональних даних;
- застосовувати засоби правового захисту у разі порушення законодавства про захист персональних даних;
- вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;
- відкликати згоду на обробку персональних даних;
- знати механізм автоматичної обробки персональних даних;
- на захист від автоматизованого рішення, яке має для нього правові наслідки.

5.3. Суб'єкт персональних даних зобов'язаний повідомляти Банк про зміну своїх персональних даних, що підлягають обробці у відповідній базі персональних даних, у порядку, визначеному у даному Положенні.

5.4. Розпорядження персональними даними фізичної особи, обмеженої в цивільній дієздатності або визнаної недієздатною, здійснює її законний представник.

6. Обов'язки працівників Банку, які обробляють персональні дані

Працівники Банку, які обробляють персональні дані:

6.1. Мають бути обізнані з вимогами Закону № 2297 та інших нормативно-правових актів у сфері захисту персональних даних.

6.2. Зобов'язані:

- 6.2.1.Запобігати втраті персональних даних або їх неправомірному використанню;
- 6.2.2.Не розголошувати персональні дані, які їм було довірено або які стали відомі у зв'язку з виконанням посадових обов'язків, при цьому таке зобов'язання чинне після припинення ними діяльності, пов'язаної з обробкою персональними даними, крім випадків, установлених законом;
- 6.2.3.Терміново повідомляти Відповідальну особу у разі:
 - втрати або неумисного знищення носіїв інформації з персональними даними;
 - втрати ними ключів від приміщень, сейфів, шаф, де зберігаються персональні дані;

- якщо ідентифікаційні дані для входу в інформаційні системи обробки персональних даних стали відомі іншим особам.;
- виявлення спроби несанкціонованого доступу до персональних даних.

6.2.4. При звільненні з роботи або переведенні на іншу посаду своєчасно передати керівнику структурного підрозділу або іншому відповідальному працівнику носії інформації, що містять відомості про персональні дані, які були отримані або створені особисто чи спільно з іншими працівниками під час виконання посадових обов'язків.

7. Порядок та документаційне забезпечення обробки персональних даних у Банку

7.1. Збирання персональних даних

- 7.1.1. Обробка (зокрема збирання) персональних даних, зазначених у пунктах 3.1, 3.2, виконується на підставі Згоди суб'єкта персональних даних відповідно до Закону № 2297.
- 7.1.2. Відповідальні працівники Банку, що виконують обробку персональних даних в рамках своїх повноважень, роз'яснюють суб'єктам персональних даних порядок та підстави для обробки їхніх персональних даних відповідно до Закону № 2297, повідомляють про мету обробки персональних даних тощо.
- 7.1.3. Персональні дані суб'єкта персональних даних вносяться до відповідних інформаційних систем («HRM», «АБС Б2», тощо) та картотек персональних даних.
- 7.1.4. Про зміну своїх персональних даних, що підлягають обробці у «Базі персональних даних працівників Банку», працівники Банку повідомляють управлінню заробітної плати і кадрового адміністрування у строк, що складає 1 календарний місяць, якщо інше не визначено чинним законодавством України у сфері захисту персональних даних.
- 7.1.5. Про зміну своїх персональних даних, що підлягають обробці у Базі персональних даних клієнтів Банку, клієнти повинні повідомляти Банк у строк, визначений чинним законодавством України у сфері захисту персональних даних.
- 7.1.6. У разі виявлення факту внесення до бази персональних даних відомостей про суб'єкта персональних даних, які не відповідають дійсності, такі відомості мають бути невідкладно виправлені або знищені.
- 7.1.7. Отримані від суб'єктів персональних даних (працівників Банку) згоди на обробку персональних даних та повідомлення зберігаються в управлінні заробітної плати і кадрового адміністрування.

7.2. Зберігання та знищення персональних даних

- 7.2.1. Персональні дані суб'єктів персональних даних зберігаються у строк не більше, ніж це необхідно відповідно до мети їх обробки, якщо інше не передбачено законодавством України.
- 7.2.2. Персональні дані в базах персональних даних Банку знищуються в порядку, встановленому відповідно до вимог ч. 2 ст. 15 Закону № 2297.

7.3. Використання персональних даних суб'єктів персональних даних Банку

- 7.3.1. Під використанням персональних даних суб'єктів персональних даних згідно зі статтею 10 Закону № 2297 розуміються будь-які дії Банку щодо обробки цих даних, дії щодо їх захисту, а також дії щодо надання часткового або повного права обробки персональних даних іншим суб'єктам відносин, пов'язаних із персональними даними, що здійснюються за згодою суб'єкта персональних даних чи відповідно до закону.
- 7.3.2. Відомості про особисте життя суб'єкта персональних даних не можуть використовуватися як чинник, що підтверджує чи спростовує його ділові якості.
- 7.3.3. Доступ до персональних даних суб'єктів персональних даних, внесених до інформаційних систем та картотек персональних даних, мають працівники Банку в рамках їх повноважень, а також голова Правління Банку, його заступники, головний бухгалтер, відповідальний працівник юридичного управління відповідно до посадових обов'язків (внесених у посадові інструкції) в обсязі, необхідному для виконання таких обов'язків.
- 7.3.4. Працівники Банку, які працюють з персональними даними, зазначені у пункті 7.3.3, дають письмове зобов'язання про нерозголошення персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням посадових обов'язків.
- 7.3.5. Право доступу до персональних даних та їх обробку надається особам, зазначеним у пунктах 7.3.3, лише після підписання зобов'язання про нерозголошення персональних даних.
- 7.3.6. Забезпечення отримання зобов'язань покладається на працівників управління заробітної плати і кадрового адміністрування.
- 7.3.7. Датою надання права доступу до персональних даних вважається дата надання зобов'язання.
- 7.3.8. Датою позбавлення права доступу до персональних даних вважається дата звільнення працівника, дата переведення на посаду, виконання обов'язків за якою не пов'язано з обробкою персональних даних.

7.4. Облік порушень режиму захисту персональних даних

- 7.4.1. Факти порушень режиму захисту персональних даних фіксуються актами, які складає Відповідальна особа.
- 7.4.2. За необхідності за фактами порушень режиму захисту персональних даних Головою Правління Банку призначається службове розслідування.
- 7.4.3. За результатами службового розслідування працівників, винних у порушеннях, може бути притягнуто до юридичної відповідальності (дисциплінарної, кримінальної тощо).

8. Передання персональних даних

8.1. Передання персональних даних суб'єктів персональних даних третім особам визначається умовами згоди суб'єкта персональних даних на обробку його персональних даних або відповідно до вимог закону. Процедура передачі персональних даних Клієнтів Банку третім особам регулюється вимогами чинного законодавства та внутрішніми положеннями Банку з питань зберігання, обробки, захисту і розкриття інформації, що містить банківську таємницю.

Процедура передачі персональних даних працівників Банку третім особам регулюється нормами цього розділу Положення.

8.2. Передання персональних даних суб'єктів персональних даних третім особам допускається в мінімально необхідних обсягах і лише з метою виконання завдань, які відповідають об'єктивній причині збирання відповідних даних або згідно із чинним законодавством України.

- 8.2.1.1. Запит про надання персональних даних (надалі - Запит) що надходить до Банку поштою або нарочним шляхом, підлягає обов'язковій реєстрації в за правилами, встановленими для реєстрації вхідної кореспонденції. До Запиту обов'язково додається конверт, у якому надійшов Запит. У разі ушкодження конверта про це в журналі вхідної кореспонденції робиться запис у момент реєстрації вхідної кореспонденції.
- 8.2.1.2. Запит разом з конвертом, в якому він надійшов, передається працівником, що зареєстрував вхідну кореспонденцію в наступному порядку:
- Голові Правління або – Члену Правління Банку (відповідальному за юридичний супровід) – копія Запиту;
 - керівнику Управління заробітної плати і кадрового адміністрування (далі - УЗПКА) – оригінал Запиту;
 - керівнику Юридичного управління (далі – ЮУ) – копія Запиту;
 - керівнику Управління безпеки і охорони (далі – УБО) – копія Запиту.
- Копії Запиту можуть бути надані як в паперовому вигляді, так і засобами корпоративної електронної пошти у вигляді скан-копії.
- 8.2.1.3. Після отримання Запиту, відповідальний працівник УЗПКА протягом 3 (трьох) робочих днів з дати отримання Запиту аналізує наявність та обсяг відповідної інформації, що запитується. ЮУ протягом 3 (трьох) робочих днів вивчає наявність правових підстав для розкриття Банком інформації, що містить персональні дані та вивчає Запит стосовно дотримання відповідним державним органом вимог щодо його форми, змісту, порядку та обсягу розкриття інформації. УБО протягом 3 (трьох) робочих днів проводить перевірку Запиту та фіксує дані про Запит згідно внутрішніх положень Банку, зокрема стосовно інформаційної безпеки.
- 8.2.1.4. У разі відповідності Запиту вимогам чинного законодавства України та відсутності підстав для відмови у виконанні останнього УЗПКА сумісно з ЮУ, готує відповідь на Запит. Термін для підготовки інформації не повинен перевищувати 5 (п'ять) робочих днів з дати отримання Запиту.
- У разі, якщо за результатами вивчення Запиту встановлюється факт невідповідності даних, невідповідності форми та/або змісту Запиту вимогам чинного законодавства України або інші підстави, які свідчать про відсутність правових підстав щодо розкриття (повністю або частково) інформації, згідно Запиту, відповідь про відмову в наданні інформації, готується УЗПКА спільно з керівником ЮУ. Відповідь має обов'язково містити посилання на підстави для відмови в розкритті інформації, що містить персональні дані.
- Відповідь на Запит візується відповідальним працівником УЗПКА, а також, керівником ЮУ, керівником УБО та іншими відповідальними за надання інформації особами (у разі залучення до підготовки відповіді інших підрозділів Банку).
- Після цього, відповідь подається на підпис Голові Правління Банку, або – Члену Правління Банку (відповідальному за юридичний супровід).
- Підписана відповідь реєструється Банком з дотриманням вимог щодо реєстрації вихідної кореспонденції, що містить комерційну таємницю.
- 8.2.1.5. Надання уповноваженому державному органу в письмовій формі інформації, що містить персональні дані, або надання відповіді про відмову в розкритті інформації, що містить персональні дані здійснюється протягом 10 робочих днів з дня отримання Банком Запиту.

У виняткових випадках, якщо підготовка інформації потребує більше часу, ніж вищезазначений строк її надання, відповідальний за підготовку інформації працівник разом із керівником ЮУ, письмово повідомляє про це відповідний державний орган, який звернувся з вимогою про надання інформації, що містить банківську таємницю, і зазначають, у який строк цю інформацію буде надано.

8.3. Доступ до персональних даних третій особі не надається, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог Закону № 2297 або неспроможна їх забезпечити.

8.4. Без згоди суб'єкта персональних даних його персональні дані можуть передаватися у випадках:

- коли передача персональних даних прямо передбачена законодавством України і лише в інтересах національної безпеки, економічного добробуту та прав людини;
- отримання запиту від органів державної влади і місцевого самоврядування, що діють у межах повноважень, наданих законодавством України.

8.5. В інших, ніж зазначені у пункті 8.4, випадках персональні дані суб'єкта персональних даних можуть надаватися третім особам лише за підтвердженої згоди суб'єкта персональних даних.

8.6. Суб'єкти персональних даних мають право на одержання будь-яких відомостей про себе, що містяться у відповідних базах персональних даних, без зазначення мети запиту.

Суб'єкт відносин, пов'язаний з персональними даними, подає запит щодо доступу (далі - запит) до персональних даних володільцю персональних даних.

У запиті зазначаються:

- 1) прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит (для фізичної особи - заявника);
- 2) найменування, місцезнаходження юридичної особи, яка подає запит, посада, прізвище, ім'я та по батькові особи, яка засвідчує запит; підтвердження того, що зміст запиту відповідає повноваженням юридичної особи (для юридичної особи - заявника);
- 3) прізвище, ім'я та по батькові, а також інші відомості, що дають змогу ідентифікувати фізичну особу, стосовно якої робиться запит;
- 4) відомості про базу персональних даних, стосовно якої подається запит, чи відомості про володільця чи розпорядника персональних даних;
- 5) перелік персональних даних, що запитуються;
- 6) мета та/або правові підстави для запиту.

8.7. У разі смерті суб'єкта персональних даних його персональні дані можуть бути надані спадкоємцям першої черги (відповідно до законодавства України) за письмовим запитом після надання оригіналу свідоцтва про смерть.

9. Захист персональних даних при їх обробці

9.1. Захист персональних даних суб'єктів персональних даних в інформаційних системах Банку

9.1.1. Право доступу до інформаційних систем (далі по тексту – ІС) надається працівникам Банку, в посадових інструкціях яких передбачено функції з обробки даних у відповідних ІС та які надали письмове зобов'язання щодо нерозголошення персональних даних.

9.1.2. Працівники Банку допускаються до обробки персональних даних в ІС лише після їх ідентифікації (логін, пароль тощо).

9.1.3. Доступ осіб, які не пройшли процедуру ідентифікації, блокується.

9.1.4. Середовище, в якому розташовані відповідні ІС (комп'ютерне обладнання з операційною системою – сервери, робочі станції тощо), в обов'язковому порядку забезпечується антивірусним захистом.

9.1.5. При переведенні працівника на іншу посаду, яка не передбачає обробки персональних даних, або звільненні працівника, який мав право на обробку персональних даних в ІС, його права доступу до ІС переглядаються, змінюються / блокуються.

9.2. Захист персональних даних у формі картотек

9.2.1. До роботи з картотеками персональних даних допускаються лише працівники, у посадових інструкціях яких передбачено відповідні функції та які надали письмове зобов'язання щодо нерозголошення персональних даних.

9.2.2. Картотеки зберігаються у шафах і сейфах, що надійно зачиняються (з урахуванням вимог нормативно-правових актів, що регламентують ведення відповідних картотек).

10. Відповідальність

10.1. Відповідальний працівник з питань інформаційної безпеки несе відповідальність за організацію роботи, пов'язаної із захистом персональних даних у Банку, відповідно до положень даного документу.

10.2. Керівник юридичного управління несе відповідальність за виконання обов'язків Відповідальної особи (щодо організації роботи щодо контролю над розголошенням персональних даних у ПАТ «АП БАНК», взаємодії із перевіряючими органами щодо персональних даних, обробки відповідних запитів, що стосуються персональних даних в ПАТ «АП БАНК»), у разі відсутності відповідального працівника з питань інформаційної безпеки.

10.3. Управління заробітної плати і кадрового адміністрування несе відповідальність за обробку персональних даних працівників Банку, збереження та захист справ документів з питань обробки персональних даних працівників в межах своїх повноважень відповідно до положень даного документу.

10.4. Працівники інших підрозділів Банку, що виконують обробку персональних даних в рамках своїх службових посадових обов'язків, несуть відповідальність відповідно до положень даного документу.

11. Перегляд документа

11.1. Це Положення набирає чинності з моменту його затвердження рішенням Правління Банку.

11.2. Зміни та доповнення до цього Положення затверджуються рішенням Правління Банку. Причинами внесення змін до документу є можуть бути зміни у чинному законодавстві України, а також в організаційній, інформаційній інфраструктурі Банку та/або впровадженні нових інформаційних систем у Банку.

11.3. У випадку невідповідності будь-якої частини цього Положення чинному законодавству України або нормативним актам Національного банку України, у тому числі у зв'язку з прийняттям нових актів законодавства України або нових нормативних документів Національного банку України, це Положення діє лише в тій частині, яка не суперечить чинному законодавству України або нормативним актам Національного банку України, до моменту прийняття відповідних змін до Положення.

11.4. У разі необхідності це Положення переглядається та актуалізується з метою поліпшення ефективності внутрішніх банківських процедур.