Витяг з Положення про використання, зберігання та захист інформації з обмеженим доступом АТ «УНІВЕРСАЛ БАНК», затвердженого Рішенням Правління АТ «УНІВЕРСАЛ БАНК» протокол № 41 від «28» жовтня 2020 р.:

Порядок обробки та захисту персональних даних у АТ «УНІВЕРСАЛ БАНК»

1. Загальні правила та умови обробки персональних даних

1.1. Особисті немайнові права на персональні дані, які має кожна фізична особа, є невід'ємними і непорушними.

1.2. Захист персональних даних від незаконної обробки, у тому числі від втрати, незаконного або випадкового знищення, а також від незаконного доступу до них покладається на Володільця персональних даних.

1.3. Усі персональні дані, Володільцем яких є Банк, за режимом доступу є інформацією з обмеженим доступом.

1.4. Банк:

- вважає себе Володільцем персональних даних у випадку їхнього отримання безпосередньо у суб'єкта персональних даних;
- вважає себе Розпорядником персональних даних у разі, якщо інша особа передає персональні дані, та у договорі, що укладається з нею є пункт щодо ствердження нею як Стороною договору, що персональні дані, набуті та передаються Банку з дотриманням норм Закону та особа, що їх передає, бере на себе усі ризики, пов'язані з претензіями суб'єктів персональних даних до Банку;
- вважає інформацію надіслану електронною поштою, чи через веб-сайт (без безпосереднього запиту від Банку), як інформацію набуту з загальнодоступних джерел;
- не вважає візитки та корпоративні підписи як такі, що становлять персональні дані, оскільки таку інформацію надають працівникам Банку добровільно і без застережень, працівники користуються цими даними особисто, а не колективно.

1.5. Банк як володілець персональних даних Наказом Голови Правління Банку визначає:

- Мету та підстави обробки персональних даних, категорії суб'єктів персональних даних, склад персональних даних та порядок їх обробки відповідно до вимог Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14;
- відповідальну особу або структурний підрозділ, що задіяний у формуванні, обробці та захисті персональних даних;
- особу або структурний підрозділ, відповідальний за організацію роботи, пов'язаної із захистом персональних даних під час їх обробки.

1.6. Структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці:

- консультує володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних;
- інформує володільця або розпорядника персональних даних з приводу звернення до Уповноваженого Верховної Ради України з прав людини (далі – Уповноважений) про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних та визначеними ним посадовими особами його секретаріату щодо запобігання та усунення порушень законодавства про захист персональних даних, в т.ч. необхідності повідомлення Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних (у разі виникнення);
- документально фіксує факти порушень процесу обробки та захисту персональних даних та надає засобами корпоративної електронної пошти інформацію про них (копію акту, справки) Департаменту комплаєнс не пізніше наступного робочого дня.

Персональні дані, що становлять особливий ризик для прав і свобод суб'єктів, що стосуються:

- расового, етнічного та національного походження;
- політичного, релігійного або світоглядного переконання;
- членства в політичних партіях та/або організаціях, професійних спілках, релігійних організаціях чи в громадських організаціях світоглядної спрямованості;
- стану здоров'я;
- статевого життя;
- біометричних даних;
- генетичних даних;

- притягнення до адміністративної чи кримінальної відповідальності;
- застосування щодо особи заходів в рамках досудового розслідування;
- вжиття щодо особи заходів, передбачених Законом України "Про оперативно-розшукову діяльність";- вчинення щодо особи тих чи інших видів насильства;
- місцеперебування та/або шляхи пересування особи.

Уповноважений повідомляється про здійснення будь-яких видів обробки персональних даних, які становлять особливий ризик для прав і свобод суб'єктів персональних даних, крім випадків, якщо обробка необхідна для реалізації прав та виконання обов'язків володільця персональних даних у сфері трудових правовідносин відповідно до закону.

З метою повідомлення Уповноваженого володілець персональних даних подає до Секретаріату Уповноваженого заповнений бланк заяви за формою, наведеною в Порядку повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації, затвердженого Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14, в межах строків, встановлених Законом України "Про захист персональних даних" (далі – Закон).

1.7. Обробка персональних даних здійснюється Банком повністю або частково в електронній формі з використанням засобів інформаційної (автоматизованої) системи та/або у паперовій формі шляхом ведення картотек персональних даних. Обробка персональних даних здійснюється відкрито і прозоро із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки.

1.8. До персональних даних належать об’єктивні та суб’єктивні відомості про фізичну особу, що містяться в первинних та інших джерелах інформації про фізичну особу, в алфавітно-цифровому, графічному чи фото-форматі, аудіо/кіно/відео записах на паперових чи електронних носіях, щодо яких застосовуються загальні чи особливі вимоги обробки, що стосуються фізичної особи безпосередньо або відповідно до сукупності яких фізична особа може бути ідентифікована за допомогою реєстраційного номера облікової картки платника податків (ідентифікаційного номера) або одного чи більше факторів, притаманних фізичним, фізіологічним, розумовим, економічним, культурним чи соціальним аспектам її особистості, а саме:

- відомості, що ідентифікують або дають змогу ідентифікувати особу;
- відомості про грошові зобов'язання суб'єкта інформації;
- документована інформація про особу з державних реєстрів;
- інформація, добровільно надана суб’єктом персональних даних про себе, тощо, яка стала відома Банку у процесі обслуговування та/або взаємовідносин з таким суб’єктом чи третіми особами при наданні послуг.

1.9. Мінімальною сукупністю відомостей, що дають можливість ідентифікувати особу (ідентифікуючими даними) є: прізвище, ім’я та по-батькові особи разом з датою її народження або домашньою, поштовою чи електронною адресою, або номером телефону, або реєстраційним номером облікової картки платника податків.

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

- принцип законності: персональні дані повинні оброблятись лише на законних підставах;
- принцип сумісності: персональні дані повинні отримуватись із конкретними законними цілями, згідно із видами діяльності банку, передбаченими Законом України «Про банки та банківську діяльність» та оброблятись відповідно до них;
- принцип адекватності і не надлишковості: персональні дані повинні бути адекватними, не надлишковими (але в обсязі не менше, ніж передбачено фінансовим законодавством та банківським правилами), відповідати цілям обробки;
- принцип точності: персональні дані повинні бути точними та актуальними;
- принцип строковості зберігання: персональні дані не повинні зберігатися довше, ніж це передбачено згодою суб'єкта персональних даних та/або вимогами законів України та прийнятим на їх виконання нормативно-правових актів Національного банку України;
- принцип дотримання прав фізичної особи: персональні данні повинні оброблятись з дотриманням прав суб’єкта персональних даних, включаючи право на доступ до даних;
- принцип захищеності: персональні дані повинні оброблятись з дотриманням вимог щодо захисту даних;
- принцип транскордонної захищеності: персональні дані не повинні передаватись іноземним

суб'єктам відносин, пов'язаних із персональними даними, без належного захисту.

1.11. Загальними підставами виникнення права на обробку персональних даних є:
- згода суб'єкта персональних даних на обробку його персональних даних;
- дозвіл на обробку персональних даних, наданий Володільцю персональних даних відповідно до закону виключно для здійснення його повноважень;
- укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних;
- захист життєво важливих інтересів суб'єкта персональних даних;
- необхідність виконання обов'язку володільця персональних даних, який передбачений законом;
- необхідність захисту законних інтересів володільця персональних даних 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.

1.12. Відповідальні працівники надають суб'єкту персональних даних інформацію про мету обробки персональних даних до моменту отримання від цього суб'єкта згоди на таку обробку, окрім випадків, визначених законодавством.

1.13. У разі зміни визначеної мети обробки персональних даних на нову мету, яка є несумісною з попередньою, для подальшої обробки даних володілець персональних даних, окрім випадків, визначених законодавством, повинен отримати згоду суб'єкта персональних даних на обробку його даних відповідно до зміненої мети.

1.14. Керівники структурних підрозділів Банку, працівники яких здійснюють обробку персональних даних (далі - керівники) виключно у письмовій формі повідомляють суб'єкта персональних даних про склад і зміст зібраних персональних даних, його права, визначені Законом, мету збору персональних даних та третіх осіб, яким передаються його персональні дані, протягом тридцяти робочих днів з дня збору його персональних даних (або в момент збору персональних даних, якщо персональні дані збираються у суб'єкта персональних даних).

1.15. Повідомлення не здійснюється, якщо персональні дані збираються із загальнодоступних джерел.

1.16. Одні й ті самі персональні дані, які належать одному і тому ж суб'єкту персональних даних, можуть оброблятися одночасно в залежності від мети та строку обробки таких даних.

1.17. Зміни до персональних даних в обов'язковому порядку вносяться відповідальними працівниками на підставі вмотивованої письмової вимоги суб'єкта персональних даних. Зміни до персональних даних можуть вноситися також за зверненням інших суб'єктів відносин, пов'язаних із персональними даними, якщо на це є згода суб'єкта персональних даних або відповідна зміна здійснюється згідно з приписом Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого чи відповідна зміна здійснюється за рішенням суду, що набрало законної сили.

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

1.19. Поновлення персональних даних здійснюється відповідальними працівниками за згодою суб'єкта персональних даних відповідно до мети та підстав обробки персональних даних.

1.20. Про поновлення персональних даних керівники виключно у письмовій формі повідомляють суб'єкта персональних даних протягом десяти робочих днів з дня поновлення його персональних даних.

1.21. Обробка персональних даних у складі інформаційних (автоматизованих) систем здійснюється із використанням програмно-технічних засобів, що використовуються в Банку.

1.22. Банк зберігає персональні дані у строк не більше, ніж це необхідно відповідно до мети їх обробки, якщо інше не передбачено законодавством.

1.23. Особливості обробки персональних даних шляхом ведення відео спостереження, в тому числі з використанням відеозапису враховують вимоги чинного законодавства України. Банк використовує такий спосіб обробки даних в своїх приміщеннях та в банкоматах у відповідності до внутрішніх актів, які регулюють здійснення такої діяльності, включаючи строк обробки даних. Метою такої діяльності є забезпечення прав та законних інтересів Банку та зацікавлених осіб. Обробка персональних даних в такий спосіб може здійснюватись у складі інформаційно-телекомунікаційної системи із застосуванням засобів мережного захисту від несанкціонованого доступу під час обробки персональних даних. Банк здійснює відеоспостереження з повідомленням суб'єктів персональних даних про факт здійснення відеоспостереження шляхом розміщення відповідного застереження. Таке застереження розташовується в загальнодоступному місці для належного візуального сприйняття суб'єктом персональних даних до початку обробки його персональних даних в системах відеоспостереження та містить попередження про факт здійснення відеоспостереження.

1.24. Банк обробляє персональні дані у фото-форматі у відповідності до внутрішніх актів, які регулюють здійснення такої діяльності, включаючи строк обробки даних. Метою такої діяльності є забезпечення прав та законних інтересів Банку та зацікавлених осіб. Обробка персональних даних в такий спосіб може здійснюватись у складі інформаційно-телекомунікаційної системи Банку із застосуванням засобів

мережного захисту від несанкціонованого доступу під час обробки персональних даних. Банк отримує фотозображення суб'єкта персональних даних від самого суб'єкта персональних даних (наприклад, при оформленні на роботу), або створює фотозображення самостійно (при наданні банківських послуг, якщо це передбачено умовами надання послуг). Така діяльність здійснюється Банком на підставі законодавства (наприклад, при оформленні на роботу) або на підставі згоди суб'єкта персональних даних. Фотозображення також може бути розповсюджене без дозволу фізичної особи, яка зображена на ній, якщо це викликано необхідністю захисту її інтересів або інтересів інших осіб відповідно до статті 308 Цивільного кодексу України.

1.25. Банк може обробляти персональні дані в аудіо-форматі у відповідності до внутрішніх нормативних документів, які регулюють здійснення такої діяльності, включаючи строк обробки даних. Метою такої діяльності є забезпечення прав та законних інтересів Банку та зацікавлених осіб. Обробка персональних даних в такий спосіб може здійснюватись у складі інформаційно-телекомунікаційної системи із застосуванням засобів мережного захисту від несанкціонованого доступу під час обробки персональних даних. Банк може здійснювати аудіозапис розмов з використанням телекомунікацій за умови повідомлення суб'єктів персональних даних про факт здійснення аудіозапису шляхом усного застереження. В такому випадку згода суб'єкта персональних даних на обробку його персональних даних, що міститимуться в аудіозапису, також отримується усно. Банк виходить з того, що суб'єкт персональних даних, який не згоден з аудіофіксацією розмови, має змогу не продовжувати спілкування з представником Банку після отримання повідомлення про аудіозапис.

1.26. Керівники, працівники яких здійснюють обробку персональних даних, відповідно до покладених завдань:

- забезпечують ознайомлення працівників відповідного структурного підрозділу Банку з вимогами законодавства про захист персональних даних, зокрема, щодо їхнього обов'язку не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали їм відомі у зв'язку з виконанням професійних, службових чи трудових обов'язків;
- забезпечують організацію обробки та захисту персональних даних працівниками відповідного структурного підрозділу Банку відповідно до їх професійних, службових чи трудових обов'язків в обсязі, необхідному для виконання таких обов'язків;
- забезпечують внесення змін до посадових інструкцій працівників, виконання професійних обов'язків яких пов'язане з обробкою персональних даних.
- організовують роботу з обробки запитів щодо доступу до персональних даних суб'єктів відносин, пов'язаних з обробкою персональних даних;
- забезпечують доступ суб'єктів персональних даних до власних персональних даних;
- інформують керівництво Банку про заходи, яких необхідно вжити для приведення складу персональних даних та процедур їх обробки у відповідності до Закону України «Про захист персональних даних» (далі - Закон) й про порушення встановлених процедур з обробки персональних даних;
- ведуть облік операцій, пов'язаних з обробкою персональних даних суб'єкта персональних даних та доступом до них.

1.27. Доступ до обробки персональних даних мають працівники структурних підрозділів в частині персональних даних, обробка яких передбачена їх професійними, трудовими чи службовими обов'язками.

2. Використання та поширення персональних даних

2.1. Використання персональних даних здійснюється за умови забезпечення захисту цих даних. Забороняється розголошувати відомості стосовно суб'єктів персональних даних, доступ до персональних даних яких надається іншим суб'єктам відносин, пов'язаних з такими даними.

2.2. Використання персональних даних працівниками здійснюється лише відповідно до їхніх професійних чи службових або трудових обов'язків.

2.3. Ці працівники зобов'язані не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків. Таке зобов'язання чинне після припинення ними діяльності, пов'язаної з персональними даними, крім випадків, установлених законом.

2.4. Відомості про особисте життя фізичної особи не можуть використовуватися як чинник, що підтверджує чи спростовує її ділові якості.

2.5. Право на використання персональних даних виникає з підстав, передбачених Законом.

2.6. Поширення персональних даних дозволяється за згодою суб'єкта персональних даних.

2.7. Працівники, задіяні в обробці персональних даних, зобов'язані отримати у суб'єкта персональних даних згоду на поширення його персональних даних.

2.8. Згода на поширення персональних даних надається суб'єктом персональних даних у письмовій формі.

2.9. Поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

2.10. Третя особа, якій передаються персональні дані, повинна попередньо вжити заходів щодо забезпечення вимог Закону.
2.11. З метою отримання доступу до персональних даних третя особа надає в письмовій формі зобов'язання дотримуватися вимог Закону та забезпечувати захист персональних даних.
2.12. Доступ до персональних даних третій особі не надається, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог Закону або неспроможна їх забезпечити.
2.13. Порядок доступу до персональних даних третіх осіб визначається умовами згоди суб'єкта персональних даних, наданої Банку на обробку цих даних, або відповідно до вимог закону.
2.14. Суб'єкт відносин, пов'язаних з персональними даними, подає до Банку запит щодо доступу (далі - запит) до персональних даних.
2.15. У запиті зазначаються:
- прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит (для фізичної особи - заявника);
- 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);
- прізвище, ім'я та по батькові, а також інші відомості, що дають змогу ідентифікувати фізичну особу, стосовно якої робиться запит;
- відомості про персональні дані, стосовно яких подається запит, чи відомості про володільця чи розпорядника персональних даних;
- перелік персональних даних, що запитуються;
- мета та/або правові підстави для запиту.

2.16. Строк вивчення запиту на предмет його задоволення не може перевищувати десяти робочих днів з дня його надходження.
2.17. Протягом цього строку керівники структурних підрозділів Банку доводять до відома особи, яка подає запит, що запит буде задоволено або відповідні персональні дані не підлягають наданню, із зазначенням підстави, визначеної у відповідному нормативно-правовому акті.
2.18. Запит задовольняється протягом тридцяти календарних днів з дня його надходження, якщо інше не передбачено законом.
2.19. Суб'єкт персональних даних має право на одержання будь-яких відомостей про себе у будь-якого суб'єкта відносин, пов'язаних з персональними даними, без зазначення мети запиту, крім випадків, установлених законом.
2.20. Відстрочення доступу суб'єкта персональних даних до своїх персональних даних не допускається.
2.21. Відстрочення доступу до персональних даних третіх осіб допускається у разі, якщо необхідні дані не можуть бути надані протягом тридцяти календарних днів з дня надходження запиту. При цьому загальний термін вирішення питань, порушених у запиті, не може перевищувати сорока п'яти календарних днів.
2.22. Повідомлення про відстрочення доводиться до відома третьої особи, яка подала запит, у письмовій формі з роз'ясненням порядку оскарження такого рішення.
2.23. У повідомленні про відстрочення зазначаються:
- прізвище, ім'я та по батькові посадової особи;
- дата відправлення повідомлення;
- причина відстрочення;
- строк, протягом якого буде задоволено запит.

2.24. Відмова у доступі до персональних даних допускається, якщо доступ до них заборонено згідно із Законом.
2.25. У повідомленні про відмову зазначаються:
- прізвище, ім'я, по батькові посадової особи, яка відмовляє у доступі;
- дата відправлення повідомлення;
- причина відмови.

2.26. Рішення Банку про відстрочення або відмову в доступі до персональних даних може бути оскаржено в порядку, встановленому Законом.
2.27. Доступ суб'єкта персональних даних до даних про себе здійснюється безоплатно.
2.28. Доступ інших суб'єктів відносин, пов'язаних з персональними даними, до персональних даних певної фізичної особи чи групи фізичних осіб може бути платним у разі додержання умов, визначених Законом. Оплаті підлягає робота, пов'язана з обробкою персональних даних, а також робота з консультування та організації доступу до відповідних даних.
2.29. Органи державної влади та органи місцевого самоврядування мають право на безперешкодний і безоплатний доступ до персональних даних відповідно до їх повноважень.
2.30. Знеособлення персональних даних здійснюється відповідальними працівниками в порядку, передбаченому чинним законодавством.

3. Зберігання та знищення персональних даних

3.1. Персональні дані зберігаються у строк не більше, ніж це необхідно відповідно до мети їх обробки, якщо інше не передбачено законодавством.
3.2. Персональні дані зберігаються в структурних підрозділів, в яких вони обробляються.
3.3. Персональні дані знищуються відповідно до вимог Закону.
3.4. Персональні дані підлягають видаленню або знищенню у разі:
- закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом;
- припинення правовідносин між суб'єктом персональних даних та Банком, якщо інше не передбачено законом;
- видання відповідного припису Уповноваженого Верховної Ради України з прав людини (далі - Уповноважений) або визначених ним посадових осіб секретаріату Уповноваженого Верховної Ради України з прав людини;
- набрання законної сили рішенням суду щодо видалення або знищення персональних даних.

3.5. Персональні дані, зібрані з порушенням вимог Закону, підлягають знищенню у встановленому законодавством порядку.
3.6. Знищення персональних даних здійснюється у спосіб, що виключає подальшу можливість поновлення таких персональних даних.
3.7. Знищення персональних даних у формі картотек здійснюється шляхом спалювання або подрібнення, яке унеможливлює поновлення документа.
3.8. Знищення персональних даних в складі інформаційної (автоматизованої) системи здійснюється за допомогою системи управління персональними даними, що виключає можливість поновлення видаленої інформації.
3.9. З метою знищення персональних даних наказом керівника Банку створюється комісія.
3.10. До складу комісії зі знищення персональних даних входять: голова комісії – керівник відповідного структурного підрозділу та члени комісії: відповідальний працівник відповідного структурного підрозділу, працівник операційного департаменту або іншого структурного підрозділу задіяного в обробці персональних даних, що підлягають знищенню.
3.11. Про знищення персональних даних у формі картотек складається Акт про знищення персональних даних у формі картотек (зразок акту приведено у розділі 7 цього Додатку).
3.12. Про знищення персональних даних в складі інформаційної (автоматизованої) системи складається Акт про знищення персональних даних у складі інформаційної (автоматизованої) системи (зразок акту приведено у розділі 7 цього Додатку).
3.13. Акт про знищення персональних даних зберігається у відповідному структурному підрозділі Банку.
3.14. Про зміну чи знищення персональних даних або обмеження доступу до них керівники протягом десяти робочих днів повідомляють суб'єкта персональних даних, а також суб'єктів відносин, пов'язаних із персональними даними, яким ці дані було передано.

4. Обробка персональних даних в складі інформаційної (автоматизованої) системи

4.1. Банк обробляє персональні дані в складі інформаційної (автоматизованої) системи, в якій забезпечується захист персональних даних відповідно до вимог закону.
4.2. Обробка персональних даних в інформаційній (автоматизованій) системі може здійснюватись у складі інформаційно-телекомунікаційної системи із застосуванням засобів мережевого захисту від несанкціонованого доступу під час обробки персональних даних.
4.3. Працівники структурних підрозділів Банку допускаються до обробки персональних даних лише після їх авторизації.
4.4. Доступ осіб, які не пройшли процедуру ідентифікації та/або автентифікації, повинен блокуватись.
4.5. Інформацію, що містить персональні дані вносять працівники відповідних структурних підрозділів Банку, задіяні у обробці персональних даних (надалі – відповідальні працівники), на підставі первинних документів, які подаються суб'єктами персональних даних в установленому порядку, та відомостей, які суб'єкт персональних даних надає про себе.

5. Обробка персональних даних у формі картотек

5.1. Банк здійснює обробку персональних даних у картотеках у порядку, визначеному Законом та цим Положенням , з урахуванням таких вимог:
- документи, що містять персональні дані, формуються у справи залежно від мети обробки персональних даних;
- справи з документами, що містять персональні дані, повинні мати внутрішні описи документів із зазначенням мети обробки і категорії персональних даних;
- картотеки зберігаються у приміщеннях (шафах, сейфах), захищених від несанкціонованого доступу.

5.2. Двері у приміщеннях (шафах, сейфах) повинні бути обладнані замком або контролем доступу.

6. Захист персональних даних

6.1. На дії Банку поширюються усі вимоги щодо захисту персональних даних від незаконної обробки, а також від незаконного доступу до них.

6.2. Персональні дані у електронній формі повинні бути захищеними від незаконної обробки, а також від незаконного доступу до них. Відповідальними за захист персональних даних у електронній формі в межах своєї компетенції є керівники структурних підрозділів задіяних у формуванні та обробці персональних даних, працівники управління інформаційних технологій, відділу інформаційної безпеки.

6.3. Відповідальними за організаційний захист персональних даних при їх обробці та технічний захист персональних даних при їх обробці у формі картотек є керівники структурних підрозділів Банку, працівники яких здійснюють обробку персональних даних.

6.4. Відповідний структурний підрозділ з інформаційно-комп'ютерного забезпечення забезпечує антивірусний захист в інформаційній (автоматизованій) системі та використання технічних засобів безперебійного живлення елементів інформаційної (автоматизованої) системи.

6.5. В інформаційній (автоматизованій) системі, де обробляються персональні дані, може здійснюватись реєстрація, зокрема:

- 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

6.6. Відповідальна особа та/або структурний підрозділ може проводити аналіз реєстраційних даних.

6.7. Реєстраційні дані захищаються від модифікації та знищення.

6.8. Реєстраційні дані повинні зберігатися та надаватися за вмотивованою вимогою для аналізу суб'єктам відносин, пов'язаним із персональними даними.

6.9. Відповідальним за захист персональних даних, що містяться у документах Банку, які передані на зберігання до архіву є працівник архіву, який згідно з посадовою інструкцією забезпечує дотримання порядку користування архівними документами.

7. Зразки актів про знищення персональних даних.

АКТ № _____
про знищення персональних даних у формі картотек

«__» _____ 20___ р. м.
Київ

Комісія, створена наказом Голови Правління від «__» _____ 20___ р. № ____, у складі:

Голова комісії _____
(посада, прізвище та ініціали)
Член комісії _____
(посада, прізвище та ініціали)
Член комісії _____
(посада, прізвище та ініціали)

склала цей акт про те, що «__» _____ 20___ р. було проведено знищення персональних даних у формі картотек.

Підстава для знищення: _____

Усього комісією знищено шляхом

_____
зазначити вид знищення: спалювання або подрібнення документи, які містять персональні дані,

у кількості _____ (_____)одиниць.
зазначити цифрами зазначити словами

Знищено такі документи:

№ з/п	Назва документа	Персональні дані, які містить документ

Голова комісії _____ _____
(підпис) (прізвище, ініціали)
Член комісії _____ _____
(підпис) (прізвище, ініціали)
Член комісії _____ _____
(підпис) (прізвище, ініціали)

АКТ №____
про знищення персональних даних в складі інформаційної (автоматизованої) системи

«__» _____ 20___ р. м. Київ

Комісія, створена наказом Голови Правління від «__» _____ 20___ р. № ____, у складі:

Голова комісії _____
(посада, прізвище та ініціали)
Член комісії _____
(посада, прізвище та ініціали)
Член комісії _____
(посада, прізвище та ініціали)

склала цей акт про те, що «__» _____ 20___ р. було проведено знищення персональних даних в складі інформаційної (автоматизованої) системи.

Підстава для знищення: _____

Усього комісією знищено за допомогою системи управління базами даних записи, які містять персональні дані, у кількості _____ (_____)одиниць.
зазначити цифрами зазначити словами

Знищено такі записи:

№ з/п	Назва запису	Персональні дані, які містить запис

Голова комісії _____ _____
(підпис) (прізвище, ініціали)
Член комісії _____ _____
(підпис) (прізвище, ініціали)
Член комісії _____ _____
(підпис) (прізвище, ініціали)