

ЗАГАЛЬНІ УМОВИ ДО ДОГОВОРІВ, ЯКІ УКЛАДЕНІ З АТ «ОТП БАНК» (ПУБЛІЧНІ)	GENERAL CONDITIONS TO CONTRACTS AND AGREEMENTS CONCLUDED WITH OTP BANK JSC (PUBLIC)
(редакція діє з 25.02.2022 року)	(edition is valid from 25.02.2022)
ЗМІСТ:	CONTENT:
1. ВИЗНАЧЕННЯ ЗАГАЛЬНИХ ТЕРМІНІВ	1. DEFINITION OF GENERAL TERMS
2. ЗАГАЛЬНІ ПОЛОЖЕННЯ	2. GENERAL
3. ПРАВА, ОБОВ'ЯЗКИ ТА ВІДПОВІДАЛЬНІСТЬ СТОРИН (ЗАГАЛЬНІ)	3. RIGHTS, OBLIGATIONS AND RESPONSIBILITY OF THE PARTIES (GENERAL)
3.1. ПРАВА КОНТРАГЕНТА	3.1. COUNTERPARTY'S RIGHTS
3.2. ОБОВ'ЯЗКИ КОНТРАГЕНТА	3.2. COUNTERPARTY'S OBLIGATIONS
3.3. ПРАВА БАНКУ	3.3. BANK'S RIGHTS
3.4. ОБОВ'ЯЗКИ БАНКУ	3.4. BANK'S OBLIGATIONS
3.5. ВІДПОВІДАЛЬНІСТЬ КОНТРАГЕНТА	3.5. COUNTERPARTY'S LIABILITY
3.6. ВІДПОВІДАЛЬНІСТЬ БАНКУ	3.6. BANK'S LIABILITY
4. УМОВИ ТА ОСОБЛИВОСТІ ВИКОНАННЯ ОКРЕМИХ ДОГОВОРІВ:	4. CONDITIONS AND PARTICULARS OF FULFILLMENT OF CERTAIN AGREEMENTS:
4.1. ДОГОВІР ПРО НЕРОЗГОЛОШЕННЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ	4.1. RESTRICTED INFORMATION NON-DISCLOSURE AGREEMENT
4.2. ДОГОВІР ПРО ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ	4.2. ELECTRONIC DOCUMENT CIRCULATION AGREEMENT
5. ВИКОРИСТАННЯ КВАЛІФІКОВАНОГО ЕЛЕКТРОННОГО ПІДПИСУ	5. QUALIFIED E-SIGNATURE USE
6. ВАЛЮТНІ ЗАСТЕРЕЖЕННЯ	6. FOREIGN CURRENCY CLAUSE
7. ДОГОВІРНЕ СПИСАННЯ	7. DIRECT DEBIT TRANSFER
8. ПОВІДОМЛЕННЯ	8. NOTICES
9. КОНФІДЕНЦІЙНІСТЬ. БАНКІВСЬКА ТАЄМНИЦЯ	9. CONFIDENTIALITY. BANKING SECRECY
10. ВРЕГУЛЮВАННЯ СПОРІВ	10. RESOLUTION OF DISPUTES
11. ЗВІЛЬНЕННЯ ВІД ВІДПОВІДАЛЬНОСТІ. ФОРС- МАЖОР (НЕПЕРЕБОРНА СИЛА)	11. RELEASE FROM LIABILITY. FORCE-MAJEURE (ACTS OF GOD)
12. ФІНАНСОВИЙ МОНІТОРИНГ	12. FINANCIAL MONITORING
13. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ	13. PERSONAL DATA PROTECTION
14. СТРОК ДІЇ ДОГОВОРУ. ЗМІНИ ТА РОЗІРВАННЯ ДОГОВОРУ/ ЗАГАЛЬНИХ УМОВ	14. TERM OF THE AGREEMENT. AMENDMENTS AND TERMINATION OF THE AGREEMENT / GENERAL TERMS AND CONDITIONS
1. ВИЗНАЧЕННЯ ЗАГАЛЬНИХ ТЕРМІНІВ	1. DEFINITION OF GENERAL TERMS
Банк - АТ «ОТП БАНК» та будь-які його структурні підрозділи на території України. Сторона за Договором.	Bank shall mean OTP BANK JSC and any its structural divisions in Ukraine, the party to the Agreement.
Боргові зобов'язання - всі та/або кожне з платіжних (грошових) та/або неплатіжних (не грошового характеру) зобов'язань Контрагента, згідно Договору та/або у зв'язку з Договором.	Debt obligations shall mean all and/or each of payment (monetary) and/or non-payment (non-monetary) obligations of the Counterparty under the Agreement and/or in relation thereto.
Договір - письмова домовленість між Банком та Контрагент-ом/-ами, спрямована на встановлення, зміну або припинення цивільних та/або господарських прав та обов'язків, який є невід'ємною частиною ЗАГАЛЬНИХ УМОВ ДО ДОГОВОРІВ, ЯКІ УКЛАДЕНІ З АТ «ОТП БАНК» (ПУБЛІЧНІ). Договір складається із 2-х частин: індивідуальної та публічної. Перелік Договорів, які можуть бути укладені з приєднанням до Загальних Умов, визначені у розділі 4 цих Загальних Умов.	Agreement shall mean a written agreement between the Bank and the Counterparty(-ies) aimed to establish, change or terminate civil and/or economic rights and obligations, which forms an integral part of GENERAL CONDITIONS TO CONTRACTS AND AGREEMENTS CONCLUDED WITH OTP BANK JSC. The Agreement shall consist of two parts: individual and public. The list of Agreements that can be concluded with accession to the General Conditions is defined in Section 4 of these General Conditions.

Законодавство - чинне законодавство України.	Legislation shall mean the effective legislation of Ukraine.
Загальні Умови – ЗАГАЛЬНІ УМОВИ ДО ДОГОВОРІВ, ЯКІ УКЛАДЕНІ З АТ «ОТП БАНК» (ПУБЛІЧНІ), які є невід’ємною частиною Договору та розміщені на Офіційному сайті Банку.	General conditions shall mean the GENERAL CONDITIONS TO CONTRACTS AND AGREEMENTS CONCLUDED WITH OTP BANK JSC, which form an integral part of the Agreement and places on the Bank’s official web-site.
НБУ – Національний банк України.	NBU shall mean the National Bank of Ukraine.
Контрагент – сторона за Договором, будь-яка фізична особа (резидент або нерезидент) та/або фізична особа-підприємець, та/або юридична особа (резидент або нерезидент), та/або іноземне представництво та/або постійне представництво, з яким Банк уклав Договір. Контрагент є відповідною Стороною по зазначеному Договору (зокрема, але не виключно в індивідуальній частині Договору може іменуватися як: Контрагент, Користувач, Виконавець, Орендар, Орендодавець, Суборендар, Суборендодавець, Замовник, Партнер, Покупець, Продавець, Клієнт, Підрядник, Постачальник, Страхова компанія і т.д.).	Counterparty shall mean a party to the Agreement, any physical person (resident and non-resident) and/or the self-employed person, and/or legal entity (resident and non-resident), and/or foreign representation office, and/or permanent representation office the Bank concluded the Agreement with. The Counterparty shall be the relevant Party to the stated Agreement (which, in particular, but not limited by the individual part of the Agreement, may be referred to as the Counterparty, User, Provider, Lessee, Lessor, Sublessee, Sublessor, Customer, Partner, Buyer, Seller, Client, Contractor, Supplier, Insurance Company etc.).
Офіційний сайт Банку – www.otpbank.com.ua	Bank’s official site shall mean www.otpbank.com.ua
Сторона/Сторони – відповідна сторона/сторони за Договором: Банк та/або Контрагент/-и.	Party/Parties shall mean the relevant party/parties to the Agreement: Bank and/or Counterparty(-ies).
<i>Терміни, що використовуються в Договорі з великої літери, є визначеними термінами і мають однакові значення, як у індивідуальній частині Договору, так і у Загальних Умовах, та можуть використовуватись, як в однині, так і в множині.</i>	<i>Capitalized terms used herein shall be the defined terms and have similar meaning both in the individual part of the Agreement and the General Conditions and may be sued both in singular and plural.</i>
2. ЗАГАЛЬНІ ПОЛОЖЕННЯ	2. GENERAL
2.1. Ці ЗАГАЛЬНІ УМОВИ ДО ДОГОВОРІВ, ЯКІ УКЛАДЕНІ З АТ «ОТП БАНК» (ПУБЛІЧНІ) (надалі – Загальні Умови), є невід’ємною та публічною частиною Договору, що укладається між Банком та Контрагентом. 2.2. Укладений Сторонами Договір містить елементи різних правовідносин та є змішаним договором в розумінні статті 628 Цивільного кодексу України. 2.3. Індивідуальна частина Договору – є договором приєднання в розумінні статті 634 Цивільного кодексу України. Шляхом підписання Контрагентом індивідуальної частини Договору, Контрагент приєднується до публічної частини Договору – Загальних Умов. 2.4. Загальні Умови застосовуються з врахуванням умов Договору, що укладений між Банком та Контрагентом. 2.5. Якщо положення індивідуальної частини Договору суперечать положенням Загальних Умов, для врегулювання відносин між Банком та Контрагентом застосовуються положення індивідуальної частини Договору. 2.6. Укладення Договору відповідає вільному волевиявленню Сторін, жодна з Сторін не знаходиться під впливом тяжких обставин, не помиляється стосовно обставин, що мають суттєве значення (природа Договору, права та обов’язки Сторін, інші умови Договору), та умови Договору є взаємовигідними для кожної із Сторін. 2.7. Мовою викладення індивідуальної частини Договору може бути українська або українська з англійською.	2.1. These GENERAL CONDITIONS TO CONTRACTS AND AGREEMENTS CONCLUDED WITH JSC OTP BANK (PUBLIC) (hereinafter referred to as the General Conditions) shall form an integral and public part of the Agreement to be concluded between the Bank and the Counterparty. 2.2. The Agreement concluded between the Parties shall contain the elements of various legal relations and shall be the mixed contract in the meaning of article 628 of the Civil Code of Ukraine. 2.3. The individual part of the Agreement shall mean the accession agreement in the meaning of article 634 of the Civil Code of Ukraine. By signing the individual part of the Agreement the Counterparty shall accede to the public part of the Agreement (General Conditions). 2.4. The General Conditions shall apply in view of the terms and conditions of the Agreement concluded between the Bank and the Counterparty. 2.5. If provisions of the individual part are contrary to the provisions of the General Conditions, the provisions of the individual part of the Agreement shall apply to settle relations between the Bank and the Counterparty. 2.6. Conclusion of the Agreement shall comply with the Parties’ will. Neither Party is influenced by severe circumstances, is mistaken about the significant circumstances (nature of the Agreement, rights and obligations of the Parties, other conditions of the

Мовою викладення публічної частини Договору (Загальних Умов) є українська з англійською. У випадку виникнення розбіжностей між україномовною та англійськомовною версіями, текст українською мовою матиме перевагу. 2.8. Шляхом підписання індивідуальної частини Договору, Контрагент підтверджує, що він особисто отримав свій примірник Договору, умови Договору йому зрозумілі; з Договором, Загальними Умовами ознайомлений, приймає та погоджується з їх положеннями, а також зобов'язується їх належно та неухильно виконувати, а також безумовно стверджує, що не позбавляється будь-яких прав, які має звичайно, а Договір не містить умов, які є для нього обтяжливими у будь-якому сенсі. 2.9. Взаємні права і обов'язки Банку та Контрагента за Договором виникають з моменту підписання Сторонами індивідуальної частини Договору. Договір зберігає свою дію при будь-якому перейменуванні, зміні місцезнаходження чи інших реквізитів Сторони, а також для будь-яких правонаступників, утворених в результаті можливої реорганізації Сторони. 2.10. Визнання недійсним будь-якої частини Договору/Загальних Умов не тягне за собою недійсності Договору/Загальних Умов в цілому. Визнання недійсним Договору не тягне за собою недійсності зобов'язань, які виникли між Сторонами на підставі обміну документами, що містять істотні умови Договору. 2.11. В тексті Договору, якщо інше не вимагається контекстом, заголовки розділів вміщено лише для зручності та вони жодним чином не впливають на тлумачення Договору; вжиті слова мають однакове значення як в однині, так і в множині; посилання на додаток, розділ, доповнення або пункт є посиланням на відповідний додаток, розділ, доповнення або пункт Договору; посилання на Сторону або будь-яку іншу особу включає також її правонаступників, дозволених цесіонаріїв і правонабувачів; посилання на третю особу включає будь-яку(их) особу(ів), в тому числі будь-яку фізичну особу та/або юридичну особу, яка(і) не є Стороною(-ами). 2.12. Договір підписаний в кількості примірників із розрахунку один примірник для кожної Сторони, кожен з яких є оригіналом. Будь-які підчистки, дописки, закреслені слова чи інші виправлення, окрім вчинення підписів уповноваженими особами за Договором, мають силу лише у разі, якщо вони були застережені підписами уповноважених осіб Сторін та відбитками печаток (у випадку наявності) Сторін. При цьому виправлення повинні бути зроблені таким чином, щоб можна було прочитати як виправлене, так і помилково написане, а потім виправлене чи викреслене.	Agreement) and the terms and conditions of the Agreement are mutually beneficial for each of the Parties. 2.7. The individual part of the Agreement may be prepared in Ukrainian or Ukrainian and English. The public part of the Agreement (General Conditions) shall be prepared in Ukrainian and English. In case of discrepancies between the Ukrainian and English versions the Ukrainian version shall prevail. 2.8. By signing the individual part of the Agreement the Counterparty acknowledges that he has received the copy of the Agreement and understands its conditions, that he has studied the Agreement and General Conditions, accepts and consents to the provisions thereof and also undertakes to fulfill the same and unconditionally declares that he shall not be deprived of any rights granted thereto and that the Agreement has no conditions in any way burdensome for him. 2.9. Mutual rights and obligations of the Bank and the Counterparty hereunder shall arise from the date of signing the individual part of the Agreement by the Parties. The Agreement shall remain valid in case of any change in the name, location or other details of the Parties and for any legal successors resulting from potential reorganization of the Party. 2.10. Invalidity of any part of the Agreement/General Conditions shall not result in invalidity of the Agreement/General Conditions in whole. Invalidity of the Agreement shall not invalidate obligations arisen between the Parties due to exchange of documents with material conditions of the Agreement. 2.11. In the Agreement, unless otherwise required by the context, heading of the sections shall be for convenience only and shall not affect interpretation thereof. Words used shall have the same meaning both in singular and plural. References to the annex, section, appendix or clause shall mean references to the relevant annex, section, appendix or clause of the Agreement. References to a Party or any other person shall also include legal successors, assigns and transferees. References to any third party shall include references to any person(-s), including any physical person and/or legal entity not being the Party(-ies). 2.12. The Agreement shall be signed in a number of copies assuming one copy for each Party, each of them is an original. Any erasures, additions, crossed out words and other corrections, except for those made by authorized persons under the Agreement, shall have effect if only they have been evidenced by signatures of the authorized representatives and seals (if any) of the Parties. In this case corrections shall be made so that the corrected and erroneously written words and thereafter the corrected or crossed out words are legible.
3. ПРАВА, ОБОВ'ЯЗКИ ТА ВІДПОВІДАЛЬНІСТЬ СТОРІН (ЗАГАЛЬНІ)	3. RIGHTS, OBLIGATIONS AND LIABILITY OF THE PARTIES (GENERAL)
Крім прав, обов'язків та відповідальності Сторін, визначених індивідуальною частиною Договору та відповідним пунктом розділу «4. ЗАГАЛЬНІ УМОВИ ТА	Except for the rights, obligations and responsibility of the Parties determined in the individual part of the Agreement and the relevant section 4. GENERAL CONDITIONS AND

ОСОБЛИВОСТІ ВИКОНАННЯ ОКРЕМИХ ДОГОВОРІВ» Загальних Умов, Сторони також домовились про наступне:	PARTICULARS OF FULFILLMENT OF CERTAIN AGREEMENTS' of the General Conditions, the Parties also agreed as follows:
3.1. ПРАВА КОНТРАГЕНТА	3.1. COUNTERPARTY'S RIGHTS
3.1.1. Контрагент має право вимагати виконання Банком умов Договору. 3.1.2. Контрагент має право достроково розірвати Договір у порядку, визначеному публічною частиною Договору (Загальними Умовами), якщо інше не визначено Сторонами в індивідуальній частині Договору. 3.1.3. Контрагент протягом строку дії Договору має право запросити у Банку установчі документи та підтвердження повноважень осіб, які підписують будь-які документи, пов'язані з Договором.	3.1.1. The Counterparty shall have the right to require fulfillment of the terms and conditions of the Agreement by the Bank. 3.1.2. The Counterparty shall have the right to early termination of the Agreement as stipulated by the public part of the Agreement (General Conditions) unless otherwise determined in the individual part of the Agreement by the Parties. 3.1.3. The Counterparty shall, within the term of the Agreement, have the right to require constituent documents from the Bank and proof of powers and authorities of the signatories to any documents related to the Agreement.
3.2. ОBOB'ЯЗКИ КОНТРАГЕНТА	3.2. COUNTERPARTY'S OBLIGATIONS
3.2.1. Контрагент зобов'язується без зволікань інформувати Банк про обставини, які мають значення для виконання умов Договору, у тому числі про зміну адрес та банківських реквізитів, перейменування, прийняття рішення про ліквідацію, реорганізацію або початок процедури банкрутства, прийняття рішення щодо визнання Контрагента неплатоспроможним у строк не пізніше 10-ти календарних днів із дня вступу таких змін в силу / прийняття такого рішення, у порядку, визначеного Сторонами у розділі «8. Повідомлення» Загальних Умов. 3.2.2. Контрагент зобов'язується самостійно ознайомлюватися з повідомленнями Банку та/або змінами/доповненнями до публічної частини Договору (Загальних Умов), що розміщуються на Офіційному сайті Банку, але не рідше ніж 1 раз на місяць. 3.2.3. Контрагент не має права передавати свої права і зобов'язання по Договору третім особам без письмової згоди Банку, якщо інше не визначене індивідуальною частиною Договору. 3.2.4. Контрагент зобов'язується протягом строку дії Договору, на запит Банку надавати установчі документи та підтвердження повноважень осіб, які підписують будь-які документи, пов'язані з Договором.	3.2.1. The Counterparty shall undertake to immediately notify the Bank of any circumstances significant for fulfillment of the terms and conditions of the Agreement including change in the address, banking details and its name, decision adopted to liquidate, reorganize or commence the bankruptcy proceedings, to recognize insolvency of the Counterparty within the period not exceeding 10 calendar days from the effective date of such changes/decision as stipulated by the Parties in Section 8 (Notices) of the General Conditions. 3.2.2. The Counterparty shall undertake to carry out independent study of the notices of the Bank and/or amendments/supplements to the public part of the Agreement (General Conditions) placed on the Bank's official web-site but not less than once in a month. 3.2.3. The Counterparty shall have no right to assign its rights and obligations under the Agreement to any third parties without the written consent of the Bank unless otherwise determined in the individual part of the Agreement. 3.2.4. The Counterparty shall undertake to provide constituent documents and proof of powers and authorities of the signatories to any documents related to the Agreement as requested by the Bank.
3.3. ПРАВА БАНКУ	3.3. BANK'S RIGHTS
3.3.1. Банк має право вимагати виконання Контрагентом умов Договору. 3.3.2. Банк має право достроково розірвати Договір у порядку, визначеному публічною частиною Договору (Загальними Умовами), якщо інше не визначено Сторонами в індивідуальній частині Договору. 3.3.3. Банк протягом строку дії Договору має право запросити у Контрагента установчі документи та підтвердження повноважень осіб, які підписують будь-які документи, пов'язані з Договором. 3.3.4. Банк має право відступити повністю чи частково свої права вимоги за Договором третій особі. Підписанням індивідуальної частини Договору Контрагент надає свою згоду на таке відступлення права вимоги за Договором	3.3.1. The Bank shall have the right to require fulfillment of the terms and conditions of the Agreement by the Counterparty. 3.3.2. The Bank shall have the right to early termination of the Agreement as determined by the public part of the Agreement (General Conditions) unless otherwise stipulated by the Parties in the individual part of the Agreement. 3.3.3. The Bank shall, within the term of the Agreement, have the right to require constituent documents from the Bank and proof of powers and authorities of the signatories to any documents related to the Agreement. 3.3.4. The Bank shall have the right to assign its rights of claim under the Agreement, partially or completely, to any third party. By signing the individual part of the Agreement the Counterparty shall give its consent to such assignment of

третій особі, якщо інше не визначено індивідуальною частиною Договору. 3.3.5. Банк має право проводити Договірне списання у порядку, визначеному розділом «Договірне списання» Загальних Умов. 3.3.6. Банк має право вносити зміни до публічної частини Договору (Загальних Умов) у порядку, визначеному розділом «Зміна та розірвання Договору» Загальних Умов.	the right of claim under the Agreement, to any third party unless otherwise stipulated in the individual part of the Agreement. 3.3.5. The Bank shall have the right to direct debit transfer as stipulated by Direct Debit Transfer section of the General Conditions. 3.3.6. The Bank shall have the right to amend the public part of the Agreement (General Conditions) as stipulated in Amendments and Termination of the Agreement of the General Conditions.
3.4. ОБОВ'ЯЗКИ БАНКУ	3.4. BANK'S OBLIGATIONS
3.4.1. Банк зобов'язується без зволікань інформувати Контрагента про обставини, які мають значення для виконання умов Договору, у тому числі про зміну адрес та банківських реквізитів, перейменування, ліквідацію, реорганізацію, початок процедури банкрутства, прийняття рішення щодо неплатоспроможності у строк не пізніше 10-ти календарних днів із дня вступу таких змін в силу / прийняття такого рішення, у порядку, визначеного Сторонам у розділі «8. Повідомлення» Загальних Умов. 3.4.2. Банк зобов'язується протягом строку дії Договору, на запит Контрагента надавати установчі документи та підтвердження повноважень осіб, які підписують будь-які документи, пов'язані з Договором.	3.4.1. The Bank shall undertake to immediately notify the Counterparty of any circumstances significant for fulfillment of the terms and conditions of the Agreement including change in the address, banking details and its name, liquidation, reorganization, commencement of the bankruptcy proceedings, decision to recognize insolvency of the within the period not exceeding 10 calendar days from the effective date of such changes/decision as stipulated by the Parties in Section 8 (Notices) of the General Conditions. 3.4.2. The Bank shall undertake to provide constituent documents and proof of powers and authorities of the signatories to any documents related to the Agreement within the term of the Agreement as requested by the Counterparty.
3.5. ВІДПОВІДАЛЬНІСТЬ КОНТРАГЕНТА	3.5. COUNTERPARTY'S LIABILITY
3.5.1. Контрагент несе відповідальність за невиконання умов Договору у порядку, визначеному Договором та Законодавством.	3.5.1. The Counterparty shall be responsible for failure to fulfill the terms and conditions of the Agreement as determined by the Agreement and Legislation.
3.6. ВІДПОВІДАЛЬНІСТЬ БАНКУ	3.6. BANK'S LIABILITY
3.6.1. Банк несе відповідальність за невиконання умов Договору у порядку, визначеному Договором та Законодавством.	3.6.1. The Bank shall be responsible for failure to fulfill the terms and conditions of the Agreement as determined by the Agreement and Legislation.
4. УМОВИ ТА ОСОБЛИВОСТІ ВИКОНАННЯ ОКРЕМИХ ДОГОВОРІВ:	4. CONDITIONS AND PARTICULARS OF FULFILLMENT OF CERTAIN AGREEMENTS:
4.1. ДОГОВІР ПРО НЕРОЗГОЛОШЕННЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ	4.1. RESTRICTED INFORMATION NON-DISCLOSURE AGREEMENT
Умови цього розділу Загальних Умов є публічною частиною <i>Договору про нерозголошення інформації з обмеженим доступом</i> (по тексту Загальних Умов – Договір).	Terms and conditions of this section of the General Conditions shall form a public part of the <i>Restricted information non-disclosure agreement</i> (in the General Conditions referred to as the Agreement).
ВИЗНАЧЕННЯ ТЕРМІНІВ: Договір – Договір про нерозголошення інформації з обмеженим доступом, який складається із індивідуальної частини Договору та публічної частини Договору (Загальні Умови), укладений Сторонами. Користувач – Сторона за Договором про нерозголошення інформації з обмеженим доступом; він же Контрагент по тексту Загальних Умов. Банк – АТ «ОТП БАНК», Сторона за Договором про нерозголошення інформації з обмеженим доступом. ІЗОД – відомості, що містять банківську, комерційну таємницю, інсайдерську, конфіденційну інформацію, власником яких є Банк, або які є предметом професійного, ділового, виробничого, комерційного та/або інших інтересів Банку, а також персональні дані, стосовно яких згідно з положеннями Закону України «Про захист персональних даних» Банк виступає у ролі володільця.	TERMS AND DEFINITIONS: Agreement shall mean the Restricted information non-disclosure agreement consisting of the individual part and the public part of the Agreement (General Conditions) concluded by the Parties. User shall mean a Party to the Restricted information non-disclosure agreement, also referred to as the Counterparty in the General Conditions. Bank shall mean OTP BANK JSC, a Party to the Restricted information non-disclosure agreement. Restricted information shall mean data containing banking and commercial secrecy, insider, confidential information owned by the Bank or being the subject matter of the Bank's professional, production, commercial and/or other interests as well as personal data in relation to which the Bank acts as a holder in accordance with the provisions of the Law of Ukraine 'On personal data protection'.

Банківська таємниця – термін вживається згідно з визначенням, наведеним у статті 60 Закону України «Про банки і банківську діяльність».

Зовнішня сторона – фізичні особи та/або фізичні особи – підприємці, та/або юридичні особи, які не асоціюються з Банком та залучаються Банком до виконання робіт, надання послуг, постачання товарів на підставі договорів цивільно-правового (господарського) характеру. Надалі також Користувач.

Залучена Користувачем Особа – фізична особа, яка є найманим працівником Користувача, залучена Користувачем, до участі у переговорах з Банком або яка є найманим працівником Користувача, яка у зв'язку з виконанням своїх службових (посадових) обов'язків має доступ до ІзОД Банку.

Залучена Користувачем (Зовнішньою стороною) Особа – фізична особа, яка є найманим працівником Користувача (який є Зовнішньою стороною), залучена Користувачем, до участі у переговорах з Банком або яка є найманим працівником Користувача, яка у зв'язку з виконанням своїх службових (посадових) обов'язків має доступ до ІзОД Банку, а також залучена Користувачем фізична особа, яка не перебуває з Користувачем у трудових відносинах, але має доступ до ІзОД Банку на умовах договору підяду, договору послуг, авторських договорів, тощо.

Особисті Зобов'язання – письмовий документ, за типовою формою Банку, підписаний Залученою Користувачем (Зовнішньою стороною) Особою, відповідно до якого Залучена Користувачем (Зовнішньою стороною) Особа зобов'язується виконувати вимоги Договору (Договору про нерозголошення інформації з обмеженим доступом).

Інсайдерська інформація – термін вживається згідно з визначенням, наведеним у статті 44 Закону України «Про цінні папери та фондовий ринок».

Інформаційний актив (ресурс) – будь-яка сутність, що має для Банку цінність і впливає на властивості та рівень захисту інформації.

Комерційна таємниця – інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці. Перелік відомостей, що становлять комерційну таємницю Банку, наведено у пункті 4.1.1.2.2. Договору.

Конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана

Banking secrecy shall have the meaning prescribed in article 60 of the Law of Ukraine 'On banks and banking activities'.

External party shall mean physical persons and/or self-employed persons, and/or legal entities not associated with the Bank and involved by the Bank into works, services, goods supply under independent contractor agreements, hereinafter also referred to as the User.

User's involved person shall mean a physical person employed by the User and involved into negotiations with the Bank or the User's employee having access to the Bank's Restricted information due to performance of his/her official duties.

Person involved by the User (External party) shall mean a physical person employed by the User (being the External Party), involved by the User into negotiations with the Bank or the User's employee having access to the Bank's Restricted information due to performance of his/her official duties and a physical person involved by the User having no labour relationship with the User but having access to the Bank's Restricted information under the contractor, service, authorship agreements etc.

Personal obligations shall mean a written document in a form approved by the Bank and signed by the Person involved by the User (External party) pursuant to which the Person involved by the User (External party) undertakes to fulfill all requirements of the Agreement (Restricted information non-disclosure agreement).

Insider information shall have the meaning prescribed in article 44 of the Law of Ukraine 'About securities and stock market'.

Information asset (recourse) shall mean anything valuable for the Bank and affecting the properties and level of information protection.

Commercial secrecy shall mean information having secrecy to the extent that it is, in whole or in a certain form and in the entirety of its constituent elements is not known and easily accessible for the persons usually dealing with such kind of information it belongs to and in this context it has commercial value and was the subject matter of measures to maintain its secrecy taken by the person controlling such information adequate to existing circumstances. Commercial secrecy may include data of technical, organizational, commercial, production and other nature except for those which may not be referred to commercial secrecy in accordance with law. The list of data representing commercial secrecy of the Bank is given in sub-clause 4.1.1.2.2. of the Agreement.

Confidentiality shall mean the particular feature of information; it means that information may not be obtained by an authorized user and/or process without the Bank's consent.

Personal data, personal databases, personal data processing, personal database owner shall have the meanings defined in article 2 of the Law of Ukraine 'On personal data protection'.

неавторизованими користувачем і/або процесом без згоди Банку. Персональні дані, база персональних даних, обробка персональних даних, володілець бази персональних даних – терміни вживаються згідно з визначеннями, наведеними в статті 2 Закону України «Про захист персональних даних». Розголошення ІзОД – ознайомлення будь-якої особи з ІзОД, що відбулось з порушенням правового режиму доступу до цієї інформації. Сторона – Користувач/Контрагент або Банк. Сторони – Користувач/Контрагент та Банк спільно. Третя особа – будь-яка особа, за винятком Сторін.	Restricted information disclosure shall mean that any person studied Restricted information in violation of the legal regime of access to such information. Party shall mean a User/Counterparty of the Bank. Parties shall mean a User/Counterparty and the Bank jointly. Third party shall mean any person except for the Parties.
4.1.1. ЗАГАЛЬНІ ПОЛОЖЕННЯ 4.1.1.1. Шляхом укладення Сторонами Договору про нерозголошення інформації з обмеженим доступом (Договору) з метою встановлення з Користувачем (Контрагентом) договірних взаємовідносин Сторін щодо порядку використання Користувачем ІзОД наданої Банком, Сторони домовились по наступне: 4.1.1.2. ПЕРЕЛІК ВІДОМОСТЕЙ, ЩО СТАНОВЛЯТЬ ІзОД: 4.1.1.2.1. Банківська таємниця Перелік відомостей, що становлять Банківську таємницю, визначено статтею 60 Закону України «Про банки і банківську діяльність». Зокрема до складу кодів, що використовуються Банком для захисту інформації і згідно з Законом України «Про банки і банківську діяльність» віднесені до Банківської таємниці, входять: ➤ значення криптографічних ключів (за виключенням ключів несиметричних криптографічних алгоритмів, що передаються відкрито у складі сертифікатів), які використовуються для захисту платіжних документів та даних трансакцій платіжних систем і систем електронної комерції, а також для захисту платіжних продуктів (платіжні картки, електронні ваучери тощо); ➤ значення криптографічних ключів, що використовуються у засобах захисту інформації Банку або надані Банку Третіми особами у зв'язку зі здійсненням ним банківської діяльності; ➤ паролі, коди доступу до інформаційних активів Банку, засобів обмеження фізичного доступу, систем охоронної сигналізації Банку; ➤ коди, що використовуються для автентифікації та захисту даних платіжних карток національних та міжнародних платіжних систем і не є криптографічними ключами (PIN-коди, PIN-блоки, дані магнітних стрічок, особисті дані власників платіжних карток, що визначені міжнародним стандартом «Payment Card Industry Data Security Standard (PCI DSS)». 4.1.1.2.2. Комерційна таємниця До комерційної таємниці Банку віднесено такі відомості: 4.1.1.2.2.1 Відомості щодо організації банківських процесів, зокрема щодо: ➤ детальної структури Банку; ➤ масштабів діяльності Банку;	4.1.1. GENERAL 4.1.1.1. By entering into the Restricted information non-disclosure agreement (Agreement) in order to establish Parties' contractual relations with the User (Counterparty) as to the User's use of the Restricted information provided by the Bank, the Parties agreed as follows: 4.1.1.2. LIST OF DATA REPRESENTING RESTRICTED INFORMATION: 4.1.1.2.1. Banking secrecy The list of data representing Banking secrecy is determined by article 60 of the Law of Ukraine 'On banks and banking activities'. In particular, in accordance with the Law of Ukraine 'On banks and banking activities' the items below are included into the codes used by the Bank to protect information: ➤ cryptographic key values (excluding asymmetric cryptographic algorithms sent publicly as part of certificates) used to protect payment documents and transaction data of the payment and e-commerce systems as well as to protect payment products (payment cards, electronic vouchers, etc.); ➤ cryptographic key values used in the devices protecting information of the Bank and provided to the Bank by Third parties in relation to banking activities; ➤ passwords, access codes to information assets of the Bank, physical access restriction devices, security alarm systems of the Bank; ➤ codes used to authenticate and protect data of the payment cards of the national and international payment systems and not being cryptographic keys (PIN-codes, PIN-blocks, magnetic tape data, personal data of payment card holders determined by the International Payment Card Industry Data Security Standard (PCI DSS)). 4.1.1.2.2. Commercial secrecy Commercial secrecy of the Bank shall include the following data: 4.1.1.2.2.1 data concerning arrangement of banking processes, in particular: ➤ detailed structure of the Bank; ➤ range of activities of the Bank; ➤ types and location of the equipment securing basic processes of the Bank; ➤ detailed information concerning topology of the computer network of the Bank;

➤ типів та розміщення обладнання, що забезпечує виконання основних процесів Банку; ➤ детальні відомості стосовно топології комп'ютерної мережі Банку; ➤ узагальнені відомості про запаси матеріалів та комплектуючих, місця зберігання коштів та платіжних засобів, а також матеріалів, що використовуються для виготовлення або введення в обіг цих платіжних засобів. 4.1.1.2.2.2. Відомості щодо методів управління Банком та процесами банківської діяльності, зокрема щодо системи підпорядкування, заохочення працівників та контролю за їх діяльністю. 4.1.1.2.2.3. Відомості щодо тактичного планування та стратегії розвитку Банку. 4.1.1.2.2.4. Відомості щодо фінансового стану Банку, якщо вони не підлягають обов'язковому опублікуванню. 4.1.1.2.2.5. Відомості щодо маркетингових досліджень, що проведені Банком або отримані за його кошти. 4.1.1.2.2.6. Відомості щодо ринкової та цінової політики Банку. 4.1.1.2.2.7 Відомості щодо проведення торгів, зокрема відомості щодо підготовки до участі тендерах, а також результатів їх проведення. 4.1.1.2.2.8. Відомості щодо матеріалів робочих нарад та засідань. 4.1.1.2.2.9 Узагальнені відомості щодо партнерів та клієнтів, якщо ці відомості не віднесено до банківської таємниці і вони можуть бути використані для конкурентної боротьби проти Банку. 4.1.1.2.2.10. Відомості щодо переговорів та контрактів, зокрема про умови контрактів, господарських договорів, а також умови забезпечення конфіденційності, якщо вони розкривають зміст угоди або інші зобов'язання Банку перед партнерами та клієнтами. 4.1.1.2.2.11. Відомості щодо досліджень та розробок, зокрема: ➤ про мету, задачі, напрямки, програми перспективних досліджень щодо запровадження нових банківських продуктів і засобів автоматизації банківської діяльності, якщо ці відомості можуть бути використані для конкурентної боротьби проти Банку; ➤ ключові відомості про оригінальні ідеї технічних розробок, особливості організаційних, технологічних, конструктивних, технічних (у тому числі, програмно-апаратних), художньо-технічних рішень (наприклад, дизайну платіжних карток, оформлення реклами), які розроблено Банком самостійно або створено за його кошти. 4.1.1.2.2.12. Детальні відомості щодо технологій, зокрема про банківські технології та специфіку їх використання, у тому числі відомості щодо технології обробки інформації, виготовлення та введення в обіг платіжних засобів. 4.1.1.2.2.13. Інформація, що є об'єктом товарних відносин, зокрема інформація, яка надається партнерам та клієнтам Банку на комерційній основі, або яка придбана Банком за власні кошти (якщо умовами контрактів цю інформацію не визнано відкритою).	➤ summarized data concerning the stock of materials and components, the place where money and payment means are kept as well as materials used to manufacture of such payment means or their putting into circulation. 4.1.1.2.2.2. Data concerning methods used to manage the Bank and processes of banking activities, in particular, subordination, employees' incentive and activity control systems. 4.1.1.2.2.3. Data concerning tactic planning and strategy of development of the Bank. 4.1.1.2.2.4. Data concerning the financial position of the Bank if they are not subject to mandatory disclosure. 4.1.1.2.2.5. Data concerning marketing researches carried out by the Bank or received at the Bank's expense. 4.1.1.2.2.6. Data concerning the market and price policy of the Bank. 4.1.1.2.2.7 Data concerning bids, in particular, data concerning preparation to participation in tenders and their results. 4.1.1.2.2.8. Data concerning the materials of working conferences and meetings. 4.1.1.2.2.9 Summarized data concerning partners and clients if such data are not a part of banking secrecy and may be used in competitive practices against the Bank. 4.1.1.2.2.10. Data concerning negotiations and contracts, in particular, conditions of the contracts, business contracts and conditions ensuring confidentiality if they disclose the content of the agreement or other Bank's obligations before partners and clients. 4.1.1.2.2.11. Data concerning researches and developments, in particular: ➤ objective, tasks, trends and programs of prospective researches concerning implementation of new bank products and bank activity automation devices if such data may be used in competitive practices against the Bank; ➤ key data concerning original ideas of engineering developments, particulars of organizational, technological, constructive, engineering (including hardware and software), art and engineering solutions (for example, design of payment cards, advertisement design) developed by the Bank or at the Bank's expense. 4.1.1.2.2.12. Detailed data concerning technologies, in particular, banking technologies and specific nature of their use, including data concerning technologies of information processing, preparation and putting payment means into circulation. 4.1.1.2.2.13. Information being a subject matter of commodity relations, in particular, information provided to the partners and clients of the Bank on a commercial basis or purchased at the Bank's expense (if conditions of contracts stipulate that such information is not public). 4.1.1.2.2.14. Відомості щодо організації та роботи системи безпеки Банку, якщо їх не віднесено до банківської таємниці, у тому числі відомості щодо інцидентів безпеки, що мали місце. 4.1.1.2.2.15. Data concerning copyright, in particular:
---	--

4.1.1.2.2.14. Відомості щодо організації та роботи системи безпеки Банку, якщо їх не віднесено до банківської таємниці, у тому числі відомості щодо інцидентів безпеки, що мали місце.

4.1.1.2.2.15. Відомості щодо авторського права, зокрема:

- відомості щодо політики управління авторським правом в Банку;
- відомості щодо планів, підготовки та результатів проведення переговорів з придбання авторських прав;
- особисті відомості про авторів, майнові авторські права яких передано Банку або використовуються Банком;
- відомості про власників майнових прав, які передано Банку або використовуються Банком;
- умови авторських договорів, які укладено Банком;
- відомості, що розкривають зміст робіт зі створення продукції, майнові права, які належать Банку (до їх офіційного оголошення).

4.1.1.2.2.16. Зміст розпорядчих та регулятивних документів, що містять рішення керівних органів Банку.

4.1.1.2.2.17. Перелік клієнтів Банку, якщо він містить інформацію стосовно 50 та більше осіб;

4.1.1.2.2.18. Інші відомості технічного, організаційного, комерційного, виробничого та іншого характеру, розголошення яких може призвести до суттєвого збитку Банку або погіршення його репутації.

4.1.1.2.3. Персональні дані

До ІзОД віднесено персональні дані співробітників Банку, клієнтів, інших фізичних осіб, володільцем яких є Банк.

4.1.1.2.4. Інсайдерська інформація

До ІзОД віднесено інсайдерську інформацію, яка знаходиться у розпорядженні Банку у зв'язку зі здійсненням своєї діяльності.

4.1.1.2.5. Конфіденційна інформація

Конфіденційна інформація – інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, що на законній підставі знаходиться у володінні, користуванні або розпорядженні Банку, доступ до якої обмежено Банком або іншими власниками цієї інформації (крім суб'єктів владних повноважень) і яка може поширюватися за рішенням Банку та/або бажанням (згодою) цих осіб у визначеному ними порядку та відповідно до передбачених ними умов.

До конфіденційної інформації Банку зокрема відносяться:

- зміст службової кореспонденції та інших внутрішніх документів Банку;
- програмні коди та параметри налаштування систем обробки інформації Банку;
- перелік клієнтів Банку, що стосується менш, як 50-ти осіб.

4.1.1.2.6. Інформація, яка не віднесена до ІзОД

Наступна інформація не вважається ІзОД і не є предметом Договору:

- інформація, доступ до якої не може бути обмежено згідно вимог законодавства України;

- data concerning the copyright management policy in the Bank;
- data concerning the plans, preparation and result of negotiations to purchase authorship rights;
- personal data about the authors whose property authorship rights are assigned to or used by the Bank;
- data concerning the holders of property rights assigned to or used by the Bank
- conditions of copyright agreements concluded by the Bank;
- data disclosing the content of creation works for products, property rights held by the Bank (before their official disclosure).

4.1.1.2.2.16. Content of administrative and regulatory documents with the decisions of management bodies of the Bank.

4.1.1.2.2.17. List of the Bank's clients with information about 50 or more persons;

4.1.1.2.2.18. Other data of engineering, organizational, commercial, production and other nature which disclosure may result in material losses of or damage to the Bank's reputation.

4.1.1.2.3. Personal data

Restricted information shall include personal data of the Bank's employees, clients, other physical persons, which are in the Bank's possession.

4.1.1.2.4. Insider information

Restricted information shall include insider information in the Bank's possession related to the Bank's activities.

4.1.1.2.5. Confidential information

Confidential information shall mean any information about a physical person and information with access restricted by a physical person or legal entity except for persons with authoritative powers possessed, used or disposed of by the Bank on legal grounds, access to which is restricted by the Bank or other information holder (except for persons with authoritative powers) and which may be disseminated as decided by the Bank and/or upon agreement of such persons in a manner and subject to the conditions stipulated by such persons.

Confidential information of the Bank shall include, in particular:

- content of business correspondence and other internal documents of the Bank;
- program codes and parameters of configuration of information processing system of the Bank;
- list of the Bank's clients, which includes less than 50 persons.

4.1.1.2.6. Information not included into Restricted information.

Information below shall not be considered Restricted information and shall not be the subject matter of the Agreement:

- information access to which may not be restricted in accordance with the requirements of legislation of Ukraine;
- information officially disclosed by the Bank in public information means, in particular, mass media;

➤ інформація, офіційно оприлюднена Банком у відкритих засобах інформації, зокрема у засобах масової інформації; ➤ інформація, щодо розкриття якої Користувачу надано офіційний дозвіл Банку (у письмовій формі). 4.1.2. ПРЕДМЕТ ДОГОВОРУ 4.1.2.1. Договір визначає порядок використання та збереження Користувачем ІзОД переданого йому Банком, а також відповідальності Користувача за порушення конфіденційності ІзОД. 4.1.2.2. Дія Договору також розповсюджується на ІзОД, що стала відома Користувачу у зв'язку зі здійсненням Банком своєї діяльності або наявністю між Банком та Користувачем певних господарських або інших відносин, що регулюються Законодавством. 4.1.3. ПРАВА, ОBOB'ЯЗКИ ТА ВІДПОВІДАЛЬНІСТЬ СТОРІН Крім прав, обов'язків та відповідальності Сторін, визначених індивідуальною частиною Договору та розділом «3. ПРАВА, ОBOB'ЯЗКИ ТА ВІДПОВІДАЛЬНІСТЬ СТОРІН (ЗАГАЛЬНІ)» Загальних Умов, Сторони також домовились про наступне: 4.1.3.1. Користувач зобов'язується: 4.1.3.1.1. Протягом всього строку дії та протягом 5-ти наступних послідовних років після закінчення дії Договору (або більш тривалого строку, якщо цей строк спеціально визначено Законодавством стосовно окремих категорій ІзОД): 4.1.3.1.1.1. Не розголошувати ІзОД Третім особам ІзОД, як вона визначена у Договорі, без письмової згоди Банку. 4.1.3.1.1.2. Не надавати, не продавати Третім особам, не відчужувати у будь-який інший спосіб ІзОД. 4.1.3.1.1.3. Не використовувати ІзОД у будь-який спосіб, офіційно не дозволений Банком, зокрема не використовувати вищезазначену інформацію у власних інтересах або інтересах Третіх осіб. 4.1.3.1.1.4. Забезпечувати виконання вимог щодо режиму доступу, обробки та захисту ІзОД, визначених Законодавством та Банком, зокрема вимоги: ➤ Закону України «Про банки і банківську діяльність» – стосовно банківської таємниці; ➤ Закону України «Про захист персональних даних» – стосовно персональних даних, наданих Банком Користувачу; ➤ Закону України «Про цінні папери та фондовий ринок» – стосовно інсайдерської інформації. 4.1.3.1.1.6. Не допускати несанкціонованого доступу до ІзОД неуповноважених осіб з числа Залучених Користувачем Осіб / Залучених Користувачем (Зовнішньою стороною) Осіб, а також Третіх осіб внаслідок незабезпечення належних заходів зберігання/режиму зберігання ІзОД, невжиття інших заходів обмеження доступу до ІзОД, які Користувач повинен вжити з метою виконання умов Договору. 4.1.3.1.1.7. У строк, який є мінімально можливим, але не більше 24 годин з моменту настання події, інформувати Банк про всі події, пов'язані з фактами розголошення або порушення конфіденційності ІзОД.	➤ information which disclosure by the User is officially permitted by the Bank (in writing). 4.1.2. SUBJECT MATTER OF AGREEMENT 4.1.2.1. The Agreement shall determine the procedure of use and storage of Restricted information by the User transferred to the User by the Bank and the User's liability for violation of confidentiality of such Restricted information. 4.1.2.2. This Agreement shall also cover Restricted information which became known to the User in a result of the Bank's activities or existence of certain business or other relations between the Bank and the User governed by Law. 4.1.3. RIGHTS, OBLIGATIONS AND RESPONSIBILITY OF THE PARTIES Except for the rights, obligations and responsibility of the Parties set forth in the individual part of the Agreement and Section 3 (RIGHTS, OBLIGATIONS AND RESPONSIBILITY OF THE PARTIES) of the General Conditions, the Parties agree on the following: 4.1.3.1. The User shall undertake: 4.1.3.1.1. within the term of the Agreement and during 5 years thereafter (or during the longer period if specifically stipulated by Legislation in relation to certain categories of Restricted information): 4.1.3.1.1.1. not to disclose Restricted information determined in the Agreement to Third parties without the Bank's written consent. 4.1.3.1.1.2. not to provide, sell or alienate Restricted information to Third parties in any other way. 4.1.3.1.1.3. not to use Restricted information in any manner not officially permitted by the Bank, in particular, not to use information above for personal purposes or for the benefit of Third parties. 4.1.3.1.1.4. to ensure fulfillment of the requirements to the mode of access, processing and protection of Restricted information determined by Legislation and the Bank, in particular, the requirements of: ➤ Law of Ukraine 'On banks and banking activities' in relation to banking secrecy; ➤ Law of Ukraine 'On personal data protection' – in relation to personal data provided to the User by the Bank; ➤ Law of Ukraine 'On securities and stock market' – in relation to insider information. 4.1.3.1.1.6. prevent unauthorized access to Restricted information by unauthorized persons from among the User's involved persons / Persons involved by the User (External party) and Third parties resulting from failure to ensure proper storage measures/conditions for Restricted information, failure to implement other measures to restrict access to Restricted information to be taken by the User in order to fulfill the terms and conditions of the Agreement. 4.1.3.1.1.7. to notify the Bank of all events related to disclosure or breach of confidentiality of Restricted information as quickly as possible but not more than within 24 hours from occurrence of such event.
--	---

4.1.3.1.1.8. Якщо Користувач є «Зовнішньою стороною», дотримуватися Вимог щодо забезпечення інформаційної безпеки Зовнішньою стороною/Залученою Користувачем (Зовнішньою стороною) Особою (згідно з п.п.4.1.5. Загальних Умов). 4.1.3.1.2. Забезпечити нерозголошення Залученою Користувачем Особою вимог зазначених у п. 4.1.3.1. (з підпунктами) Загальних Умов (публічної частини Договору). 4.1.3.1.3. Якщо Користувач є «Зовнішньою стороною», такий Користувач зобов'язується забезпечити нерозголошення Залученою Користувачем (Зовнішньою стороною) Особою вимог, зазначених у п. 4.1.3.1. (з підпунктами) Загальних Умов (публічної частини Договору), а також довести вимоги Договору до кожної Залученої Користувачем (Зовнішньою стороною) Особи, шляхом підписання Залученою Користувачем (Зовнішньою стороною) Особою Особистих Зобов'язань за зразком, наведеним у Додатку № 1 до індивідуальної частини Договору. 4.1.3.1.4. У строк, який є мінімально можливим, але не більше 5-ти робочих днів після закінчення строку дії або припинення Договору, а також після отримання письмової вимоги Банку, повернути Банку носії ІзОД, не залишаючи у Користувача жодних копій (у тому числі електронних), а також відтворень чи витягів з документів, файлів, даних тощо, які зазначені як ІзОД. 4.1.3.1.5. забезпечувати належне збереження наданих Банком програмних засобів і не передавати їх Третім особам; 4.1.3.1.6. своєчасно інформувати Банк про зміни місцезнаходження, телефонів, прізвищ відповідальних осіб тощо. Обов'язково відповідати на запити Банку щодо надання інформації, яка використовується для оперативної взаємодії з Користувачем. 4.1.3.1.7. Користувач не має права на копіювання та/або розповсюдження, передавання третім особам програмно-технологічного забезпечення та інших об'єктів права інтелектуальної власності Банку, отриманих у зв'язку з виконанням Договору. 4.1.3.2. Користувач має право: 4.1.3.2.1. Використовувати ІзОД у зв'язку з установленням ділових відносин/співпраці чи інших відносин з Банком у спосіб, у межах та з метою, що офіційно дозволені Банком. 4.1.3.2.2. Надавати ІзОД уповноваженим державним органам на їх письмовий запит належної форми виключно у межах та випадках, передбачених Законодавством. Про кожний випадок отримання запиту на розкриття ІзОД Користувач повинен не пізніше 24 годин з моменту отримання запиту направити відповідне письмове повідомлення Банку. 4.1.3.3. Банк має право: 4.1.3.3.1. Здійснювати аудит та моніторинг діяльності Користувача, пов'язаної з доступом до ІзОД. 4.1.3.3.2. вносити зміни до публічної частини Договору (Загальних Умов) у порядку, визначених розділом «14.	4.1.3.1.1.8. If the User is an External party, to meet the Requirements to information security to be provided by the External party / Person involved by the User (External party) (in accordance with clause 4.1.5. of the General Conditions). 4.1.3.1.2. to ensure non-disclosure of the requirements stated in clause 4.1.3.1. of the General Conditions (public part of the Agreement) by the User's involved person. 4.1.3.1.3. if the User is an External party, such User shall undertake to ensure non-disclosure of the requirements stated in clause 4.1.3.1. (with sub-clauses) of the General Conditions (public part of the Agreement) by the Person involved by the User (External party) and also bring the requirements of the Agreement to knowledge of each Person involved by the User (External party) by way of signing the Personal Commitments by the Person involved by the User (External party) in a form given in Annex 1 to the individual part of the Agreement. 4.1.3.1.4. to return all media with Restricted information without no copies being kept by the User (including in an electronic form) and reproductions or extracts from documents, files, data etc. marked as Restricted information as quickly as possible but not more than within 5 business days upon expiry or termination of the Agreement and also after receipt of the Bank's request. 4.1.3.1.5. to ensure proper security of software applications provided by the Bank and not to transfer the same to Third parties; 4.1.3.1.6. to notify the Bank immediately of the change in the location, telephones, surnames of responsible persons, etc; to reply to the Bank's requests as to provision of information used for immediate cooperation with the User. 4.1.3.1.7. The User shall have no right to copy and/or distribute, transfer software and other intellectual property of the Bank obtained in a result of fulfillment of the Agreement to Third parties. 4.1.3.2. The User shall have the right: 4.1.3.2.1. to use Restricted information to establish relations/cooperation or other relations with the Bank in a manner, to the extent and for the purpose officially permitted by the Bank. 4.1.3.2.2. to provide Restricted information to the authorized governmental bodies upon their proper written request to the extent and in cases stipulated by Legislation. The User shall be obliged to notify the Bank in writing of each request for disclosure not later than 24 hours from receipt of such request. 4.1.3.3. The Bank shall have the right: 4.1.3.3.1. to audit and monitor the User's activity related to access to Restricted information. 4.1.3.3.2. to amend the public part of the Agreement (General Conditions) as stipulated by Section 14 (AMENDMENTS AND TERMINATION OF THE AGREEMENT / GENERAL CONDITIONS) of the General Conditions. 4.1.3.4. Responsibility of the Parties:
---	--

ЗМІНА ТА РОЗІРВАННЯ ДОГОВОРУ /
ЗАГАЛЬНИХ УМОВ» Загальних Умов.

4.1.3.4. Відповідальність Сторін:

Відповідальність Сторін визначається індивідуальною частиною Договору, пунктом 4.1.3.4. (з підпунктами) Загальних Умов, розділом «3. ПРАВА, ОБОВ'ЯЗКИ ТА ВІДПОВІДАЛЬНІСТЬ СТОРІН (ЗАГАЛЬНІ)» Загальних Умов та Законодавством.

4.1.3.4.1. За невиконання або неналежне виконання своїх зобов'язань однією із Сторін, передбачених Договором та Законодавством, винна Сторона несе відповідальність згідно з умовами Договору та Законодавством.

4.1.3.4.2. Сторона, яка порушила зобов'язання, взяті на себе за Договором, повинна усунути ці порушення в найкоротший строк.

4.1.3.4.3. Сплата штрафних санкцій (пені/штрафу) не звільняє Сторони від виконання договірних зобов'язань.

4.1.3.4.4. Користувач несе відповідальність за невиконання вимог п.4.1.3.1. (з підпунктами) Загальних Умов (публічної частини Договору).

4.1.3.4.5. Якщо Користувач **НЕ Є «Зовнішньою стороною»**, за невиконання/неналежне виконання Користувачем вимог п. 4.1.3.1. Загальних Умов (публічної частини Договору), Користувач несе відповідальність у розмірі визначеному індивідуальною частиною Договору. Банк має право додатково вимагати відшкодування Користувачем у повному обсязі збитків завданих Користувачем Банку шляхом розголошенням ІзОД або порушенням вимог п. 4.1.3.1.2. Загальних Умов (публічної частини Договору) сума яких визначається за згодою Сторін або рішенням суду.

4.1.3.4.6. Якщо Користувач **Є «Зовнішньою стороною» і при цьому не здійснює і не зобов'язаний здійснювати, відповідно до Загальних Умов, залучення Залученої Користувачем (Зовнішньою стороною) Особи**, за невиконання/неналежне виконання Користувачем вимог п.4.1.3.1. Загальних Умов (публічної частини Договору), Користувач протягом **10-ти календарних днів** з дати отримання письмової вимоги Банку, сплачує Банку штраф у розмірі **100 000,00 гривень** за кожний випадок порушення, якщо інший розмір штрафу не передбачено індивідуальною частиною Договору.

Крім того, Банк має право додатково вимагати відшкодування Користувачем у повному обсязі збитків завданих Користувачем Банку шляхом розголошенням ІзОД або порушенням вимог п. 4.1.3.1. Загальних Умов (публічної частини Договору) сума яких визначається за згодою Сторін або рішенням суду.

4.1.3.4.7. Якщо Користувач **Є «Зовнішньою стороною», і при цьому здійснює або зобов'язаний здійснити, відповідно до Загальних Умов, залучення Залученої Користувачем (Зовнішньою стороною) Особи** за невиконання/неналежне виконання Користувачем вимог п. 4.1.3.1. Загальних Умов (публічної частини Договору), Користувач протягом **10-ти календарних днів** з дати отримання письмової вимоги Банку, сплачує Банку штраф

Responsibility of the Parties shall be determined by the individual part of the Agreement, clause 4.1.3.4 (with sub-clauses) of the General Conditions, Section 3 (RIGHTS, OBLIGATIONS AND RESPONSIBILITY OF THE PARTIES) of the General Conditions and Legislation.

4.1.3.4.1. for failure or improper fulfillment of its obligations by one of the Parties stipulated by the Agreement and Legislation the guilty Party shall be responsible in accordance with the terms and conditions of the Agreement and Legislation.

4.1.3.4.2. The Party in default of obligations hereunder shall be obliged to remedy such violations as soon as possible.

4.1.3.4.3. Payment of penalties (fines) shall not release the Party from fulfillment of its contractual obligations.

4.1.3.4.4 The User shall be responsible for failure to fulfill the requirements of clause 4.1.3.1. (with sub-clauses) of the General Conditions (public part of the Agreement).

4.1.3.4.5. IF the User is **NOT an External party**, for failure/improper fulfillment of the requirements of clause 4.1.3.1. of the General Conditions (public part of the Agreement) by the User, the User shall be responsible to the extent determined by the individual part of the Agreement. The Bank shall have the right to require further reimbursement of losses caused by the User to the Bank in full due to disclosure of Restricted information or breach of the requirements of clause 4.1.3.1.2. of the General Conditions (public part of the Agreement), which amount is determined as agreed by the Parties or by a court decision.

4.1.3.4.6. If the User **IS an External party and does not involve and is not obliged to involve the Person involved by the User (External party) in accordance with the General Conditions**, for failure /improper fulfillment of the requirements of clause 4.1.3.1. of the General Conditions (public part of the Agreement) by the User, the User shall, within **10 calendar days** from receipt of the written request from the Bank, pay the penalty in the amount of **UAH 100 000,00** for each violation unless other amount of penalty is stipulated in the individual part of the Agreement.

In addition, the Bank shall have the right to require further reimbursement of all losses caused by the User to the Bank in a result of disclosure of Restricted information or breach of the requirements of clause 4.1.3.1. of the General Conditions (public part of the Agreement), which amount is determined as agreed by the Parties or by a court decision.

4.1.3.4.7. If the User **IS an External party and involves or is obliged to involve the Person involved by the User (External party) in accordance with the General conditions**, for failure /improper fulfillment of the requirements of clause 4.1.3.1. of the General Conditions (public part of the Agreement) by the User, the User shall, within **10 calendar days** from receipt of the written request from the Bank, pay the penalty in the amount of **UAH 100 000,00** for each violation.

In addition, the Bank shall have the right to require further reimbursement of all losses caused by the User to the Bank in a result of disclosure of Restricted information or breach of the requirements of clause 4.1.3.1. of the General

у розмірі 100 000,00 гривень за кожний випадок порушення. Крім того, Банк має право додатково вимагати відшкодування Користувачем у повному обсязі збитків завданих Користувачем Банку шляхом розголошенням ІзОД або порушенням вимог п. 4.1.3.1. Загальних Умов (публічної частини Договору) сума яких визначається за згодою Сторін або рішенням суду. 4.1.3.4.8. Кожна із Сторін несе відповідальність за збої в обміні інформацією, викликані навмисними, необережними або некомпетентними діями їх персоналу. 4.1.4. СТРОК ДІЇ ДОГОВОРУ ТА ПОРЯДОК ЙОГО РОЗІРВАННЯ 4.1.4.1. Строк дії Договору складає більший із вказаних нижче періодів: 4.1.4.1.1. 5 років з дати набуття чинності Договору для Користувача, або 4.1.4.1.2. Якщо Користувач є «Зовнішньою стороною», період з дати набуття чинності Договору для Користувача і до завершення 5-ти послідовних років з дати припинення Договору за яким Користувач надає Банку послуги, поставляє товари, виконує роботи. 4.1.4.2. Договір може бути розірваний за згодою Сторін або з ініціативи Банку в односторонньому порядку шляхом надсилання відповідного письмового повідомлення Користувачу. 4.1.4.3. Ініціювання розірвання Договору за ініціативою Користувача можливе тільки за умови, якщо у Користувача немає заборгованості перед Банком за Договором. Заборгованістю Користувача є несплачені штрафних санкції, збитки відповідно до Договору. 4.1.4.4. Розірвання Договору, у тому числі за ініціативою Банку, не звільняє Користувача від обов'язку сплатити заборгованість, що виникла протягом дії Договору в повному обсязі. 4.1.4.5. Закінчення строку дії Договору не звільняє Сторони від виконання всіх передбачених Договором зобов'язань та від відповідальності за невиконання чи неналежне виконання зобов'язань в період дії Договору. 4.1.4.6. Дія Договору припиняється у разі ліквідації Банку чи Користувача.	Conditions (public part of the Agreement), which amount is determined as agreed by the Parties or by a court decision. 4.1.3.4.8. Each of the Parties shall be responsible for information exchange interruptions caused by willful, negligent or unqualified actions of their personnel. 4.1.4. TERM OF THE AGREEMENT AND ITS TERMINATION 4.1.4.1. The term of the Agreement shall be the longest of the periods stated below: 4.1.4.1.1. 5 years from the effective date of the Agreement for the User or 4.1.4.1.2. If the User is an External party, from the effective date of the Agreement for the User and till expiry of 5 consecutive years from the date of termination of the Agreement in accordance with which the User provides services, goods, works to the Bank. 4.1.4.2. The Agreement may be terminated upon agreement between the Parties or the Bank's initiative unilaterally on a basis of the relevant written notice sent to the User. 4.1.4.3. The User may initiate termination of the Agreement provided that the User has no amounts outstanding before the Bank under the Agreement. The User's debts shall include penalties, fines and losses unpaid under the Agreement. 4.1.4.4. Termination of the Agreement, including upon the Bank's initiative, shall not release the User from its obligation to pay all debts arisen during the term of the Agreement. 4.1.4.5. Expiry of the Agreement shall not release the Parties from fulfillment of their obligations stipulated by the Agreement and for failure or improper fulfillment thereof during the term of the Agreement. 4.1.4.6. The Agreement shall terminate in case of liquidation of the Bank or the User Користувача.
4.1.5. Вимоги щодо забезпечення інформаційної безпеки Зовнішньою стороною / Залученою Користувачем (Зовнішньою стороною) Особою	4.1.5. Requirements to information security to be ensured by the External Party / Person involved by the User (External party)
Терміни та поняття: Банк – АТ «ОТП БАНК»; Договір – Договір про нерозголошення інформації з обмеженим доступом, який складається із індивідуальної частини Договору та публічної частини Договору (Загальні Умови), укладений Сторонами. Договір про надання послуг – договір, що укладається між Банком та Зовнішньою стороною про надання послуг, виконання робіт, поставки товару у галузі інформаційних технологій, пов'язаних з банківською діяльністю. ІБ – інформаційна безпека; ІзОД – інформація з обмеженим доступом.	Terms and definitions: Bank shall mean OTP BANK JSC; Agreement shall mean the Restricted information agreement consisting of the individual part and public part (General Conditions) of the Agreement concluded between the Parties. Service agreement shall mean an agreement concluded between the Bank and the External Party concerning provision of services, fulfillment of works and delivery of goods in the sphere of information technologies related to the banking activities. IS shall mean information security;

Автентифікація користувача – процедура перевірки відповідності пред’явленого ідентифікатора користувача на предмет належності цьому користувачеві; встановлення або підтвердження справжності користувача.

Аутсорсинг – передача Зовнішній стороні певних бізнес-функцій або складових бізнес-процесу Банку з метою підвищення продуктивності праці або зниження собівартості послуг.

Аутстафінг – виведення персоналу за штат Банку, що передбачає використання Банком послуг робітників, які юридично є представниками Зовнішньої сторони.

Банківська таємниця – інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку (Закон України «Про банки і банківську діяльність»).

Користувач – Сторона за Договором, надалі також Зовнішня сторона.

Вразливість – нездатність протистояти реалізації певної загрози або сукупності загроз.

Доступність – властивість ресурсу системи обробки інформації, яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний.

Загроза ІБ – будь-яка обставина або подія ІБ, що можуть бути причиною порушення політики безпеки інформації або нанесення збитків Банку.

Захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї (Закон України «Про інформацію»).

Зовнішня сторона – фізичні особи та/або фізичні особи – підприємці, та/або юридичні особи, які не асоціюються з Банком та залучаються Банком до виконання робіт, надання послуг, постачання товарів на підставі договорів цивільно-правового (господарського) характеру. Надалі також Користувач.

Залучена Користувачем (Зовнішньою стороною) Особа – фізична особа, яка є найманим працівником Користувача (який є Зовнішньою стороною), залучена Користувачем, до участі у переговорах з Банком або яка є найманим працівником Користувача, яка у зв’язку з виконанням своїх службових (посадових) обов’язків має доступ до ІЗОД Банку, а також залучена Користувачем фізична особа, яка не перебуває з Користувачем у трудових відносинах, але має доступ до ІЗОД Банку на умовах договору підряду, договору послуг, авторських договорів, тощо, укладеного між Користувачем та Банком.

Особисті Зобов’язання – письмовий документ, за типовою формою Банку, підписаний Залученою

Restricted information shall mean information with limited access.

User’s authentication shall mean the procedure of verification of the user’s identifier to find that the user is its holder; the procedure of authentication of the user.

Outsourcing shall mean assignment of certain business functions or constituents of the business process of the Bank to the External party in order to increase productivity of labour or reduce cost of services.

Outstaffing shall mean exclusion of the personnel from the staff of the Bank that implies the use of services of the employees by the Bank who are legal representatives of the External party.

Banking secrecy shall mean information in relation to activity and financial position of the client which became known to the Bank during provision of services to and relations with the client or third parties during provision of banking services (Law of Ukraine ‘On banks and banking activities’).

User shall mean a Party to the Agreement, hereinafter also referred to as the External party.

Sensitivity shall mean inability to resist to certain threat or a range of threats.

Availability shall mean the feature of the resource of the information processing system that implies that a user and/or a process having relevant powers may use the resource in accordance with the rules determined by the security policy without waiting beyond the established time period, i.e. when it is in a form, in a place and in a time necessary for the user.

IS threat shall mean any IS circumstance or event, which may cause violation of the information security policy or damage to the Bank.

Information protection shall mean the aggregate of legal, administrative, organizational, technical and other measures ensuring security, integrity of information and proper access thereto (Law of Ukraine ‘On information’).

External party shall mean physical and/or self-employed persons not associated with the Bank and involved by the Bank into works, services, goods supply under independent contractor agreements, hereinafter also referred to as the User.

Person involved by the User (External party) shall mean a physical person employed by the User (being the External Party), involved by the User into negotiations with the Bank or the User’s employee having access to the Bank’s Restricted information due to performance of his/her official duties and a physical person involved by the User having no labour relationship but having access to the Bank’s Restricted information under the contractor, service, authorship agreements etc. Concluded between the User and the Bank.

Personal obligations shall mean a written document in a form approved by the Bank and signed by the Person

Користувачем (Зовнішньою стороною) Особою, відповідно до якого Залучена Користувачем (Зовнішньою стороною) Особа зобов'язується виконувати вимоги Договору (Договору про нерозголошення інформації з обмеженим доступом).

Ідентифікатор – унікальний атрибут (ім'я) об'єкта (користувача, процесу), що дозволяє однозначно виділити даний об'єкт серед подібних.

Інсайдерська інформація – неоприлюднена інформація про емітента, його цінні папери та похідні (деривативи), що перебувають в обігу на фондовій біржі, або правочини щодо них, у разі якщо оприлюднення такої інформації може істотно вплинути на вартість цінних паперів та похідних (деривативів), та яка підлягає оприлюдненню відповідно до вимог Законодавства. Інформація щодо оцінки вартості цінних паперів та/або фінансово-господарського стану емітента, якщо вона отримана виключно на основі оприлюдненої інформації або інформації з інших публічних джерел, не заборонених законодавством, не є інсайдерською інформацією. Інформація не вважається інсайдерською з моменту її оприлюднення відповідно до закону (Закон України «Про цінні папери та фондовий ринок»).

Інформаційна безпека Банку – стан інформації, в якому забезпечується збереження конфіденційності, цілісності та доступності інформації, а також цілісності, спостереженості та керованості процесів її обробки згідно з вимогами, визначеними політикою ІБ Банку.

Інформаційний ресурс – будь-яка сутність, що має для Банку цінність і впливає на властивості та рівень захисту інформації. До інформаційних ресурсів зокрема належать: власне інформація, обладнання, програмні ресурси, інженерна інфраструктура, інформаційні послуги та сервіси життєзабезпечення, персонал, причетний до обробки інформації тощо.

Інформаційна система (система інформаційних технологій) – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів, зокрема, САБ, системи зв'язку тощо.

Інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді (Закон України «Про інформацію»).

Інформація з обмеженим доступом – відомості, що містять банківську, комерційну таємницю, конфіденційну, інсайдерську інформацію, власником яких є Банк, або які є предметом професійного, ділового, виробничого, комерційного та інших інтересів Банку, інформація, яка стосується здійснення Банком фінансового моніторингу, а також персональні дані, стосовно яких згідно з положеннями Закону України «Про захист персональних даних» Банк виступає у ролі володільця, розпорядника персональних даних або у ролі третьої особи. Перелік ІзОД Банку та порядок її визначення наведено в регуляторному документі Банку «Положення про

involved by the User (External party) pursuant to which the Person involved by the User (External party) undertakes to fulfill all requirements of the Agreement (Restricted information non-disclosure agreement).

Identifier shall mean a unique attribute (name) of the object (user, process) allowing clear distinction of such object from among similar ones.

Insider information shall mean non-public information about the issuer, its securities and derivatives in circulation at the stock market or deeds in relation to the same if disclosure of such information may have significant effect on the value of securities and derivatives and which is subject to disclosure in accordance with the requirements of Legislation. Information about assessment of the value of securities and/or financial and economic position of the issuer, if obtained only on the basis of the disclosure information or information from public sources not prohibited by Legislation, shall not be insider information. Information shall not be considered as insider information from the date of its disclosure in accordance with Law (Law of Ukraine 'On securities and stock market').

Bank's information security shall mean the status of information allowing to keep it confidential, integral and available and also to keep the processing procedure integral, observable and manageable in accordance with the requirements set forth in the IS Policy of the Bank.

Information resource shall mean anything valuable for the Bank affecting the features and level of information protection. Information resources, in particular, include information, equipment, program resources, engineering infrastructure, information services and life support services, personnel involved into information processing, etc..

Information system (information technology system) shall mean the organizational and engineering system implementing the information processing technology using technical devices and software, in particular, Bank Automatization System (BAS), communication system, etc.

Information shall mean any information and/or data, which may be stored on material media or displayed in an electronic form (Law of Ukraine 'On information').

Restricted information shall mean data containing banking and commercial secrecy, insider, confidential information owned by the Bank or being the subject matter of the Bank's professional, production, commercial and/or other interests of the Bank, information concerning financial monitoring carried out by the Bank as well as personal data in relation to which the Bank acts as a holder, controller or third party in accordance with the provisions of the Law of Ukraine 'On personal data protection'. The list of Restricted information and the procedure for determining the same shall be given in regulatory document of the Bank 'Regulation on classification of information and measures ensuring protection of restricted information'.

Information security incident shall mean occurrence of one or more uncontrolled or unforeseen IS events, which

класифікацію інформації та заходи щодо забезпечення захисту інформації з обмеженим доступом».

Інцидент інформаційної безпеки – поява однієї або кількох небажаних або непередбачених подій ІБ, з якими пов'язана значна ймовірність компрометації процесів банківської діяльності та створення загроз ІБ.

Комерційна таємниця – інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці (Цивільний кодекс України).

Конфіденційна інформація – інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом (Закон України «Про інформацію»).

Конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом.

Правила інформаційної безпеки – приписи, інструкції, регламенти, вимоги, рекомендації щодо забезпечення безпеки інформації, які містяться у стандартах України, міжнародних стандартах сімейства ISO/IEC 27000, стандартах платіжних систем, національних документах інших країн, міжнародних науково-дослідних організацій та професійних об'єднань.

Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (Закон України «Про захист персональних даних»). До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження (Закон України «Про інформацію»).

Система автоматизації банку – система інформаційних технологій, що вирішує задачі автоматизації банківської діяльності (наприклад, система «Операційний день банку», система «Клієнт-Банк» тощо).

Спостережність – властивість системи обробки інформації, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

are likely to compromise banking activity processes and create IS threats.

Commercial secrecy shall mean information having secrecy to the extent that it is, in whole or in a certain form and in the entirety of its constituent elements is not known and easily accessible for the persons usually dealing with such kind of information it belongs to and in this context it has commercial value and was the subject matter of measures to maintain its secrecy taken by the person controlling such information on legal grounds. Commercial secrecy may include data of technical, organizational, commercial, production and other nature except for those which may not be referred to commercial secrecy (Civil Code of Ukraine).

Confidential information shall mean any information about a physical person and information with access restricted by a physical person or legal entity except for persons with authoritative powers. Confidential information may be disclosed if so desired (agreed) by the relevant person in a manner and under the conditions prescribed and in other cases stipulated by Law (Law of Ukraine 'On information'),

Confidentiality shall mean the particular feature of information; it means that information may not be obtained by an authorized user and/or process.

Information security rules shall mean orders, instructions, regulations, requirements, recommendations concerning information security contained in the standards of Ukraine, international standards ISO/IEC 27000, payment system standards, national documents of other counties, international scientific and research organizations and professional unions.

Personal data shall mean the data or the pool of data about the physical person identified or identifiable (Law of Ukraine 'On personal data protection'). Confidential information about the physical entity shall include, in particular, nationality, education, marital status, religious beliefs, health condition and place of birth (Law of Ukraine 'On information').

Bank's automation system shall mean the system of information technologies dealing with banking activity automation (for example, Bank's operating day, Client-Bank systems, etc.).

Observability shall mean the feature of the information processing system allowing to record activity of the users and processes, use of passive objects and to expressly determine identifiers of users and processes involved in certain events in order to avoid violation of the security policy and/or to ensure responsibility for certain actions.

Stenography shall mean the concealed writing when the notice is coded in such a way that it does not look like a notice.

Стеганографія – тайнопис, при якому повідомлення закодоване таким чином, що не виглядає як повідомлення.

Третя сторона – фізична або юридична особа, організація, орган державної влади тощо, які не асоціюються з Банком або особами, що перебувають у ділових відносинах з Банком у зв'язку зі здійсненням банківської діяльності.

Цілісність інформації – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом.

Цілісність системи – властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки.

4.1.5.1. Вимоги інформаційної безпеки

4.1.5.1.1. Доступ Зовнішній стороні до інформаційних ресурсів та приміщень Банку, де ці ресурси розміщено, надається виключно з дозволу і в інтересах Банку у зв'язку зі здійсненням ним банківської діяльності.

4.1.5.1.2. Загальною підставою для надання доступу є Договір про надання послуг, укладений між Банком та Зовнішньою стороною.

4.1.5.1.3. У випадку, якщо в процесі підготовки або виконання умов Договору про надання послуг, Зовнішня сторона отримує можливість доступу до ІЗОД та інформаційних ресурсів Банку, Зовнішня сторона зобов'язана дотримуватись в ході співробітництва з Банком вимог щодо конфіденційності та інформаційної безпеки.

4.1.5.1.3.1. Зобов'язання Зовнішньої сторони щодо дотримання в ході співробітництва з Банком вимог щодо конфіденційності та інформаційної безпеки фіксуються шляхом укладення Договору.

4.1.5.1.3.2. Вимоги інформаційної безпеки щодо Зовнішньої сторони визначаються регулятивними документами банку (політиками, положеннями, регламентами, інструкціями, порядками тощо) щодо забезпечення інформаційної безпеки і включають (але не обмежуючись):

- визначення ІЗОД, що є предметом Договору;
- цінність для Банку та конфіденційність залученої інформації;
- відповідальність та дії Зовнішньої сторони щодо запобігання несанкціонованому розголошенню ІЗОД;
- право власності на інформацію у тому числі, право інтелектуальної власності;
- дозволені способи використання Зовнішньою стороною ІЗОД Банку;
- процедуру сповіщення та звітування щодо фактів розголошення або порушення конфіденційності ІЗОД Банку.
- перелік інформаційних ресурсів Банку, до яких надається доступ Зовнішній стороні;
- спосіб та термін надання доступу Зовнішній стороні до інформаційних ресурсів Банку;

Third party shall mean a physical person, legal entity, organization, governmental authority etc. Not associated with the Bank or persons in business relations with the Bank resulting from banking activities.

Information integrity shall mean a feature of information implying that information may not be modified by an authorized user and/or process.

System integrity shall mean a feature of the system implying that neither component may be removed, modified or added in violation of the security policy.

4.1.5.1. Information security requirements

4.1.5.1.1. The External party shall be provided access to information resources and premises of the Bank, where such resources are placed, only with permission from and in the interests of the Bank in connection with banking activities.

4.1.5.1.2. The general ground for access shall be the Service agreement concluded between the Bank and the External party.

4.1.5.1.3. If during preparation or fulfillment of the terms and conditions of the Service agreement the External party gains the opportunity to access Restricted information and information resources of the Bank, the External party shall be obliged to meet the confidentiality and information security requirements during cooperation with the Bank.

4.1.5.1.3.1. The External party's obligations to meet the confidentiality and information security requirements during cooperation with the Bank shall be recorded in the Agreement.

4.1.5.1.3.2. Information security requirements in relation to the External party shall be determined by the regulatory documents of the Bank (policies, regulations, rules, instructions, procedures, etc.) related to information security, including (but not limited by):

- determination of Restricted information being the subject matter of the Agreement;
- value for the Bank and confidentiality of information involved;
- responsibility and actions of the External party to avoid unauthorized disclosure of Restricted information;
- property right to information including intellectual property right;
- permitted uses of Restricted information of the Bank by the External party;
- procedure of notification and reporting in relation to events of disclosure or violation of confidentiality of Restricted information of the Bank.
- list of information resources of the Bank to which the External party receives access;
- mode and the term of access to information resources of the Bank granted to the External party;

➤ спосіб ідентифікації співробітників Зовнішньої сторони, Залучених Користувачем (Зовнішньою стороною) Осіб, а також порядок санкціонування, верифікації, перегляду та скасування прав доступу до інформаційних ресурсів Банку; ➤ інциденти ІБ, що можуть мати місце, та порядок реагування на інциденти; ➤ заходи безпеки, які мають бути застосовані Зовнішньою стороною для захисту інформаційних ресурсів Банку. ➤ заходи безпеки, які мають бути застосовані Зовнішньою стороною для захисту власних інформаційних ресурсів з метою унеможливлення шкоди інформаційним ресурсам Банку. 4.1.5.1.4. У випадках, якщо послуги Зовнішньої сторони: ➤ надаються на умовах аутстафінгу; ➤ передбачають створення окремих робочих місць або присутність представників Зовнішньої сторони на території Банку; ➤ надання представникам Зовнішньої сторони віддаленого доступу до ресурсів, розміщених в інформаційній мережі Банку, до моменту фактичного надання доступу Зовнішній стороні до інформаційних ресурсів Банку повинні бути виконані такі умови: ➤ підписання Залученою Користувачем (Зовнішньою стороною) Особою Особистих Зобов'язань; ➤ надання Зовнішньою стороною клопотання (у формі офіційного листа) щодо забезпечення її представникам віддаленого доступу до інформаційних ресурсів Банку або організації робочих місць та надання доступу до службових приміщень Банку та підтвердження дотримання правил інформаційної безпеки на комп'ютерах, з яких її представники підключатимуться до інформаційних ресурсів банку. 4.1.5.1.5. Представники Зовнішньої сторони ЗОБОВ'ЯЗАНІ: 4.1.5.1.5.1. Знати та виконувати вимоги ІБ, що їх стосуються, визначені Договором, у тому числі на комп'ютерах, з яких відбувається підключення до інформаційних ресурсів банку. 4.1.5.1.5.2. Знати та виконувати вимоги щодо забезпечення режиму конфіденційності ІзОД Банку, визначені Договором. Не розголошувати ІзОД (у тому числі відомості, що містять банківську таємницю, комерційну таємницю, конфіденційну та інсайдерську інформацію, персональні дані клієнтів та співробітників Банку), власником якої є Банк або які є предметом професійного, ділового, виробничого, комерційного та інших інтересів Банку, яка була доведена представнику у встановленому Банком порядку або стала відома у зв'язку з виконанням представником його обов'язків. 4.1.5.1.5.3. Не допускати несанкціонованого доступу до ІзОД неуповноважених осіб з числа Залучених Користувачем (Зовнішньою стороною) Осіб, а також Третіх осіб внаслідок незабезпечення належних заходів зберігання/режиму зберігання ІзОД, нежиття інших	➤ method of identification of the employees of the External party, Persons involved by the User (External party) and the procedure of authorization, verification, review and cancellation of the rights of access to information resources of the Bank; ➤ IS incidents, which may occur, and the incident response procedure; ➤ security measures to be applied by the External party to protect information resources of the Bank. ➤ security measures applicable by the External party to protect own information resources in order to make it impossible to cause damage to information resources of the Bank. 4.1.5.1.4. In cases when the External party services: ➤ are provided on an outstaffing basis; ➤ stipulate creation of separate working places or presence of the External party's representatives in the Bank; ➤ grant remote access to the External party's representatives to the resources placed in the information network of the Bank till the actual access is granted to the External party to information resources of the Bank the following conditions shall be met: ➤ signing Personal commitments by the Person involved by the User (External party); ➤ submission of an application (in a form of official letter) for remote access to its representatives to information resources of the Bank or arrangement of working places and access to office premises of the Bank and confirmation of observance of the information security rules when working on the computers connected by its representatives to the information resources of the Bank. 4.1.5.1.5. Representatives of the External party SHALL BE OBLIGED: 4.1.5.1.5.1. to know and fulfill IS requirements related thereto and determined by the Agreement, including when working on the computers connected to information resources of the Bank. 4.1.5.1.5.2. to know and fulfill the requirements to confidentiality regime in relation to Restricted information of the Bank determined by the Agreement; not to disclose Restricted information (including data containing banking secrecy, commercial secrecy, confidential and insider information, personal data of the clients and employees of the Bank) owned by the Bank or which are the subject matter of the professional, business, production, commercial and other interests of the Bank brought to the representative's knowledge as determined by the Bank or known to the Bank due to performance of duties by its representative. 4.1.5.1.5.3. prevent unauthorized access to Restricted information by unauthorized persons from among Persons involved by the User (External party) and Third parties due to failure to take proper measures for storage/storage regime in relation to Restricted information, failure to take other measures in order to restrict access to Restricted information, which the User should take to fulfill the terms and conditions of the Agreement.
---	---

заходів обмеження доступу до ІзОД, які Користувач повинен вжити з метою виконання умов Договору. 4.1.5.1.5.4. Своєчасно та у повному обсязі виконувати заходи, визначені Банком, щодо запобігання несанкціонованого доступу до ІзОД, безпечного використання та збереження інформаційних ресурсів Банку, які були надані Зовнішній стороні у зв'язку з виконанням Договору. 4.1.5.1.5.5. Під час перебування на території Банку виконувати доведені до представника Зовнішньої сторони правила внутрішнього розпорядку та режиму безпеки Банку. 4.1.5.1.5.6. Знати перелік інформаційних ресурсів Банку, до яких представнику Зовнішньої сторони надається доступ, а також дозволені методи та регламент доступу, включаючи терміни початку надання та припинення доступу. 4.1.5.1.5.7. Знати та виконувати вимоги Банку щодо дозволу або заборони здійснення Зовнішньою стороною процесів управління змінами інформаційних ресурсів Банку (оновлення програмного та апаратного забезпечення, зміна конфігурації засобів обробки інформації тощо) та керування вразливостями (у тому числі, вимоги щодо здійснення процесу сканування ресурсів інформаційної мережі, підтримка яких здійснюється на умовах аутсорсингу), а також порядок виконання таких дій, що стосуються представника Зовнішньої сторони (у випадку наявності відповідного дозволу). 4.1.5.1.5.8. Виконувати вимоги Банку, які стосуються представників Зовнішньої сторони, стосовно ідентифікації та автентифікації під час здійснення логічного доступу до інформаційної мережі та інформаційних систем Банку (зокрема вимоги щодо застосування унікальних ідентифікаторів та паролів доступу). 4.1.5.1.5.9. По закінченню виконання робіт, обумовлених Договором про надання послуг, повернути Банку всі носії ІзОД, що є власністю або знаходяться у розпорядженні Банку і були надані представнику у зв'язку з виконанням представником його обов'язків або фактично знаходяться у розпорядженні представника. Знищити всі копії даних та документів, які містять ІзОД, у спосіб, що гарантує неможливість відновлення цієї інформації, якщо такі копії тимчасово використовувались під час виконання робіт. 4.1.5.1.5.10. Знати спосіб, у який мають здійснюватись комунікації з Банком у випадку виникнення інцидентів ІБ та надзвичайних ситуацій. Негайно інформувати Банк стосовно фактів виникнення інцидентів ІБ або надзвичайних ситуацій, що мають відношення до виконання робіт, обумовлених Договором про надання послуг. 4.1.5.1.6. Представникам Зовнішньої сторони ЗАБОРОНЯЄТЬСЯ: 4.1.5.1.6.1. Розголошувати ІзОД (у тому числі відомості, що містять банківську таємницю, комерційну таємницю, конфіденційну та інсайдерську інформацію, персональні	4.1.5.1.5.4. to take timely measures to the fullest extent set by the Bank to avoid unauthorized access to Restricted information, secure use and storage of information resources of the Bank granted to the External party due to fulfillment of the Agreement. 4.1.5.1.5.5. to fulfill the internal code of conduct and security regime of the Bank when being in the premises of the Bank it has been informed of. 4.1.5.1.5.6. to know the list of information resources of the Bank to which the External party's representative is granted access and also the permitted methods and access rules including the start and termination of access. 4.1.5.1.5.7. to know and fulfill the requirements of the Bank related to access or prohibition to carry out the processes managing the changes in the information resources of the Bank by the External party (hardware and software update, change in the configuration of the information processing equipment, etc.) and sensitivity (including requirements to scanning of the information network resources supported on an outsourcing basis) and the procedure of performance of such actions related to the representative of the External party (in case of the relevant permit). 4.1.5.1.5.8. to fulfill the requirements of the Bank related to the External party's representatives concerning identification and authentication during logic access to the information network and information systems of the Bank (in particular, requirements to unique identifiers and access passwords used). 4.1.5.1.5.9. to return all media with Restricted information to the Bank owned or disposed of by the Bank, upon termination of works stipulated by the Service agreement, which have been given to the representative due to fulfillment of his duties or are at the representative's disposal; to destruct all copies of data and documents with Restricted information in a manner guaranteeing non-retrieval of such information if such copies are temporarily used during works. 4.1.5.1.5.10. to know how to communicate with the Bank in case of IS incidents or extraordinary events; to notify the Bank forthwith of the IS incidents or extraordinary events related to works stipulated by the Service agreement. 4.1.5.1.6. Representatives of the External party SHALL NOT BE ALLOWED: 4.1.5.1.6.1. to disclose Restricted information (including data with banking, commercial secrecy, confidential and insider information, personal data of the clients and representatives of the Bank) owned by the Bank or which are the subject matter of the professional, business, production, commercial and other interests of the Bank brought to the representative's knowledge in a manner determined by the Bank or known due to performance of his duties by the representative. 4.1.5.1.6.2. to use Restricted information of the Bank in own interests or in the interests of Third parties. 4.1.5.1.6.3. to access information resources and production premises of the Bank in manner not permitted by the Bank
--	---

дані клієнтів та представників Банку), власником якої є Банк або які є предметом професійного, ділового, виробничого, комерційного та інших інтересів Банку, яка була доведена представнику у встановленому Банком порядку або стала відома у зв'язку з виконанням представником його обов'язків. 4.1.5.1.6.2. Використовувати ІзОД Банку у власних інтересах або в інтересах третіх осіб. 4.1.5.1.6.3. Здійснювати доступ до інформаційних ресурсів, а також виробничих приміщень Банку у спосіб, який не дозволено Банком (при цьому слід керуватись принципом, «дії, які не дозволені Банком, вважаються забороненими»). 4.1.5.1.6.4. Використовувати з метою здійснення доступу до інформаційних ресурсів та виробничих приміщень Банку будь-які персональні атрибути доступу (ідентифікатори, паролі, коди, перепустки тощо), які належать іншій особі, а також надавати власні атрибути доступу будь-яким іншим особам. 4.1.5.1.6.5. Здійснювати несанкціоноване Банком втручання в роботу комп'ютерів, інформаційних систем, комп'ютерних мереж чи мереж електрозв'язку Банку. 4.1.5.1.6.6. Здійснювати несанкціоновані Банком зміну, знищення або блокування інформації, яка оброблюється в комп'ютерах, інформаційних системах чи комп'ютерних мережах Банку або зберігається на носіях такої інформації. 4.1.5.1.6.7. Здійснювати несанкціоновані Банком дії, спрямовані на отримання ІзОД Банку, у тому числі шляхом перехоплення або копіювання інформації, яка оброблюється в комп'ютерах, інформаційних системах, комп'ютерних мережах Банку або зберігається на носіях такої інформації (зокрема засобами технічної розвідки, шляхом фотографування документів та пристроїв відображення інформації, шляхом застосування пристроїв аудіозапису тощо). Здійснювати несанкціоновані Банком дії, спрямовані на отримання інформації щодо топології комп'ютерних мереж, а також конфігурації, параметрів, ідентифікаторів доступу мережевих ресурсів та пристроїв Банку, у тому числі із застосуванням мережевих сканерів. 4.1.5.1.6.8. Порушувати правила експлуатації комп'ютерів, інформаційних систем, комп'ютерних мереж чи мереж електрозв'язку Банку або порядку чи правил захисту інформації, яка в них оброблюється. 4.1.5.1.6.9. Навмисно або ненавмисно розповсюджувати в середовищі Банку шкідливі програмні засоби, застосовувати (у тому числі приховано) технічні засоби, призначені для несанкціонованого втручання в роботу комп'ютерів, інформаційних систем, комп'ютерних мереж чи мереж електрозв'язку Банку, у тому числі комп'ютерні віруси та програмні закладки (шпигунське програмне забезпечення). 4.1.5.1.6.10. Нехтувати правилами інформаційної безпеки, які можуть призвести до ураження комп'ютерів Зовнішньої сторони, які взаємодіють з Банком, комп'ютерними вірусами та шкідливими програмними	(in this case all actions not permitted by the Bank shall be treated as prohibited). 4.1.5.1.6.4. to use any personal access attributes (identifiers, passwords, codes, ID cards, etc.) owned by the other person and to give own attributes to any other persons to access information resources and production premises of the Bank. 4.1.5.1.6.5. to interfere with the operation of the computers, information systems, computer networks or other telecommunication systems of the Bank without the Bank's permit. 4.1.5.1.6.6. to introduce changes, destruct or block information processes using the computers, information systems or computer networks of the Bank or stored on information media without the Bank's permit. 4.1.5.1.6.7. to carry out actions without the Bank's permit to obtain Restricted information of the Bank including by way of interception or coping information processed on the computers, information systems, computer networks of the Bank or stored on information media (in particular, using technical intelligence means, taking photos of documents and information presentation devices, using audiorecording devices, etc.). to perform actions not permitted by the Bank in order to obtain information concerning topology of computer networks and configuration, parameters, access identifiers to network resources and devices of the Bank, including with use of network scanners. 4.1.5.1.6.8. to violate the rules of operation of the computers, information systems, computer or telecommunication networks of the Bank or procedure or rules for protection of information processed using the same. 4.1.5.1.6.9. to disseminate, willfully or unintentionally, malicious software in the Bank, to use technical equipment (including secretly) aimed at unauthorized interference with functioning of computers, information systems, computer or telecommunication networks of the Bank including computer viruses and implant tools (spyware). 4.1.5.1.6.10. to neglect information security rules, which may result in infection of the External party's computers interacting with the Bank, computer viruses and malicious software and thus to affect information security of the Bank. 4.1.5.1.6.11. To transmit Restricted information in communication and data transmission networks that are not controlled by the Bank (including using Internet, e-mail, instant messages), unless sanctioned by the Bank and the message itself is not encrypted by cryptographic means in accordance with requirements of the Bank.
---	--

засобами і, таким чином, вплинути на інформаційну безпеку Банку.

4.1.5.1.6.11. Передавати у мережах зв'язку та передачі даних, що не контролюються Банком (у тому числі із застосуванням сервісів Internet, електронної пошти, миттєвих повідомлень), ІзОД Банку, якщо на це Банком не надано санкцію, а само повідомлення не зашифровано криптографічними засобами відповідно до вимог Банку.

4.1.5.1.6.12. Якщо Зовнішній стороні надані засоби зв'язку або передачі даних (у тому числі сервіси Internet, електронної пошти, миттєвих повідомлень тощо), що використовуються від імені Банку з метою передачі інформації за його межі, **ЗАБОРОНЯЄТЬСЯ**:

- використовувати вищезазначені засоби з метою, що суперечить інтересам Банку, вимогам законодавства України, міжнародним законодавчим актам, які ратифіковано Україною, а також з метою заподіяння шкоди іншим особам у наслідок порушення їх прав, релігійних, етнічних, політичних переконань тощо;
- використовувати засоби, що підміняють або маскують мережеву адресу комп'ютера користувача (IP- та MAC адресу), поштову адресу, а також ім'я (ідентифікатор доступу) користувача, під яким його зареєстровано у комп'ютерній мережі Банку (т.зв. анонімайзери);
- не надавати доступ до засобів Internet та електронної пошти із застосуванням власного ідентифікатора доступу та пароля іншим особам, у тому числі шляхом створення спільних (shared) ресурсів;
- не використовувати засоби Internet та електронної пошти з комерційними цілями, з метою реклами, агітації тощо, у тому числі не створювати засоби публікації в Internet (FTP, WWW-сторінки, електронні дошки об'яв), якщо це не пов'язано з виробничою діяльністю Банку;
- не розсилати поштові повідомлення будь-якого розміру або змісту, отримання яких не санкціоновано адресатами (spam), у тому числі рекламних та інформаційних об'яв на велику кількість адрес;
- не використовувати засоби Internet для отримання програмного забезпечення та даних з ненадійних джерел, а також у спосіб, що порушує авторське право та ліцензійні умови щодо їх розповсюдження;
- не використовувати криптографічні методи для приховування змісту повідомлень, що передаються, та методи стеганографії для приховування самого факту передачі, якщо ці дії не санкціоновано Банком;
- під час роботи в середовищі Internet не використовувати технічні засоби, призначені для збору та передачі медіа інформації (WEB-камери, мікрофони тощо), якщо такі дії не санкціоновано Банком.

4.1.5.1.7. Права представника Зовнішньої сторони

Представник Зовнішньої сторони, якого залучено до виконання робіт на підставі Договорів про надання послуг, укладених між Банком та Зовнішньою стороною, має право:

- бути ознайомленим з вимогами ІБ, визначені Договором, що його стосуються;

4.1.5.1.6.12. If the External Party is provided with communication or data transmission tools (including Internet, e-mail, instant messaging, etc.) used on behalf of the Bank for the purpose of transmitting information outside the Bank, it is **PROHIBITED**:

- to use the abovementioned tools for the purpose contradicting the interests of the Bank, the requirements of the legislation of Ukraine, international legal acts ratified by Ukraine, as well as for the purpose of causing damage to other persons as a result of violation of their rights, religious, ethnic, political beliefs, etc.;
- use tools that substitute for or mask the network address of the user's computer (IP and MAC address), the mailing address, as well as the name (access identifier) of the user under which he is registered on the Bank's computer network (so-called anonymizers);
- not to share access to Internet and e-mail tools using their own access ID and password to others, including through the creation of shared resources;
- not to use the Internet and e-mail tools for commercial purposes, for advertising, propaganda, etc., including not to create Internet publishing tools (FTP, WWW pages, electronic bulletin boards), unless it is related to production activities of the Bank;
- not send mail messages of any size or content which receipt is not authorized by recipients (spam), including commercial and informational advertisements to a large number of addresses;
- not to use the Internet tools to obtain software and data from unreliable sources, and in a way that violates copyright and license terms for their distribution;
- not to use cryptographic methods to conceal the content of transmitted messages and steganography methods to conceal the very fact of transmission unless these actions are authorized by the Bank;
- while using the Internet, do not use technical means intended for the collection and transmission of media information (webcams, microphones, etc.), unless such actions are authorized by the Bank.

4.1.5.1.7. External Party Representative Rights

A representative of the External Party who is engaged in the performance of works under the Service Agreements concluded between the Bank and the External Party shall have the right to:

- to be familiar with the requirements of the IS set out in the Agreements relating to him or her;

➤ бути ознайомленим з вимогами Договору, в частині, що його стосуються; ➤ бути ознайомленим з вимогами ІБ, правилами внутрішнього розпорядку та режиму безпеки Банку в частині, що його стосуються, а також зі змістом цих Інструктивних матеріалів; ➤ бути ознайомленим з переліком, методами та регламентом доступу до інформаційних ресурсів Банку, до яких представнику Зовнішньої сторони надається доступ; ➤ отримати відомості щодо порядку здійснення комунікацій з Банком у випадку виникнення інцидентів ІБ та надзвичайних ситуацій.	➤ to be familiar with the requirements of the Agreement, in so far as they relate to him or her; ➤ to be familiar with the requirements of the IS, the internal rules and security regime of the Bank in so far as they relate to him or her, as well as with the content of these Guidance Materials; ➤ be familiar with the list, methods and rules of access to the Bank's information resources to which the External Party representative is granted access; ➤ to obtain information on the procedure for communication with the Bank in the event of IS incidents of and emergencies.
4.2. ДОГОВІР ПРО ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ	4.2. ELECTRONIC DOCUMENT CIRCULATION AGREEMENT
Визначення термінів: Договір - Договір про електронний документообіг, який складається із індивідуальної частини Договору та публічної частини Договору (Загальні Умови), укладений Сторонами. Загальні Умови - ЗАГАЛЬНІ УМОВИ ДО ДОГОВОРІВ, ЯКІ УКЛАДЕНІ З АТ «ОТП БАНК» (ПУБЛІЧНІ), які є невід'ємною частиною Договору про електронний документообіг та розміщені на Офіційному сайті Банку. Офіційний сайт Банку - www.otpbank.com.ua Сторона/Сторони – відповідна сторона/сторони за Договором: Банк та/або Контрагент/-и. Сервіс (Сервіс електронного документообігу) – програмна продукція або онлайн-сервіс, призначені для автоматизації процесів документообігу з іншими зареєстрованими учасниками документообігу та передбачає підписання, надсилання, отримання та зберігання Електронних Документів. Сервіс/-и, які Сторони використовують в рамках Договору, визначаються Сторонами в індивідуальній частині Договору про електронний документообіг. «М.Е.Doc» (My Electronic Document, також Medoc, Медок) - програмне забезпечення для подання звітності до контролюючих органів та обміну юридично значущими первинними документами між контрагентами в електронному вигляді. Сервіс електронного документообігу «Вчасно» - сервіс, який призначений для обміну документами в електронному вигляді, підписання і зберігання будь-яких юридично значущих документів. Електронні Документи (Е-Документи) – належно оформлені документи, інформація в яких зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа, які передбачені Законодавством, перелік яких Сторонами визначається в індивідуальній частині Договору про електронний документообіг; Кваліфікований електронний підпис (КЕП) – електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа; Особистий ключ – параметр алгоритму криптографічного перетворення, який використовується	Definition of terms: Agreement - E-document Circulation Agreement, which consists of the individual part of the Agreement and the public part of the Agreement (General Conditions), concluded by the Parties. General conditions - GENERAL CONDITIONS FOR AGREEMENTS CONCLUDED WITH OTP BANK JSC (PUBLIC), which are an integral part of the E-document Circulation Agreement and are posted on the Bank's official website. Official website of the Bank - www.otpbank.com.ua Party – Parties - the corresponding Party/Parties under the Agreement: the Bank and/or counterparty / -parties. Service (E-document Circulation Service) - software products or online services designed to automate document circulation processes with other registered document circulation participants and provides for signing, sending, receiving and storing E-documents. The services that the Parties use under the Agreement are determined by the Parties in the individual part of the E-document Circulation Agreement. «M.E.Doc» (My E-document, also Medoc) is a software for submitting reports to regulatory authorities and exchanging legally significant primary documents between counterparties in electronic form. Vchasno E-document Circulation Service - the service that is designed for exchanging documents in electronic form, signing and storing any legally significant documents. Vchasno E-document Circulation Service - the service that is designed for exchanging documents in electronic form, signing and storing any legally significant documents. Qualified electronic signature (QES) – an electronic signature that is created using the Qualified Electronic Signature tool and is based on a qualified public key certificate; Private key - a parameter of the cryptographic conversion algorithm used as unique electronic data to create an electronic signature or seal, available only to the signer or creator of the electronic seal, as well as for purposes defined by the standards for qualified public key certificates; Public key - a parameter of a cryptographic conversion algorithm that is used as electronic data for verifying an

як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів; Відкритий ключ – параметр алгоритму криптографічного перетворення, який використовується як електронні дані для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів; Кваліфікований сертифікат відкритого ключа (Кваліфікований сертифікат) – сертифікат відкритого ключа, який видається кваліфікованим надавачем електронних довірчих послуг, засвідчувальним центром або центральним засвідчувальним органом і відповідає вимогам Законодавства; Компрометація особистого ключа – будь-яка подія, що призвела або може призвести до несанкціонованого використання Особистого ключа; Засоби криптографічного захисту інформації – це програмний, апаратно-програмний та апаратний засіб, призначений для криптографічного захисту інформації. Законодавство – чинне законодавство України. <i>Терміни, що використовуються в Загальних Умовах з великої літери, є визначеними термінами і мають однакові значення, як у індивідуальній частині Договору, так і у Загальних Умовах, та можуть використовуватись, як в однині, так і в множині.</i>	electronic signature or seal, as well as for purposes defined by the standards for qualified public key certificates; Qualified public key certificate (qualified certificate) – a public key certificate that is issued by a qualified provider of electronic trust services, a certification center or a central certification body and meets the requirements of the legislation; Private key compromise – any event that has led to or may lead to unauthorized use of the private key; Cryptographic information security tools – software and hardware tools designed for cryptographic information protection. Legislation – the current legislation of Ukraine. Terms used in the General Conditions with a capital letter are defined terms and have the same meanings, both in the individual part of the Agreement and in the General Conditions, and can be used both in the singular and in the plural.
4.2.1. Предмет Договору про електронний документообіг. В порядку передбаченому Договором про електронний документообіг та Загальними Умовами Сторони визначили порядок формування, обміну та підписання Е-Документів, а також виконання всіх інших зобов'язань, як вони визначені Договором про електронний документообіг та Загальними Умовами.	4.2.1. Subject of the E-document Circulation Agreement. In accordance with the procedure provided for in the E-document Circulation Agreement and the General Conditions, the Parties determined the procedure for forming, exchanging and signing E-documents, as well as fulfilling all other obligations, as defined in the E-document Circulation Agreement and the General Conditions.
4.2.2. Порядок формування, обміну та підписання Е-Документів. 4.2.2.1. Кожна зі Сторін Договору для електронного документообігу використовує Сервіс електронного документообігу, який визначений Сторонами в індивідуальній частині Договору. 4.2.2.2. Сторони домовилися застосовувати в електронному документообігу із дотриманням Законодавства про Електронні Документи та електронний документообіг з використанням Сервісу види Е-Документів, перелік яких визначений Сторонами в індивідуальній частині Договору. Вказані в індивідуальній частині Договору Е-Документи, оформлені в електронному вигляді, являють собою Електронний Документ, інформація в якому зафіксована у вигляді електронних даних. 4.2.2.3. Електронні Документи повинні містити всі реквізити аналогічних паперових документів, а також інші реквізити, якщо вони передбачені індивідуальною частиною Договору та/або іншим договором, укладеним між Сторонами та містити обов'язкові реквізити, що визначені Законодавством, без яких вони не можуть	4.2.2. Procedure for forming, exchanging and signing E-documents. 4.2.2.1. Each Party to the Agreement uses the E-document Circulation Service for E-document circulation, which is defined by the Parties in the individual part of the Agreement. 4.2.2.2. The Parties have agreed to apply in E-document circulation in compliance with the legislation on E-documents and E-document circulation using the service types of E-documents, the list of which is defined by the Parties in the individual part of the Agreement. The E-documents specified in the individual part of the Agreement, issued in electronic form, mean an E-document, the information in which is recorded in the form of electronic data. 4.2.2.3. The E-documents shall contain all the details of similar paper documents, as well as other details, if they are provided for by the individual part of the Agreement and/or another Agreement concluded between the Parties and contain mandatory details defined by law, without which they cannot be considered primary documents and be the basis for accounting and will not have legal force.

вважатися первинними документами та бути підставою для бухгалтерського обліку і не матимуть юридичної сили.

4.2.2.4. Первинні бухгалтерські документи, що були сформовані в електронному вигляді, в обов'язковому порядку повинні бути підписані за допомогою КЕП, який в свою чергу, має бути підтверджений Кваліфікованим сертифікатом та відповідати правовому статусу, що визначений в Законі України «Про електронні документи та електронний документообіг». Сторони повинні зберігати Е-Документи у порядку визначеному Законодавством.

4.2.2.5. За необхідності, на підставі звернення будь-якої із Сторін Договору, Сторони можуть створювати, підписувати та обмінюватися в паперовій формі дублікатами Е-Документів.

4.2.2.6. Сторони погодили, що відповідальність за наслідки підписання Е-Документів не уповноваженими на те працівниками відповідної Сторони покладається на Сторону, КЕПом якої скріплений відповідний Е-Документ.

4.2.2.7. Сторони зобов'язуються до реалізації умов Договору вжити всіх підготовчих та організаційних заходів для переходу на обмін Е-Документами, забезпечити виготовлення необхідних КЕП відповідальних працівників. Електронні документи підписуються КЕП уповноваженим працівником Банку та/або Контрагента, що вважається підписаними відповідно Стороною Договору.

4.2.2.8. Сторони погодили, що у разі необхідності коригування електронного первинного документу, виключно остання його версія підписана обома Сторонами, є підставою для проведення такої господарської операції в обліку обох Сторін.

4.2.2.9. Сторони дійшли згоди, що розірвання (скасування) Електронного документа, підписаного Сторонами з використанням електронного підпису здійснюється виключно шляхом складення та підписання Сторонами Акту про анулювання Електронного документа. Зазначені Акти про анулювання Електронного документа в праві складати обидві Сторони з власної ініціативи, якщо є порушення домовленостей, зазначених у відповідних Договорах.

4.2.2.10. Використання Сервісу під час передачі документів, якими обмінюються Сторони для належного виконання умов цього Договору, оплачує Сторона, яка відправляє Е-Документ.

4.2.2.11. Кожна Сторона зобов'язана щоденно слідкувати за надходженням Е-Документів та своєчасно здійснювати їх приймання, перевірку, підписання з використанням КЕП та повернення іншій Стороні. Сторона яка здійснює надсилання Е-Документа вважається Стороною-відправником, а Сторона яка здійснює отримання Е-Документа, вважається Стороною-одержувачем.

4.2.2.12. Підготовка Е-Документів здійснюється відповідною Стороною, в строки, якщо вони встановлені

4.2.2.4. The primary accounting documents that were generated in electronic form shall necessarily be signed using the QES, which in turn shall be confirmed by a qualified certificate and correspond to the legal status defined in the law of Ukraine "On E-documents and E-document circulation". The Parties shall store E-documents in accordance with the procedure established by law.

4.2.2.5. If necessary, based on the request of any of the Parties to the Agreement, the Parties may create, sign and exchange duplicate E-documents in paper form.

4.2.2.6. The Parties have agreed that responsibility for the consequences of signing E-documents by unauthorized employees of the relevant Party is assigned to the Party whose QES is attached to the corresponding E-document.

4.2.2.7. The Parties shall implement the terms of the Agreement to take all preparatory and organizational measures for the transition to the exchange of E-documents, to ensure the production of the necessary QES of responsible employees. Electronic documents shall be signed by the QES by an authorized employee of the Bank and/or the counterparty, which is considered signed by the Party to the Agreement, respectively.

4.2.2.8. The Parties have agreed that if it is necessary to adjust the electronic primary document, only the latest version of it signed by both Parties is the basis for conducting such a business transaction in the accounting of both Parties.

4.2.2.9. The Parties have agreed that the termination (cancellation) of an E-document signed by the Parties using an electronic signature is carried out exclusively by drawing up and signing an act of cancellation of the E-document by the Parties. Both Parties have the right to draw up these acts of cancellation of an E-document on their own initiative, if there is a violation of the Agreements specified in the relevant Agreements.

4.2.2.10. The use of the service during the transfer of documents exchanged by the Parties for proper performance of the terms of this Agreement is paid for by the Party sending the E-Document.

4.2.2.11. Each Party shall monitor the receipt of E-documents on a daily basis and promptly accept, verify, sign them using the QES and return them to the other Party. The Party that sends the E-document is considered the sending Party, and the Party that receives the E-document is considered the receiving Party.

4.2.2.12. The preparation of E-documents is carried out by the relevant Party, within the time limits established by the individual part of the Agreement and/or another Agreement concluded between the Parties.

4.2.2.13. By the time of transfer to the other Party, the sending Party shall properly draw up a new and/or verify the received E-document and sign it using the QES (which is created using a qualified electronic signature and based on a qualified public key certificate) within the time limits stipulated in the Agreement. A reasoned refusal to sign an E-document is sent through the system through the mechanism for rejecting an E-document with an indication

індивідуальною частиною Договору та/або іншим договором, укладеним між Сторонами. 4.2.2.13. До моменту передачі іншій Стороні, Сторона-відправник зобов'язана належним чином скласти новий та/або перевірити отриманий Е-Документ та підписати його з використанням КЕП (який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа) у строки, передбачені Договором. Мотивована відмова від підписання Е-Документа надсилається через Систему через механізм відхилення Е-Документа із зазначенням причин. Е-Документи, які передаються, підписуються у всіх випадках з використанням КЕП відповідної Сторони. Перевірка факту підписання відповідною Стороною конкретного Е-Документа, здійснюється Стороною-одержувачем з використанням Відкритого ключа і Кваліфікованого сертифіката. 4.2.2.14. Е-Документи вважаються підписаними і набирають чинності з моменту підписання з використанням КЕП Стороною-одержувачем Е-Документа, отриманого від Сторони-відправника з накладеним нею КЕП. При цьому, Сторони домовилися, що дія Е-Документу розповсюджується на відносини, що виникли після дати укладення Договору. 4.2.2.15. Е-Документ, підписаний Стороною з використанням КЕП і переданий Стороні одержувачу вважатиметься в усіх випадках підписаним уповноваженим представником Сторони-відправника, в межах наданих повноважень, що не потребуватиме щоразу перевірки документів на представництво, якщо Сторони інше не визначили індивідуальною частиною Договору та/або іншим договором, укладеним між Сторонами. КЕП за правовим статусом прирівнюється до власноручного підпису (печатки) та має презумпцію його відповідності власноручному підпису. 4.2.2.16. Сторони домовилися, що Е-Документи, які відправлені та завірені КЕП, мають повну юридичну силу, породжують права та обов'язки для Сторін, можуть бути представлені до суду в якості належних доказів та визнаються рівнозначними документам, що складаються на паперовому носіїві. Сторони, шляхом підписання індивідуальної частини Договору, підтверджують, що документи підписані КЕП, підписанні уповноваженими представниками Сторін. 4.2.2.17. Будь-яка із Сторін вправі ініціювати паралельне (одночасне) оформлення і електронних, і паперових форм первинних бухгалтерських документів. У разі паралельного існування двох форм документів пріоритет мають електронні документи (у випадку їх належного оформлення).	of the reasons. E-documents that are transmitted are signed in all cases using the QES of the relevant Party. The verification of the fact that the relevant Party has signed a specific E-document is carried out by the recipient Party using a public key and a qualified certificate. 4.2.2.14. E-documents are considered to be signed and enter into force from the moment the recipient Party signs by the QES the E-document received from the sending Party with the QES imposed by it. At the same time, the Parties agreed that the E-document applies to relations that have arisen after the date of conclusion of the Agreement. 4.2.2.15. E-document signed by the Party using the QES and transferred to the recipient Party will be considered in all cases signed by the authorized representative of the sending Party, within the limits of the powers granted, it will not require each time verification of documents for representation, unless the Parties have determined otherwise as an individual part of the Agreement and/or other agreement concluded between the Parties. The QES is equal in legal status to a handwritten signature (seal) and has a presumption of its compliance with a handwritten signature. 4.2.2.16. The Parties have agreed that E-documents sent and certified by the QES have full legal force, give rise to rights and obligations for the Parties, can be submitted to the court as appropriate evidence and are recognized as equivalent to documents drawn up on paper. The Parties, by signing the individual part of the Agreement, confirm that the documents are signed by the QES, signed by authorized representatives of the Parties. 4.2.2.17. Either Party has the right to initiate parallel (simultaneous) processing of both electronic and paper forms of primary accounting documents. If two forms of documents exist in parallel, E-documents prevail (if they are properly executed).
4.2.3. Конфіденційність та безпека 4.2.3.1. Кожна Сторона вживає всіх необхідних засобів щодо збереження конфіденційності КЕП та забезпечення безпечного режиму їх використання. Сторони визнають, що КЕП, накладений відповідно до вимог Законодавства,	4.2.3. Confidentiality and security 4.2.3.1. Each Party shall take all necessary measures to preserve the confidentiality of QES and ensure a safe mode of their use. The Parties recognize that QES which is imposed in accordance with the requirements of the

за правовим статусом прирівнюється до власноручного підпису (та за наявності - печатки) Сторін. Сторони також домовились, що у випадку анулювання КЕП, отримання доступу до КЕП третіми особами та/або у інших випадках, пов'язаних з неправомірним використанням КЕП, збитки, заподіяні одній із Сторін Договору або третім особам, підлягають відшкодуванню за рахунок винної Сторони. 4.2.3.2. Сторони погоджуються, що використання засобів криптографічного захисту інформації, які реалізують шифрування і КЕП, достатньо для забезпечення конфіденційності інформаційної взаємодії Сторін щодо захисту від несанкціонованого доступу та безпеки обробки інформації, а також для підтвердження того, що: - Е-Документ надходить від Сторони, яка його передала (підтвердження авторства документа); - Е-Документ не зазнав змін при інформаційній взаємодії Сторін (підтвердження цілісності та автентичності документа). 4.2.3.3. З метою забезпечення безпеки обробки та конфіденційності інформації Сторони зобов'язані: - не допускати появи в комп'ютерному середовищі, де функціонує система для обміну Е-Документами, комп'ютерних вірусів і програм, спрямованих на її руйнування; - не нищити та / або не змінювати архіви Відкритих ключів КЕП, електронних Е-Документів; - не використовувати для підписання Е-Документів скомпрометовані ключі. 4.2.3.4. Сторони самостійно забезпечують збереження програмного забезпечення, яке використовується для обміну Відкритих ключів та Е-Документів, розміщених на своїх комп'ютерах. 4.2.3.5. Видача, заміна, знищення Особистих та Відкритих ключів, в тому числі у випадках їх компрометації, а також видача Кваліфікованого сертифіката, здійснюється тільки кваліфікованим надавачем електронних довірчих послуг. Сторони зобов'язані повідомити одна одну про наявність вищевказаних обставин в строк, що не перевищує 5 (п'ять) робочих днів з моменту виникнення таких обставин.	Legislation by legal status is equal to a handwritten signature (and, if any, a seal) of the Parties. The Parties also agreed that in case of cancellation of the QES, access to the QES by third Parties and/or other cases related to the misuse of the QES, losses caused to one of the Parties to the Agreement or to third Parties are subject to compensation at the expense of the guilty Party. 4.2.3.2. The Parties agree that the use of cryptographic information protection tools that implement encryption and QES is sufficient to ensure the confidentiality of information interaction between the Parties regarding protection against unauthorized access and security of information processing, as well as to confirm that: - The E-document comes from the Party that transferred it (confirmation of the authorship of the document); - The E-document has not been changed during the information interaction of the Parties (confirmation of the integrity and authenticity of the document). 4.2.3.3. In order to ensure the security of information processing and confidentiality, the Parties shall: - In order to ensure the security of information processing and confidentiality, the Parties shall: - not destroy and / or change the archives of QES public keys, electronic E-documents; - not use compromised keys to sign E-documents. 4.2.3.4. The Parties independently ensure the safety of the software used for exchanging public keys and E-documents placed on their computers. 4.2.3.5. Issuance, replacement, destruction of personal and public keys, including in cases of their compromise, as well as issuance of a qualified certificate, is carried out only by a qualified provider of electronic trust services. The Parties are obliged to notify each other of the existence of the above circumstances within a period not exceeding five (5) working days from the date of occurrence of such circumstances.
4.2.4. Інші умови 4.2.4.1. У випадку неможливості виконання зобов'язань за Договором, Сторони негайно повідомляють про це одна одну. 4.2.4.2. Сторони не несуть відповідальності та не надають консультаційних послуг щодо роботи Сервісу. 4.2.4.3. При вирішенні всіх інших питань, пов'язаних з електронним документообігом, які не врегульовані Договором, Сторони керуються положеннями Законодавства. 4.2.4.4. У випадку будь-яких розбіжностей між положеннями Загальних Умов та індивідуальної частини Договору, положення індивідуальної частини Договору матимуть переважну силу.	4.2.4. Other conditions 4.2.4.1. If it is impossible to fulfill its obligations under the Agreement, the Parties immediately notify each other. 4.2.4.2. The Parties are not responsible and do not provide consulting services regarding the operation of the service. 4.2.4.3. When resolving all other issues related to E-document circulation that are not regulated by the Agreement, the Parties shall be guided by the provisions of the legislation. 4.2.4.4. In case of any discrepancies between the provisions of the General Conditions and the individual part of the Agreement, the provisions of the individual part of the Agreement will prevail. 4.2.4.5. The Agreement shall come into force from the date of signing the individual part of the Agreement by the

4.2.4.5. Договір набирає чинності з дати підписання індивідуальної частини Договору Сторонами. Сторони на власний розсуд також можуть скріпити Договір печатками, за умови їх використання згідно з положеннями Статуту. 4.2.4.6. Договір укладений українською та/або українською та англійською мовою (двомовний) та у кількості оригінальних примірників, як те визначено в індивідуальній частині Договору, які мають однакову юридичну силу, по одному примірнику для кожної із Сторін. 4.2.4.7. Договір регулюється і тлумачиться згідно з Законодавством України. 4.2.4.8. Сторони в індивідуальній частині Договору можуть передбачити умови щодо автоматичного продовження строку дії Договору (автопродлонгації). Детальний порядок автопродлонгації Договору визначений у розділі 14 Загальних Умов. 4.2.4.9. Кожна із Сторін має право розірвати Договір. Детальний порядок розірвання Договору визначений у розділі 14 Загальних Умов.	Parties. The Parties, at their sole discretion, may also seal the Agreement, provided that they are used in accordance with the provisions of the Charter. 4.2.4.6. The Agreement is concluded in Ukrainian and/or Ukrainian and English (bilingual) and in the number of original copies, as defined in the individual part of the Agreement, having equal legal force, one copy for each of the Parties. 4.2.4.7. The Agreement shall be regulated and interpreted in accordance with the legislation of Ukraine. 4.2.4.8. The Parties in the individual part of the Agreement may provide for conditions for automatic extension of the term of validity of the Agreement (auto-extension). A detailed procedure for auto-renewal of the Agreement is defined in Section 14 of the General Conditions. 4.2.4.9. Each Party has the right to terminate the Agreement. A detailed procedure for terminating the Agreement is defined in Section 14 of the General Conditions.
5. ВИКОРИСТАННЯ КВАЛІФІКОВАНОГО ЕЛЕКТРОННОГО ПІДПISУ	5. USE OF QUALIFIED ELECTRONIC SIGNATURE
Терміни та поняття: КЕП - удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа. 5.1. Шляхом підписання Сторонами Договору, індивідуальна частина якого містить умови про використання КЕП та за умови, що Сторонами не укладався окремий Договір про електронний документообіг, Сторони домовилися про наступне: 5.1.1. Протягом дії Договору акти приймання-передачі наданих послуг/товару, рахунки-фактури, накладні на зняття з відповідального зберігання, видаткові накладні, акти про анулювання документа, рахунки, акти, податкові накладні за роботи, послуги або товари, передбачені Договором, надаються іншій Стороні в електронному вигляді, з накладанням на документ КЕП уповноважених осіб Сторони, та відправленням електронних документів у середовищі програмного забезпечення «ВЧАСНО» та/або «МЕДок», за умови, що вони складені згідно вимог Законодавства про електронні документи, електронний документообіг та електронний цифровий підпис. 5.1.2. У разі необхідності, зазначені у пункті 5.1.1. Загальних Умов документи можуть складатись та надаватись іншій Стороні у паперовій формі з дотриманням вимог Законодавства. 5.1.3. Підписанням Договору Сторони погодилися та взаємно визнали, що КЕП має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису, за умови, що порядок складання, погодження та затвердження документів електронним підписом відповідає вимогам Законодавства, зокрема порядку складання, погодження та затвердження документів у паперовому вигляді.	Terms and definitions: QES is an advanced electronic signature that is created using a qualified electronic signature tool and is based on a qualified public key certificate. 5.1. By signing the Agreement, the individual part of which contains the conditions for the use of QES and provided that the Parties have not concluded a separate E-document Circulation Agreement, the Parties have agreed as follows: 5.1.1. During the validity of the Agreement, the acts of acceptance-transfer of services/goods, invoices, waybills for removal from responsible storage, delivery notes, acts of withdrawal of documents, bills, acts, tax invoices for the works, services or goods envisaged in the Agreement shall be provided to the other Party electronically, with QES of the authorized persons of the Party on the document, and sending electronic documents in the software environment "TIMELY" and / or "MEDOK", provided that they are made in accordance with the requirements of the Legislation about electronic documents, electronic document circulation and electronic digital signature. 5.1.2. If necessary, the documents referred to in clause 5.1.1. of the General Conditions may be drawn up and submitted to the other Party in hard copy in compliance with the requirements of the Legislation. 5.1.3. By signing the Agreement, the Parties agreed and mutually acknowledged that QES has the same legal force as a handwritten signature and has the presumption of its correspondence with a handwritten signature, provided that the procedure for drafting, approving and adopting documents by electronic signature meets the requirements of the Legislation, including drafting and approval of paper documents.

5.1.4. Обмін електронними документами між Сторонами здійснюється з урахуванням вимог Законодавства в сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, та фінансуванню тероризму, Закону України «Про електронні довірчі послуги», Закону України «Про електронні документи та електронний документообіг». 5.1.5. Сторони домовилися, що електронні документи, відправлені по системі електронного документообігу, засвідчені КЕП Сторони, мають повну юридичну силу, породжують права та обов'язки для Сторін, можуть бути представлені до суду в якості належних доказів та визнаються рівнозначними документам, що складаються на паперовому носіїві. Підтвердження передачі документів по системі електронного документообігу (відправлення, отримання, тощо) вважається легітимним підтвердженням фактичного прийому-передачі таких документів уповноваженими особами Сторін і не вимагає додаткового доказування. 5.1.6. У випадку компрометації особистого ключа підписувача, скасування чи блокування його сертифіката ключа останній зобов'язаний невідкладно повідомити про це отримувача.	5.1.4. Exchange of electronic documents between the Parties is carried out in accordance with the requirements of the Legislation in the field of prevention and counteraction to the legalization (laundering) of proceeds from crime and terrorist financing, the Law of Ukraine "On Electronic Trust Services", the Law of Ukraine "On Electronic Documents and Electronic Document Circulation". 5.1.5. The Parties have agreed that electronic documents sent through the electronic document circulation system certified by QES of the Party have full legal force, create rights and obligations for the Parties, can be presented in court as proper evidence and recognized as equivalent to the documents, made on paper. Confirmation of the transmission of documents through the electronic document circulation system (sending, receiving, etc.) is considered to be a legitimate confirmation of the actual receipt and transmission of such documents by the authorized persons of the Parties and does not require additional proof. 5.1.6. In case of compromise of the personal key of the signer, cancellation or blocking of his key certificate, the latter is obliged to immediately inform the recipient thereof.
6. ВАЛЮТНІ ЗАСТЕРЕЖЕННЯ	6. CURRENCY WARNINGS
6.1. Платежі щодо виконання Сторонами боргових зобов'язань мають бути здійснені Сторонами у валюті боргових зобов'язань в порядку та на умовах, встановлених Договором. 6.2. Інші платежі за Договором підлягають виконанню у валюті України (гривнях), виходячи з валютного курсу НБУ та/або іншого погодженого Сторонами курсу на день виконання (сплати). Сторона не зобов'язана приймати виконання боргових зобов'язань в валюті іншій, ніж визначена Договором. Відмова Сторони від прийняття виконання боргових зобов'язань в валюті іншій, ніж передбачено Договором, не може розглядатися як сприяння збільшенню збитків через прострочення виконання зобов'язань.	6.1. Debt payments by the Parties shall be made by the Parties in the currency of the obligations in accordance with the terms and conditions established by the Agreement. 6.2. Other payments under the Agreement are subject to execution in the currency of Ukraine (hryvnia) based on the NBU exchange rate and/or other exchange rate agreed by the Parties on the day of execution (payment). The party is not obliged to accept debt obligations in a currency other than that specified in the Agreement. A Party's refusal to accept a debt obligation in a currency other than that specified in the Agreement may not be regarded as contributing to an increase in losses due to delay in fulfilment of obligations.
7. ДОГОВІРНЕ СПИСАННЯ	7. CONTRACTUAL WRITE-OFF
7.1. Право Банку на договірне списання коштів з рахунків Контрагента. У випадку настання строку сплати Контрагентом Банку боргових зобов'язань, комісії, відшкодування витрат або іншої оплати за Договором та/або настання строку виконання інших боргових зобов'язань (як діючих зобов'язань так і майбутніх зобов'язань) Контрагента перед Банком за Договором та/або будь-яким іншим договором, який укладено між Контрагентом та Банком (в тому числі кредитним договором, договором страхування, іншим договором про надання банківських послуг), а також у інших випадках та в порядку, що передбачені Договором та/або іншим договором між Сторонами та/або Законодавством, Банк набуває право (але не зобов'язаний), а Контрагент цим беззаперечно та безвідклично доручає Банку самостійно списувати грошові кошти в розмірі, необхідному для виконання таких боргових зобов'язань, а також страхове відшкодування за договором страхування за якими Банк	7.1. Bank's right to contractually write off from Counterparty's accounts. In the event of the maturity of debt obligations, commission, reimbursement of expenses or other payment under the Agreement of the Counterparty to the Bank and/or the maturity of other debt obligations (both current and future obligations) of the Counterparty to the Bank under the Agreement and/or any other agreement entered into between the Counterparty and the Bank (including loan agreement, insurance contract, other banking service contract), as well as in other cases and in the manner provided by the Agreement and/or other agreement between the Parties and/or the Legislation, the Bank acquires the right (but is not obligated), and the Counterparty thereby indisputably and irrevocably instructs the Bank to independently write off the monetary funds in the amount necessary to fulfill such debt obligations, as well as insurance indemnity under the insurance contract under which the Bank is the beneficiary, from any Account of the

виступає вигодонабувачем, з будь-якого рахунку Контрагента на вибір Банку, які відкриті та/або будуть відкриті Контрагентом в Банку, та направити списані таким чином грошові кошти Контрагента в рахунок виконання його боргових зобов'язань перед Банком. 7.2. Договірне списання у випадку, якщо валюта рахунку не відповідає валюті боргового зобов'язання. У випадку відсутності або недостатності у Контрагента коштів на рахунку у валюті, необхідній для оплати його боргових зобов'язань, Банк має правоздійснити договірне списання коштів Контрагента у іншій валюті та зарахувати списані таким чином грошові кошти Контрагента в рахунок виконання його боргових зобов'язань перед Банком за курсом, у порядку та у спосіб, встановленого у відповідному договорі, укладеного між Сторонами, на підставі якого відкрито Контрагенту рахунок у Банку. 7.3. Невикористання Банком його права на договірне списання коштів з рахунків Контрагента не звільняє Контрагента від відповідальності за порушення боргових зобов'язань та від сплати неустойки за таке порушення.	Counterparty at the Bank's choice, which are opened and/or will be opened by the Counterparty in the Bank, and to send the written-off funds of the Counterparty towards fulfillment of its debt obligations to the Bank. 7.2. Contractual write-off in case the currency of the account does not correspond to the currency of the debt obligation. In case the Counterparty does not have or lacks funds in the account in the currency necessary to pay its debt obligations, the Bank has the right to contractually write off the Counterparty's funds in another currency and to deduct the Counterparty's funds written off towards the fulfillment of its debt obligations to the Bank at the rate and in the manner established in the relevant Agreement concluded between the Parties, under which a Counterparty's account is opened in the Bank. 7.3. Non-use by the Bank of its right to contractually write off funds from the Counterparty's accounts does not exempt the counterparty from liability for violation of debt obligations and from paying a penalty for such violation.
8. ПОВІДОМЛЕННЯ	8. NOTICE
8.1. Повідомлення Банку іншій Стороні, що стосується Контрагентів Банку і не містить відомостей, що становлять банківську таємницю чи конфіденційну інформацію Контрагента, може бути направлено Банком Контрагенту шляхом розміщення такого повідомлення у відділені Банку та/або на Офіційному сайті Банку, та/або в будь-якому офіційному друкованому виданні, в якому здійснюється офіційне оприлюднення законів та інших актів Верховної Ради України та/або актів Президента України, та/або шляхом направлення повідомлень по електронній пошті або по факсу. 8.2. Контрагент зобов'язується самостійно ознайомлюватися з повідомленнями Банку, які йому було надіслано у порядку, що визначено у пункті 8.1. Загальних Умов, але не рідше ніж один раз на місяць. 8.3. Інші повідомлення, що направляє одна Сторона іншій згідно з Договором або в ході його виконання (надалі – Повідомлення), повинні бути оформлені в письмовій формі, українською мовою або українською з англійською мовами одночасно, в залежності як-ою/-ими мов-ою/-ами було укладено Договір, і будуть вважатися направленими належним чином, якщо вони відправлені поштовим зв'язком (рекомендованим листом, листом з оголошеною цінністю з описом вкладення або іншим листом, доставка якого може бути документально підтверджена), доставлені особисто однією із Сторін іншій Стороні чи кур'єрською доставкою за вказаними в Договорі адресами/реквізитами Сторін Договору, направлені по факсу, а також за допомогою системи «Клієнт-Банк»/іншої системи, яку використовують Сторони, якщо така можливість передбачена умовами окремого договору між Банком та Контрагентом. 8.3.1. Якщо у реквізитах Контрагента зазначено декілька адрес, Банк надсилає Повідомлення за адресою, яка	8.1. The Bank's notice to the other Party, regarding the Bank's Counterparties and does not contain information constituting banking secrecy or confidential information of the counterparty, may be sent by the Bank to the counterparty by posting a notice in the Bank's branch and/or on the Bank's official website and/or in any official print media, in which the laws and other acts of the Verkhovna Rada of Ukraine and/or acts of the President of Ukraine are officially promulgated, and/or by sending notices by e-mail or by fax. 8.2. The counterparty undertakes to independently familiarize itself with the messages of the Bank that were sent to it in the manner specified in clause 8.1. of the General Conditions, but at least once a month. 8.3. Other notices sent by one Party to another under the Agreement or during its implementation (hereinafter referred to as the Notices) must be made in writing, in Ukrainian or Ukrainian and English at the same time, depending on the language(s) in which the agreement was concluded, and will be considered to be sent properly if they are sent by post (registered mail, letter of declared value with a list of enclosures, or another letter, the delivery of which can be documented), delivered personally by one of the Parties to the other Party or by courier delivery to the addresses/details of the Parties to the Agreement specified in the Agreement, sent by fax, as well as using the Client-Bank system/other system used by the Parties, if this is possible under the terms of a separate agreement between the Bank and the Counterparty. 8.3.1. If several addresses are indicated in the details of the Counterparty, the Bank sends a Message to the address located in the territory of Ukraine (except for the territory of the JFO and the temporarily occupied territory).

значиться на території України (за винятком території проведення ООС і тимчасово окупованої території). 8.4. Повідомлення, які надіслані поштою або службою кур'єрської доставки, вважається одержаним іншою Стороною в день, зазначений в квитанції чи іншому документі із штемпелем відділення поштового зв'язку або служби кур'єрської доставки, отриманим відправником Повідомлення, про відправлення Повідомлення. Повідомлення, які надіслані за допомогою системи «Клієнт-Банк» / іншої системи, яку використовують Сторони, за умови, що система підтвердила успішність доставлення такого відправлення, вважаються отриманими у дату відправлення Повідомлення. 8.5. Повідомлення, доставлені телеграфом, по телетайпу, телефаксу, факсу, якщо інше не домовлено між Сторонами, носять попередній характер і повинні бути в подальшому направлені відповідно до вимог пункту 8.4. Загальних Умов. 8.6. Сторони зобов'язані невідкладно повідомляти один одного про будь-які події, факти, упущення або помилки, які є істотними для відносин між ними, та невідкладно надавати відповідь на будь-які запити, що вони надсилають одне одному стосовно таких подій, фактів, упущень або помилок. 8.7. Протягом дії Договору кожна Сторона зобов'язується негайно повідомляти іншу Сторону про появу факту або обставини, що стали їй відомими, які можуть привести до необхідності зміни умов Договору, порушення або зміни зобов'язань, заяв або гарантій Сторін, викладених у Договорі.	8.4. The messages sent by mail or courier delivery service are considered to have been received by the other Party on the day specified in the receipt or other document with the postmark of the post office or courier delivery service received by the sender of the message about sending the message. Messages sent using the client-bank system / other system used by the Parties, provided that the system has confirmed the success of such delivering, are considered received on the date of sending the message. 8.5. Notices delivered by telegraph, teletype, fax, telefax, unless otherwise agreed between the Parties, are preliminary in nature and should be sent in accordance with the requirements of clause 8.4. of the General Conditions. 8.6. The parties are obliged to immediately notify each other of any events, facts, omissions or errors that are essential to the relationship between them, and to provide an immediate response to any requests, they send to each other regarding such events, facts, omissions or errors. 8.7. During the term of the Agreement, each Party undertakes to immediately inform the other Party of the occurrence of a fact or circumstance that has become known to it, which may lead to the need to amend the terms of the Agreement, violation or change of the obligations, representations or warranties of the Parties set forth in the Agreement.
9. КОНФІДЕНЦІЙНІСТЬ. БАНКІВСЬКА ТАЄМНИЦЯ	9. CONFIDENTIALITY. BANKING SECRECY
9.1. Сторони зобов'язуються зберігати в межах, визначених Законодавством, конфіденційність стосовно змісту Договору, а також будь-якої інформації та відомостей, що надаються кожній зі Сторін у зв'язку з виконанням Договору. 9.2. Вказана вимога про нерозголошення конфіденційної інформації поширюється на всіх співробітників Сторін та залучених ними третіх осіб, задіяних при виконанні Договору. 9.3. Вимога про нерозголошення конфіденційної інформації, вказана вище діє протягом усього строку дії Договору, а також протягом 5-ти наступних років з моменту припинення його дії. 9.4. Сторони зобов'язуються належним чином зберігати та не розголошувати інформацію, яка містить банківську таємницю, отриману при виконанні умов Договору. Передача такої інформації третім особам, за винятком уповноважених осіб і організацій, можлива лише з письмової згоди іншої Сторони, а також у випадках, передбачених Законодавством України та/або Договором. 9.4.1. Банк цим гарантує Контрагенту збереження банківської таємниці щодо операцій, проведених Банком відповідно до Договору, відомостей про Контрагента, що стали відомі Банку у зв'язку з укладенням Договору,	9.1. The Parties undertake to keep confidential the content of the Agreement, as well as any information and data provided by each of the Parties in connection with the implementation of the Agreement, within the limits established by the Legislation. 9.2. The specified requirement of non-disclosure of confidential information applies to all employees of the Parties and third parties involved by them in the implementation of the Agreement. 9.3. The requirement of non-disclosure of confidential information specified above is valid for the entire duration of the Agreement, as well as for the next 5 years from the date of its termination. 9.4. The parties undertake to appropriately store and not disclose information containing banking secrecy obtained in fulfilling the terms of the Agreement. The transfer of such information to third parties, with the exception of authorized persons and organizations, is possible only with the written consent of the other Party, as well as in cases provided by the Legislation of Ukraine and/or the Agreement. 9.4.1. The Bank hereby guarantees the Counterparty to maintain banking secrecy in transactions carried out by the Bank in accordance with the Agreement, information about the Counterparty that the Bank became aware in connection with the conclusion of the Agreement, and other information

інших відомостей, що становлять банківську таємницю відповідно до Законодавства. 9.4.2. Контрагент розуміє, що незважаючи на п. 9.4.1. Загальних Умов, Банк зобов'язаний розкривати інформацію, що становить банківську таємницю, на вимоги державних органів у випадках та в порядку, передбаченому Законодавством. Ніякі зобов'язання Банку в зв'язку із збереженням банківської таємниці та конфіденційної інформації, викладені в Договорі або в інших договорах (угодах, протоколах, листах) Банку з Контрагентом, не розповсюджуються на випадки, коли Банк вимушений на свій розсуд передавати таку інформацію третім особам (включаючи адвокатів, факторингові та колекторські компанії, в тому числі надання контролюючим органам інформації та її документального підтвердження стосовно виконання Банком вимог податкового Законодавства, тощо) для захисту своїх інтересів та/або у випадку порушення Контрагентом своїх обов'язків за Договором перед Банком. 9.4.3. Контрагент надає Банку дозвіл на розголошення банківської таємниці та конфіденційної інформації, що містяться в Договорі або в інших договорах (угодах, протоколах, листах) Банку з Контрагентом, або іншим чином робити інформацію доступною своїм працівникам, компаніям, з якими Банк перебуває в договірних відносинах, їх працівникам та зовнішнім (юридичним, аудиторським) консультантам в тій мірі, в якій це необхідно для забезпечення виконання Договору або іншого договору між Сторонами, а також з метою захисту прав Банку за Договором та/або іншим договором між Сторонами, здійснення таких прав або примусового забезпечення їх виконання. Крім того, Банк має право збирати, зберігати, використовувати та розголошувати (розкривати / поширювати) у будь-який спосіб інформацію про Контрагента, що містить банківську та/або комерційну таємницю, наступним особам: бюро кредитних історій, користувачем якого(их) є Банк; та/або аудитор(ам) та/або аудиторській(им) фірмі(ам) під час здійснення ним(и) аудиторської діяльності відносно Банку та/або Контрагента; та/або архівній(им) установі(ам), що забезпечує(ють) облік та зберігання документів для Банку; та/або рейтинговим агентствам та/або фінансовим та/або юридичним радникам / консультантам для цілей рейтингування Банку та/або будь-якої з пов'язаних осіб щодо Банку; та/або міжнародному(им) фінансовому(им) інституту(ам) / організації(ям) та/або іноземному(им) банку(ам); та/або будь-яким контрагентам Банку за документами забезпечення, які укладені на забезпечення зобов'язань Контрагента за Договором; та/або за обставини настання випадку невиконання Контрагентом умов Договору та/або документів забезпечення, укладених для забезпечення виконання зобов'язань за Договором (за наявності), будь-якій третій особі. 9.4.4. Контрагент також надає Банку право надавати на запит банку-кореспондента інформацію, яка стосується	constituting banking secrecy in accordance with the Legislation. 9.4.2 The Counterparty understands that despite clause 9.4.1. of the General Conditions, the Bank is obliged to disclose information constituting bank secrecy, upon the requests of state authorities in cases and in the manner prescribed by Legislation. No obligations of the Bank in connection with the maintenance of bank secrecy and confidential information set forth in the Agreement or in other agreements (contracts, protocols, letters) of the Bank with the Counterparty shall apply to cases when the Bank is forced to transfer such information to third parties (including lawyers, factoring and debt collection companies, including the provision of information and documentary evidence to the regulatory authorities on the Bank's compliance with tax legislation, etc.) to protect their interests and/or in case of violation by the Counterparty of its obligations under the Agreement to the Bank. 9.4.3. The Counterparty grants the Bank permission to disclose banking secrecy and confidential information contained in the Agreement or in other agreements (contracts, protocols, letters) of the Bank with the Counterparty, or otherwise make information available to its employees, companies with which the Bank is in a contractual relationship, their employees and external (legal, audit) consultants to the extent necessary to ensure the implementation of the Agreement or other agreement between the Parties, as well as to protect the Bank's rights under the Agreement and / or other agreement between the Parties, by the exercise of such rights, or the enforcement of their implementation. In addition, the Bank has the right to collect, store, use and make public (disclose / distribute) in any way information about the Counterparty containing banking and/or commercial secrets to the following persons: credit reference bureau, the user of which the Bank is; and/or to the auditor(s) and/or audit firm(s) in the course of its (their) audit activities in relation to the Bank and/or Counterparty; and/or archival institution(s), which provides accounting records and storage of documents for the Bank; and/or rating agencies and/or financial and/or legal advisers / consultants for the purposes of rating the Bank and/or any of the related parties regarding the Bank; and/or international financial institution(s) / organization(s) and/or foreign bank(s) and/or any counterparties of the Bank under security documents concluded to secure the obligations of the Counterparty under the Agreement; and/or subject to the occurrence of a case of non-fulfilment by the Counterparty of the terms of the contract and/or security documents concluded to ensure the fulfilment of obligations under the Agreement (if any), to any third party. 9.4.4. The Counterparty also grants the Bank the right to provide, at the request of the correspondent bank, information relating to the identification of the Counterparty and/or transactions carried out in favor of or on behalf of the Counterparty, at the corresponding request of the bank involved in ensuring such operations.
--	--

ідентифікації Контрагента та/або операцій, що здійснюються на користь або за дорученням Контрагента, на відповідний запит банку, який бере участь у забезпеченні проведення таких операцій. 9.4.5. Банк є частиною групи ОТП в яку входять ОТП Банк (Угорщина), його місцеві та іноземні філії та їх дочірні компанії (Група ОТП). Компанії Групи ОТП постійно обмінюються інформацією через загальну інформаційну систему, завданням якої є мінімізація ризику групи в цілому. Контрагент надає дозвіл на отримання, використання та розголошення інформації в середині Групи ОТП, що стосується безпосередньо Контрагента (для оцінки ризику), що стала відома Банку у зв'язку з діловими стосунками з Контрагентом. Цей дозвіл поширюється на Банк, інших членів Групи ОТП в Угорщині та за її межами, які організовані та функціонують як єдиний банк. Контрагент дає дозвіл Банку на передачу для конфіденційного використання інформації про нього та/або будь-яку його дочірню компанію в середині Групи. Зазначена інформація може передаватися, зокрема, у зв'язку з наданням Контрагенту будь-якої послуги чи банківського продукту, а також в цілях обробки даних, проведення статистичного аналізу та аналізу ризиків. Цей дозвіл знімає будь-які претензії Контрагента щодо порушення Банком положень про нерозголошення банківської таємниці, які існують у Законодавстві. 9.4.6. Якщо в ході виконання Контрагентом своїх зобов'язань за Договором йому стане відома інформація, що містить банківську таємницю, така інформація не може бути розкрита Контрагентом третім особам ні в якому випадку і ні за якою умовою. 9.4.7. Сторони, шляхом підписання Договору, дозволяють одна одній відсилати документи та інформацію, яка стосується Договору, через відкритий канал мережі Інтернет на вказану Сторонами електронну адресу електронної пошти. У таких випадках, Сторони не несуть відповідальність за можливе розголошення конфіденційної інформації та/або банківської таємниці третім особам, що відбулося внаслідок надсилання Сторонами конфіденційної інформації та/або банківської таємниці через відкритий канал мережі Інтернет на вказану Сторонами адресу електронної пошти.	9.4.5. The Bank is part of the OTP group, which includes OTP Bank Plc. (Hungary), its local and foreign branches and their subsidiaries (OTP Group). OTP Group companies constantly exchange information through a common information system, the task of which is to minimize the risk of the group as a whole. The Counterparty gives permission to receive, use and disclose information relating the Counterparty directly (for risk assessment), which became known to the Bank in connection with business relations with the Counterparty, within the OTP Group. This permission applies to the Bank, other members of the OTP Group in Hungary and abroad, which are organized and operate as a single bank. The Counterparty gives the Bank permission to transfer information about it and / or any of its subsidiaries within the Group for confidential use. The specified information may be transmitted, in particular, in connection with the provision of any service or banking product to the Counterparty, as well as for the purpose of processing data, conducting statistical and risk analysis. This permission removes any claims of the Counterparty regarding the Bank's violation of provisions on non-disclosure of bank secrecy that exist in the Legislation. 9.4.6. If, in the course of fulfillment of obligations under the Agreement by the Counterparty, it becomes aware of information containing bank secrecy, such information can be in no case and under no condition disclosed by the Counterparty to third parties. 9.4.7. By signing the Agreement, the Parties allow each other to send documents and information regarding the Agreement through an open Internet channel to the email address indicated by the Parties. In such cases, the Parties are not responsible for the possible disclosure of confidential information and/or banking secrecy to third parties, which occurred as a result of the transfer of confidential information and/or banking secrecy by the Parties through an open Internet channel to the email address specified by the Parties.
10. ВРЕГУЛЮВАННЯ СПОРІВ	10. DISPUTE SETTLEMENT
10.1. Будь-які суперечки, розбіжності, вимоги або претензії, що виникають з Договору розглядаються шляхом проведення переговорів, а у випадку недосагнення згоди - в судових органах та в порядку, визначеному Законодавством. 10.2. Договір регулюється правом України.	10.1. Any disputes, disagreements, demands or claims arising from the Agreement are resolved through negotiations, and in case of failure to reach agreement, in the judicial authorities and in the manner specified by the Legislation. 10.2. The Agreement is regulated by the Law of Ukraine.
11.ЗВІЛЬНЕННЯ ВІД ВІДПОВІДАЛЬНОСТІ. ФОРС-МАЖОР (НЕПЕРЕБОРНА СИЛА)	11. RELEASE OF LIABILITY. FORCE MAJEURE (IRRESISTABLE FORCE)
11.1. Сторони звільняються від відповідальності за часткове або повне невиконання своїх зобов'язань за Договором у разі настання та дії обставин непереборної сили, що знаходяться поза межами контролю Сторін, та які Сторони не могли передбачити або яким не могли	11.1. The Parties are released from liability for partial or full failure to fulfil their obligations under the Agreement in the event of force majeure circumstances that are beyond the control of the Parties and which the Parties could not foresee or prevent. In this context, force majeure means: a) natural

запобігти. У цьому контексті обставини непереборної сили означають: а) стихійне лихо (пожежа, вибух, повінь, землетрус), природні та неприродні катастрофи та інші обставини, непередбачені та які є поза контролем Банку; б) війну (оголошену чи неоголошену), військові дії, окупацію, акти тероризму, громадянську війну, акти громадської непокори, революції, громадські безпорядки, громадські заворушення, повстання, страйки, в) дії, вимоги або обмеження, що їх встановлює для Банку Уряд України або інші треті сторони, у тому числі встановлені Урядом обмеження на доступ до рахунків, іноземної валюти або банківського законодавства України або його тлумачення у тих межах, у яких вони можуть завадити Банку у виконанні його обов'язків, діяння будь-якого національного, іноземного або міжнародного урядового або іншого контролюючого органу, націоналізацію, експропріацію, вихід з ладу (збої) в платіжній системі, в тому числі в Системі електронних платежів НБУ, заходи, що вживаються будь-яким урядом або НБУ або іншим повноважним органом, валютні обмеження, заборони чи обмеження щодо переказу коштів або такі, що стосуються банківської діяльності в цілому, дії чи заходи урядових органів, установ, організацій, або офіційних осіб в Україні або за кордоном (незалежно від того, чи діє цей урядовий орган, установа, організація або офіційна особа в межах своїх повноважень), незаконні дії третіх осіб. 11.2. Сторона не звільняється від відповідальності за несвоєчасне виконання зобов'язань, якщо обставини непереборної сили, визначені п. 11.1. Загальних Умов, настали у період прострочення виконання боргових зобов'язань. 11.3. Сторона зобов'язана повідомити іншу Сторону про настання та припинення дії обставин непереборної сили, з наданням підтвердження Торгово-промислової палати України, протягом 3-х робочих днів від дати настання або припинення їх дії. Недотримання строків повідомлення про настання обставин непереборної сили позбавляє Сторону права посилаючись на такі обставини як підставу звільнення від відповідальності. 11.4. У разі настання обставин, визначених п. 11.1. Загальних Умов, термін виконання зобов'язань за Договором подовжується на строк дії таких обставин, але не більше як на 1 місяць. 11.5. Якщо обставини, визначені п. 11.1. Загальних Умов, діятимуть понад 1 місяць, відповідна Сторона за Договором зобов'язана протягом 5-ти робочих днів від закінчення строку, визначеного п. 11.4. Загальних Умов, погасити заборгованість за Договором. Застереження: Сторони домовились, що письмове повідомлення Контрагента про настання обставин непереборної сили Банк здійснює шляхом розміщення відповідної інформації в операційних залах установ Банку та на Офіційному сайті Банку.	disaster (fire, explosion, flood, earthquake), natural and unnatural disasters and other circumstances unforeseen and beyond the control of the Bank; b) war (declared or undeclared), hostilities, occupation, acts of terrorism, civil war, acts of civil disobedience, revolution, public unrest, riots, uprisings, strikes, c) actions, requirements or restrictions established by the Government of Ukraine or other third parties for the Bank, including restrictions imposed by the Government on access to the accounts, foreign currency or banking legislation of Ukraine or its interpretation to the extent that they may interfere with the performance of Bank's duties, actions of any national, foreign or international governmental or other regulatory body, nationalization, expropriation, failure (malfunctions) of the payment system, including the NBU Electronic Payment System, measures taken by any government or NBU or other authorized body, currency restrictions, prohibitions or restrictions on the transfer of funds or those that relate to banking activities in general, actions or measures of government bodies, institutions, organizations or officials in Ukraine or abroad (regardless of whether this a governmental body, institution, organization or official acts within its powers), illegal actions of third parties. 11.2. The Party is not released from liability for untimely fulfilment of obligations if force majeure circumstances specified in clause 11.1. of the General Conditions occurred during the period of delay in the fulfilment of debt obligations. 11.3. A Party shall notify the other Party of the occurrence and termination of force majeure circumstances, with the confirmation of the Chamber of Commerce and Industry of Ukraine, within 3 working days from the date of their occurrence or termination. Failure to comply with the terms for notification of the occurrence of force majeure circumstances deprives the Party of the right to invoke such circumstances as the basis for release of liability. 11.4. In the event of circumstances specified in clause 11.1. of the General Conditions, the term for fulfilment of obligations under the Agreement is extended for the duration of such circumstances, but not more than 1 month. 11.5. If the circumstances specified in clause 11.1. of the General Conditions last for more than 1 month, under the Agreement the Party is obliged to pay off the debt under the Agreement within 5 business days from the date of expiration of the period specified in clause 11.4. of the General Conditions. Caution: The Parties agreed that the Bank makes a written notice for the Counterparty about the occurrence of force majeure circumstances by posting relevant information in the operating rooms of the Bank's institutions and on the Bank's official website.
12. ФІНАНСОВИЙ МОНІТОРИНГ	12. FINANCIAL MONITORING

12.1. Контрагент розуміє, що Банк є суб'єктом первинного фінансового моніторингу і зобов'язаний надавати відповідному уповноваженому органу держави інформацію про фінансові операції Контрагента, що підлягають фінансовому моніторингу, та здійснювати інші передбачені Законодавством дії, пов'язані з моніторингом фінансових операцій Контрагента, в тому числі відмовитися від здійснення фінансової операції Контрагента, якщо вона порушує Законодавство щодо протидії легалізації доходів, одержаних злочинним шляхом. В такому випадку Банк звільняється від відповідальності (в тому числі від сплати неустойки та збитків) за відмову від здійснення відповідної фінансової операції Контрагента чи припинення співпраці за Договором. Контрагент погоджується з тим, що Банк має право відмовитися від виконання Договору з вищевикладених підстав та ініціювати дострокове розірвання Договору за ініціативою Банку.	12.1. The Counterparty understands that the Bank is the subject of initial financial monitoring and is obliged to provide information on the financial transactions of the Counterparty subject to financial monitoring to the relevant authorized state body and to carry out other actions provided by the Legislation related to monitoring the financial transactions of the Counterparty, including to refuse to carry out the financial transactions of the Counterparty if it violates the law on anti-money laundering. In this case, the Bank is released from liability (including from payment of forfeit and losses) for refusing to carry out the Counterparty's financial transaction or terminating cooperation under the Agreement. The Counterparty agrees that the Bank has the right to refuse to implement the Agreement on the above grounds and to initiate early termination of the Agreement at the initiative of the Bank.
13. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ	13. PERSONAL DATA PROTECTION
13.1. Я, Власник персональних даних (особа, уповноважена на підписання Договору однією із Сторін), повідомлений про мету обробки іншою Стороною моїх персональних даних (будь-яка інформація про фізичну особу або інформація, що стосується фізичної особи, в тому числі, однак не виключно інформація щодо прізвища, імені, по батькові, даних, які зазначені в паспорті (або даних, які зазначені в іншому документі, що посвідчує особу), реєстраційного номеру облікової картки платника податків, громадянства, місця проживання або перебування, місця роботи, посади, номерів контактних телефонів/факсів, адреси електронної пошти, тощо, надалі – Персональні дані) а саме: укладення, зміни, припинення договорів, виконання договорів, а також для здійснення дій, пов'язаних із укладенням, зміною, припиненням та/або виконанням договорів, у тому числі шляхом здійснення прямих контактів із Власником персональних даних за допомогою засобів зв'язку; захисту іншою Стороною своїх прав та інтересів. 13.2. Підписанням Договору Власник персональних даних однієї Сторони дає свою згоду на передачу (поширення), у т.ч. транскордонну, іншою Стороною Персональних даних Третім особам (особи, з якими інша Сторона перебуває у договірних відносинах та/або члени материнської групи іншої Сторони), зміну, знищення Персональних даних або обмеження доступу до них відповідно до вимог Закону України «Про захист персональних даних» (надалі – Закон) та без необхідності надання Власнику персональних даних письмового повідомлення про здійснення зазначених дій. 13.3. Підписанням Договору Власник персональних даних кожної Сторони підтверджує, що в момент збору Персональних даних інша Сторона повідомила його про володільця Персональних даних, склад та зміст зібраних Персональних даних, права, передбачені Законом, про мету збору Персональних даних та осіб, яким передаються його Персональні дані.	13.1. I, the Owner of personal data (a person authorized to sign an Agreement by one of the Parties), is informed of the purpose of processing of my personal data (any information about an individual or information relating to an individual, including, but not limited to, information on surname, name, patronymic, data indicated in the passport (or data indicated in another identification document), registration number of the taxpayer registration card, citizenship, place of residence or stay, place of employment, position, contact telephone/fax numbers, e-mail addresses, etc., hereinafter referred to as the Personal Information) by the other Party, namely: conclusion, amendment, termination of agreements, implementation of agreements, as well as for the performance of actions related to conclusion, amendment, termination and / or implementation of agreements, including through direct contacts with the Owner of personal data using communication tools; protecting of own rights and interests by the other Party. 13.2. By signing the Agreement, the Owner of the personal data of one Party gives his consent to the transfer (distribution), incl. cross-border, of personal data by the other Party to third parties (persons with whom the other Party is in a contractual relationship and/or members of the parent group of the other Party), change, destruction of personal data or restricting access to them in accordance with the requirements of the Law of Ukraine "On Personal Data Protection" (Hereinafter - the Law) and without the need to provide the Owner of personal data with a written notice on the performance of these actions. 13.3. By signing the Agreement, the Owner of the personal data of each Party confirms that at the time of the collection of personal data, the other Party informed him about the keeper of the personal data, the composition and content of the collected personal data, the rights stipulated by law, the purpose of collecting personal data and the persons to whom his personal data is transmitted.

13.4. Сторона підтверджує (гарантує), що Персональні дані фізичних осіб, які передаються іншій Стороні, здійснюється за згодою таких фізичних осіб і такі особи повідомлені про відомості, зазначені в ч.2 ст.12 Закону.

13.5. У разі, якщо умовами Договору передбачено передача Сторонами одна одній Персональних даних фізичних осіб, Сторони беруть на себе зобов'язання:

13.5.1. Забезпечувати виконання вимог щодо режиму доступу, обробки та захисту Персональних даних, які вони отримують для та/або у зв'язку з виконанням Договору, зокрема вимог Закону;

13.5.2. Не допускати несанкціонованого доступу до Персональних даних не уповноваженими особами з числа співробітників Сторін, а також будь-якими третіми особами внаслідок незабезпечення належних заходів зберігання/режиму зберігання Персональних даних, невжиття інших заходів обмеження доступу до Персональних даних, які Сторона повинна вжити з метою виконання умов Договору та відповідно до Закону;

13.5.3. У строк, який є мінімально можливим, але не більше 24 годин з моменту настання події, інформувати іншу Сторону про всі події, пов'язані з фактами розголошення або порушення конфіденційності Персональних даних.

13.5.4. Вимоги щодо нерозголошення, зазначені у пп. 13.5.1.- 13.5.2. Загальних Умов, розповсюджуються на всіх співробітників Сторін, які у зв'язку з виконанням своїх службових (посадових) обов'язків мають доступ до Персональних даних. Якщо до виконання Договору або виконання робіт згідно з умовами Договору Сторони залучають Третіх осіб, вимоги пп. 13.5.1.- 13.5.2. Загальних Умов у повній мірі розповсюджуються на таких осіб. Сторони зобов'язані офіційно довести вимоги Договору/Загальних Умов до таких Третіх осіб.

13.5.5. Сторони зобов'язуються запровадити та належно застосовувати заходи безпеки щодо забезпечення конфіденційності Персональних даних під час здійснення між ними інформаційного обміну, у тому числі забезпечити шифрування Персональних даних в процесі їх поширення відкритими каналами зв'язку та мережами передачі даних. Вимоги щодо заходів безпеки та засобів захисту інформації можуть погоджуватися Сторонами в окремому порядку. Вищезазначені заходи повинні бути запроваджені Сторонами до початку інформаційного обміну Персональними даними.

13.5.6. Якщо інше не передбачено Законодавством та умовами Договору/Загальних Умов, у строк, який є мінімально можливим, але не більше 5-ти робочих днів після закінчення строку дії або припинення Договору, а також після отримання письмової вимоги від однієї із Сторін, інша Сторона зобов'язується повернути Стороні, яка надіслала таку письмову вимогу, носії тих Персональних даних, які передані для та/або у зв'язку з виконанням Договору, не залишаючи у себе жодних копій (у тому числі електронних чи у формі картотек), а також відтворень чи витягів з документів, файлів, даних тощо, які зазначені як Персональні дані, якщо інше не

13.4. The Party confirms (guarantees) that the transfer of Personal data of individuals to the other Party is carried out by agreement of such individuals and they are notified of the information specified in part 2 of article 12 of the Law.

13.5. In the event that the terms of the Agreement provide for the transfer Personal data of individuals by the Parties to each other, the Parties undertake:

13.5.1. to ensure compliance with the requirements for access, processing and protection of Personal data that they receive for and/or in connection with the implementation of the Agreement, in particular the requirements of the Law;

13.5.2. To prevent unauthorized access to personal data by unauthorized persons from among the employees of the Parties, as well as by any third parties due to the failure to provide appropriate measures for storage/storage mode of personal data, and other measures to restrict access to personal data that the Party should take in order to fulfil the conditions of the Agreement and in accordance with the Law;

13.5.3. To inform the other Party of all events related to the disclosure or violation of the confidentiality of personal data within the time period that is the minimum possible, but no more than 24 hours from the moment the event occurred.

13.5.4. The requirements for non-disclosure specified in sub-clauses 13.5.1.- 13.5.2. of the General Conditions apply to all employees of the Parties who have access to personal data in connection with the performance of their official (position) duties. If the Parties involve third parties in the performance of the Agreement or work according to the conditions of the Agreement, the requirements of sub-clauses 13.5.1. - 13.5.2. of the General Conditions fully apply to such persons. Parties are required to formally communicate the requirements of the Agreement / General Conditions to such third parties.

13.5.5. The parties undertake to introduce and duly apply security measures to ensure the confidentiality of personal data when exchanging information, including ensuring the encryption of personal data during its distribution through open communication channels and data transmission networks. The requirements for security measures and information protection means may be agreed by the Parties separately. The above measures should be introduced by the Parties before the exchange of personal data begins.

13.5.6. Unless otherwise provided by the Legislation and the conditions of the Agreement/General Conditions, within the period that is the minimum possible, but not more than 5 working days after the expiration or termination of the Agreement, and also after receiving a written request from one of the Parties, the other Party returns to the Party that sent such a written request, the carriers of the personal data that were transferred for and/or in connection with the implementation of the Agreement, without retaining any copies (including electronic or in the form of a card file), as well as reproductions or extracts from documents, files, data, etc., which are indicated as Personal Data, unless otherwise provided by the Legislation or the conditions of consent of the personal data subject.

передбачено Законодавством або умовами згоди суб'єкта персональних даних.	
14. СТРОК ДІЇ ДОГОВОРУ. ЗМІНИ ТА РОЗІРВАННЯ ДОГОВОРУ/ ЗАГАЛЬНИХ УМОВ	14. TERM OF THE AGREEMENT. AMENDMENTS AND TERMINATION OF THE AGREEMENT / GENERAL CONDITIONS
14.1.Строк дії Договору зазначається Сторонами у індивідуальній частині Договору. Сторони можуть визначити строк дії Договору у публічній частині Договору (Загальних Умовах), зазначивши про це в індивідуальній частині Договору. Договір не поширюється на зобов'язання, що виникли у Сторін до укладення ними Договору, якщо інше прямо не передбачене Договором. Закінчення строку дії Договору не звільняє Сторони від відповідальності за його порушення, що мало місце під час дії Договору. 14.2.У разі, якщо за 15 календарних днів до моменту припинення строку дії Договору жодна із Сторін не заявить про його розірвання, то Договір вважається продовженим (продлонгованим) на кожний наступний календарний рік. Дана процедура пролонгації застосовується в кожному випадку спливу строку дії Договору, якщо інше не визначено Сторонами у індивідуальній частині Договору. 14.3. Договір може бути достроково розірваний за ініціативою будь-якої із Сторін у випадках, визначених Загальними Умовами, шляхом відправлення іншій Стороні письмового повідомлення з підписом уповноваженої особи Сторони з проставленням печатки (за умови її використання), якщо інше не визначено Сторонами у індивідуальній частині Договору. Таке письмове повідомлення надсилається Сторонами у порядку, визначеного розділом «8. Повідомлення» Загальних Умов, не пізніше ніж за 15 календарних днів до запланованої дати розірвання Договору, якщо інше не визначено Сторонами у індивідуальній частині Договору. 14.4. Всі зміни та доповнення до індивідуальної частини Договору оформлюються Сторонами у письмовій формі, у вигляді договорів про внесення змін та доповнень (додаткових угод), які повинні бути підписані уповноваженими представниками обох Сторін та скріплені відбитками печаток Сторін (у разі їх використання). Всі зміни і доповнення до Договору є його невід'ємними частинами. 14.5. Банк має право в односторонньому порядку відповідно до статті 651 Цивільного кодексу України змінювати та/або доповнювати умови публічної частини Договору (Загальних Умов), шляхом розміщення таких змін на Офіційному сайті Банку за 30 календарних днів до дати набрання чинності таких змін/доповнень. 14.6. У разі відсутності письмових заперечень зі сторони Контрагента щодо запропонованих Банком змін/доповнень до публічної частини Договору (Загальних Умов), поданих до Банку до вступу в дію згаданих змін/доповнень, Контрагент вважається таким, що прийняв та погодився із запропонованими Банком змінами/доповненнями до публічної частини Договору (Загальних Умов).	14.1. The Parties shall specify the term of the Agreement in the individual part thereof. The Parties may set the term of the Agreement in the public part thereof (General Conditions) specifying the same in the individual part of the Agreement. The Agreement shall not cover obligations of the Parties arisen before the date of the Agreement unless otherwise expressly stipulated therein. Expiry of the Agreement shall not release the Parties from liability for violation occurred during the term of the Agreement. 14.2. If 15 calendar days before the expiry of the Agreement neither Party notifies of termination, then the Agreement shall be treated as renewed (extended) for each following calendar year. This procedure of renewal shall apply to each expiry of the Agreement unless otherwise stipulated by the Parties in the individual part of the Agreement. 14.3. The Agreement may be early terminated upon the initiative of any of the Parties in cases determined by the General Conditions by a written notice sent to the other Party and signed by the authorized representatives of the Party and affixed with the seal (if any) unless otherwise determined by the Parties in the individual part of the Agreement. Such written notice shall be sent to the Parties as specified in Section 8 (Notices) of the General Conditions not later than 15 calendar days before the scheduled termination date unless otherwise stipulated by the Parties in the individual part of the Agreement. 14.4. All amendments and additions to the individual part of the Agreement are executed by the Parties in writing, in the form of agreements on amendments and additions (supplementary agreements), which must be signed by authorized representatives of both Parties and sealed with stamps of the Parties (if used). All amendments and additions to the Agreement are its integral parts. 14.5. In accordance with Article 651 of the Civil Code of Ukraine, the Bank has the right to unilaterally amend and/or supplement the conditions of the public part of the Agreement (General Conditions) by posting such amendments on the Bank's official website 30 calendar days prior to the date of entry into force of such amendments/additions. 14.6. In the absence of written objections from the Counterparty regarding the amendments/additions proposed by the Bank in the public part of the Agreement (General Conditions) submitted to the Bank before the said amendments/additions take effect, the Counterparty is deemed to have accepted and agreed with the amendments/additions to the public part of the Agreement proposed by the Bank (General Conditions). 14.7. If the Counterparty does not agree with new amendments/additions to the public part of the Agreement (General Conditions), it has the right to bring the agreement to an early termination and provide the Bank with a written

14.7. Якщо Контрагент не згоден з новими змінами/доповненнями до публічної частини Договору (Загальних Умов), він має право достроково розірвати Договір з наданням Банку відповідного письмового повідомлення за **30 календарних днів** до дати такого припинення, попередньо виконавши всі зобов'язання перед Банком, встановлені Договором/Загальними Умовами. В іншому випадку такі зміни вважаються прийнятими Контрагентом.

14.8. Контрагент зобов'язується самостійно ознайомлюватися з повідомленнями Банку та/або змінами/доповненнями до публічної частини Договору (Загальних Умов), що розміщуються на Офіційному сайті Банку, але не рідше ніж **1 раз на місяць**.

14.9. Шляхом підписання індивідуальної частини Договору, Контрагент підтверджує, що він в день укладення Договору особисто отримав свій примірник індивідуальної частини Договору, а також ознайомлений та згодний із Загальними Умовами.

notice **30 calendar days** prior to the date of such termination, after having fulfilled all obligations to the Bank established by the Agreement / General Conditions. Otherwise, such amendments are considered accepted by the Counterparty.

14.8. The Counterparty undertakes to independently familiarize itself with the Bank's notices and/or amendments/additions to the public part of the Agreement (General Conditions) posted on the Bank's official website, but at least **1 time per month**.

14.9. By signing the individual part of the Agreement, the Counterparty confirms that on the day of conclusion of the Agreement he personally received his copy of the individual part of the Agreement, as well as he is familiar with and agrees to the General Conditions.