Outsourcing Supplement - Annex DORA

1. SUBJECT MATTER OF THE ANNEX

1.1. This Annex (the "**Annex**") regulates the obligations and obligations of the Parties to the Agreement, taking into account the requirements arising from Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 ("**DORA").**

1.2. The Annex may be extended to include regulatory technical standards ("**RTS**") published by competent authorities based on the provisions of DORA.

1.3. The Annex also takes into account the following guidelines from supervisory authorities:

1.3.1. announcement of the Polish Financial Supervision Authority on the processing of information by supervised entities in public or hybrid cloud computing of 23 January 2020 ("**Cloud Communication**");

1.3.2. European Banking Authority's Guidelines on Outsourcing of 25 February 2019, EBA/GL/2019/02 (the "**EBA Guidelines**").

1.4. The Parties have decided to assume the obligations and obligations set out in the Annex, due to the fact that NTT Poland sp. z o.o. with its seat in Warsaw, Poland, (hereinafter "**NTT**") provides services to the CONTRACTING AUTHORITY constituting "ICT services" within the meaning of Article 3(21) DORA ("**Services**"), referring to specific functions performed by the ORDERING PARTY, a detailed and exhaustive description of which (Services and functions) can be found in the Agreement/Order.

1.5. In the event of a conflict between the provisions of the Agreement and the Supplement, the provisions of the Appendix shall prevail.

1.6. The Parties declare that entrusting NTT by the ORDERING PARTY with the provision of Services will not adversely affect:

1.6.1. conducting business activity by the ORDERING PARTY in accordance with the law,

1.6.2. prudent and stable management of the ORDERING PARTY,

1.6.3. effectiveness of the internal control system at the ORDERING PARTY,

1.6.4. the ability to perform the duties of a statutory auditor authorized to audit the financial statements of the ORDERING PARTY on the basis of the agreement concluded with the ORDERING PARTY, and

1.6.5. protection of legally protected secrets.

1.7. NTT declares that the Services will be provided in accordance with the laws applicable to the CLIENT.

1.8. NTT declares that within the NTT Group:

1.8.1. It has the following certificates:

(a) PN-ISO/IEC ISO 20000 for IT service management;

(b) PN-EN ISO/IEC 27001 on information security management;

(c) PN-EN ISO 22301 on business continuity management;

(d) ISO/IEC 27017 on information security in cloud computing;

(e) ISO/IEC 27018 on good practices for securing personal data in cloud computing.

1.8.2. The CPD in which NTT processes data for the purposes of providing the Services meets the requirements of the PN-EN 50600 (Data Center Equipment and Infrastructure) minimum Class 3 or ANSI/TIA-942 minimum Tier III, or other standard appropriate and recognized for the assessment of CPD or containing requirements related to it - applies to CPD: Google, AWS and Azure.

2. DEFINITIONS

2.1. Capitalized terms in the Appendix shall have the meaning given to them in the Agreement and other Appendices to the Agreement, unless they are explicitly defined differently in the Appendix – in particular in this Chapter.

2.2. Notwithstanding the foregoing, the terms written below in lowercase letters shall be given the meaning indicated herein, in accordance with Article 3 of the DORA:

2.2.1. **digital operational resilience** means the ability of a financial entity to build, guarantee and verify its operational integrity and reliability by providing, directly or indirectly, through the services of ICT third-party service providers, the full range of ICT capabilities necessary to ensure the security of the network and information systems used by the financial entity and that support the continuous provision of financial services and their quality, including during disruptions;

2.2.2. **network and information systems** means (a) electronic communications networks, i.e. transmission systems, whether or not they are based on fixed infrastructure or centralised asset management, and, where applicable, switching or routing equipment and other assets, including inactive network elements, that enable the transmission of signals by wire, radio, optical means or other wave-based solutions, including satellite, fixed (switched and packet networks, including the Internet) and mobile networks, power cable systems, to the extent that they are used to transmit signals, in radio and television broadcasting networks and cable television networks, regardless of the type of information transmitted, or (b) a device or group of interconnected or related devices, of which at least one, automatically processes digital data; or (c) digital data stored, processed, retrieved, or transmitted by the items specified in points (a) and (b) for their use, use, protection, and maintenance;

2.2.3. **legacy ICT system** means an ICT system that has reached the end of its life cycle (end of life), which cannot be upgraded or repaired for technological and commercial reasons, or which is no longer operated by an ICT provider or third-party service provider, but which is still in use and supports the functions of the financial entity concerned;

2.2.4. **security of network and information systems** means the resilience of network and information systems, at a given level of trust, to any event that may compromise the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed, or services offered by or accessible through these networks and information systems;

2.2.5. **ICT risk** means any reasonably identifiable circumstance related to the use of network and information systems which, if it materialises, may jeopardise the security of network and information systems, any technology-dependent tool or process, the security of operations and processes or the provision of services by having adverse effects in the digital or physical environment;

2.2.6. **information resources** means a set of information, in tangible or intangible form, that is worth protecting;

2.2.7. **ICT asset** means software or computer resources in the network and information systems used by the financial entity;

2.2.8. **ICT-related incident** means a single event or a series of interrelated events, not planned by a financial entity, that compromise the security of network and information systems and adversely affect the availability, authenticity, integrity or confidentiality of data or services provided by that financial entity;

2.2.9. **major ICT-related incident** means an ICT-related incident with a high negative impact on network and information systems that support critical or essential functions of a financial entity;

2.2.10. **cyberthreat** means any potential circumstance, event or activity that may cause harm, disruption or otherwise adversely affect network and information systems, users of such systems and others;

2.2.11. **significant cyber threat** means a cyber threat whose technical characteristics indicate that it has the potential to cause a major ICT-related incident or a major operational or serious security incident related to payments;

2.2.12. **cyber-attack** means a malicious ICT-related incident triggered by an attempt to destroy, disclose, alter, deactivate, steal or gain unauthorised access to or use of an asset by any aggressor;

2.2.13. **threat analysis** means information that has been aggregated, transformed, analysed, interpreted or enriched in order to provide the necessary context for decision-making

and to enable an adequate and sufficient understanding to mitigate the effects of an ICT-related incident or cyber threat, including information on the technical details of the cyber-attack, the persons responsible for the attack and their modus operandi and motivations;

2.2.14. **vulnerability** means a weakness, vulnerability, or defect in an asset, system, process, or control that can be exploited;

2.2.15. **Threat Warfare Penetration Testing (TLPT)** means a framework that mimics the tactics, techniques and procedures used in real life by attackers identified as a real cyber threat, which provides controlled, tailor-made, threat intelligence-based (red team) testing of a financial entity's critical production systems in operation;

2.2.16. **ICT third-party risk** means the ICT-related risk that may arise for a financial entity in relation to its use of ICT services provided by ICT third-party service providers or their subcontractors, including through outsourcing arrangements;

2.2.17. **ICT third-party service provider** means an undertaking providing ICT services;

2.2.18. **intra-group ICT service provider** means an undertaking that is part of a financial group and that provides primarily ICT services to financial entities in the same group or to financial entities that are part of the same institutional protection scheme, including their parents, subsidiaries, branches or other entities jointly owned or controlled

2.2.19. **ICT services** means digital and data services provided on a continuous basis through ICT systems to one or more internal or external users, including hardware as a service and hardware services including the provision of technical support through software or firmware updates by the hardware provider, excluding traditional analogue telephony services;

2.2.20. **critical or material function** means a function the disruption of which would materially affect the financial performance of a financial entity, the security or continuity of its services and business, or the cessation or malfunction or failure of which would materially affect the financial entity's continued compliance with the conditions and obligations arising from its authorization or other obligations under applicable laws financial services;

2.2.21. **critical ICT third-party service provider** means an ICT third-party service provider appointed in accordance with Article 31 of DORA;

2.2.22. **ICT third-party service provider established in a third country** means an ICT third-party service provider that is a legal person established in a third country and that has entered into a contractual arrangement with a financial entity for the provision of ICT services;

2.2.23. **subsidiary means** an undertaking controlled by a parent undertaking, including any subsidiary of the ultimate parent undertaking (i.e. an undertaking that controls one or

more subsidiary undertakings), i.e. a subsidiary undertaking within the meaning of Article 2(10) and Article 22 of Directive 2013/34/EU of the European Parliament and of the Council on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC

2.2.24. **group** means an undertaking that controls one or more subsidiaries and all of its subsidiaries, i.e. a group as defined in Article 2(11) of Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013. on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC;

2.2.25. **parent undertaking** means an undertaking that controls one or more subsidiary undertakings, i.e. a parent undertaking within the meaning of Article 2(9) and Article 22 of Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013. on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC;

2.2.26. **ICT subcontractor established in a third country** means an ICT subcontractor that is a legal person established in a third country and which has entered into a contractual arrangement with an ICT third-party service provider or with an ICT third-party service provider established in a third country;

2.2.27. **ICT concentration risk** means exposure to individual or multiple interrelated critical ICT third-party service providers that leads to such a degree of dependency that the unavailability, failure or other deficiencies of the latter may potentially jeopardise the financial entity's ability to perform critical or significant functions or contribute to other adverse impacts on the financial entity; financial stability of the Union as a whole;

2.2.28. **management body** means the management body as defined in Article 4(1)(36) of Directive 2014/65/EU, Article 3(1)(7) of Directive 2013/36/EU, Article 2(1)(s) of Directive 2009/65/EC, Article 2(1)(45) of Regulation (EU) No 909/2014, Article 3(1)(20) of Regulation (EU) 2016/1011, and the relevant provision of the Markets in Crypto-assets Regulation or equivalent persons, that effectively manage the entity or perform key functions in accordance with the relevant Union or national legislation.

2.3. The following capitalized terms have the following meanings:

2.3.1. **CPD** – data processing center.

2.3.2. **Supervisory authority** – any public authority supervising the activities of the CONTRACTING AUTHORITY, in particular the European Banking Authority (EBA), the Polish Financial Supervision Authority (KNF), the President of the Personal Data

Protection Office (PUODO), the Inspector General for Financial Information (GIIF), as well as a "public authority" within the meaning of Article 3(65) of DORA.

2.3.3. **Subcontractor** – a third-party ICT service provider who is not an employee of NTT or a sole proprietorship with NTT on a regular basis, to whom NTT entrusts the performance of the Service in whole or in part.

2.3.4. **RTO (*recovery time objective*)** – the time from the moment of the failure of the IT system to the moment of restoring the functioning of the IT system.

2.3.5. **RPO (*recovery point objective*)** – the maximum time from the last data backup to the occurrence of a cloud service failure. This means that the ORDERING PARTY accepts the potential risk of losing the results of information processing generated in a specific period of time.

2.3.6. **Force Majeure** – an event occurring after signing the Agreement and, despite exercising due diligence, unforeseeable, beyond the control of the PARTY, preventing the PARTY from performing its obligations under the Agreement. Such events may include, in particular, wars, revolutions, fires, floods, epidemics, transport embargoes or announced general strikes in branches of the economy.

2.3.7. **TLPT** – penetration tests for threat hunting, within the meaning of Article 3(17) of DORA, means a framework that mimics the tactics, techniques and procedures used in reality by aggressors considered to be a real cyber threat, which provides controlled, tailored to specific threats, based on threat analysis (red team) tests of the critical production systems of a financial entity operating on an ongoing basis.

2.3.8. **NTT Group** – a capital group which includes NTT, NTT's parent companies and those to which NTT is the parent company, as well as companies related to NTT – within the meaning of Article 4 § 1 points 4 and 5 of the Act of 15 September 2000 on the Commercial Companies Code (i.e. Journal of Laws of 2024, item 18, as amended).

3. SUBCONTRACTING

3.1. NTT is entitled to entrust Subcontractors to perform, in part or in whole, only the Services specified in the Contract/Order.

3.2. If NTT intends to entrust the Subcontractor with the provision of the Service referred to in pt. 3.1 Annex NTT is required to:

3.2.1. inform the ORDERING PARTY about the Subcontractor who will commence the provision of a given Service, no later than 14 days before allowing this Subcontractor to perform the works covered by this Service – this obligation does not apply to the Subcontractors indicated directly in the Order;

3.2.2. provide, at the request of the EMPLOYER, the contract under which the Subcontractor will carry out the work covered by the Service or an appropriate extract from the contract, if NTT cooperates with the Subcontractor in a broader scope than that applicable to the

Service in question, provided that NTT is not obliged to disclose the remuneration due to the Subcontractor;

3.2.3. inform the EMPLOYER of the Subcontractor's discontinuation of the work covered by the Service within 14 days after the expiry of the contract between the Subcontractor and NTT or the actual, permanent cessation of the contract by the Subcontractor. If it is necessary to replace one Subcontractor with another, point 1 of the Subcontractor applies. 3.2.1 Annex.

3.3. If NTT informs the ORDERING PARTY of its intention to entrust the performance of a given Service to a Subcontractor, including the intention to replace one Subcontractor with another, the ORDERING Party is entitled to object within 7 days from the date of receipt of such notification. Failure to object within the time limit referred to in the preceding sentence shall be considered by the PARTIES as the EMPLOYER's acceptance of entrusting NTT with the performance of a given Service to a Subcontractor or replacing one Subcontractor with another.

3.4. In the event that NTT's use of a particular Subcontractor threatens or violates a material interest of the EMPLOYER, the ORDERING PARTY will request NTT to amend or terminate NTT's contract with that Subcontractor, and the PARTIES will enter into negotiations on the terms of termination of the specific Subcontractor.

3.5. In the event that the ORDERING PARTY objects in accordance with point 3.3 of the Appendix, the PARTIES shall enter into negotiations on entrusting the performance of a given Service to a Subcontractor.

3.6. NTT is entitled to grant a Subcontractor, accepted by the ORDERING PARTY in accordance with this chapter 3 Appendix, access to information processed in connection with the performance of the Agreement, to the extent necessary due to the scope of the Services in the provision of which the Subcontractor participates.

4. DATA LOCATION AND SECURITY

4.1. NTT undertakes to provide the Services, including the processing of data in connection with the provision of the Services, only at the locations indicated in the Contract/Order.

4.2. If it is necessary to change the location of the Service or to process and store data related to the Service, NTT is obliged to inform the ORDERING PARTY of the planned change in advance, but no later than 14 days before the change. The ORDERING PARTY is entitled to object to the change within 7 days of receipt of the notification and in such a case the Parties will jointly determine the location of further provision of the Service or processing and storage of data related to the Service. Failure to object by the ORDERING PARTY within the time limit referred to in the preceding sentence shall be deemed as the consent of the ORDERING PARTY to change the location of the provision of the Service or the processing and storage of data related to the Service.

4.3. NTT is committed to maintaining the availability, authenticity, integrity, and confidentiality of data processed in connection with the provision of the Services, including personal data. A detailed

description of NTT's mechanisms, procedures, rules, measures and policies to maintain data security is included in **Appendix 1 – Data Security**.

4.4. The Parties declare that the personal data, the processing of which will be entrusted to NTT by the ORDERING PARTY in connection with the performance of this Agreement, will be processed in accordance with the principles specified in detail in a separate agreement on entrusting the processing of personal data, in accordance with the law of the European Union, including the GDPR.

4.5. Each PARTY retains ownership of the information processed in the course of performance of the Agreement, including information generated by the PARTY, unless the PARTIES expressly agree otherwise, in writing under pain of nullity.

5. DETAILED RULES OF COOPERATION BETWEEN THE PARTIES

INCIDENT HANDLING AND SLA

5.1. The Contract/Order sets out the detailed rules for NTT's provision of support in handling ICT incidents related to the Services, including the guaranteed Service Levels (SLAs) and the rules for the exchange of information between NTT personnel (including Subcontractors) and the ORDERING PARTY in the event of an ICT incident.

5.2. The Agreement/Order specifies the RPO and RTO guaranteed by NTT with respect to the data processed in connection with the provision of the Services, if such guarantee is covered by the scope of the Services.

RIGHT TO AUDIT AND COOPERATION WITH SUPERVISORY AUTHORITIES

5.3. In the course of performance of the Agreement, the EMPLOYER is entitled to carry out – at its own expense – an audit of the proper performance of the Agreement, including an inspection of the processing location by NTT or its Subcontractor, information in connection with the provision of the Services, whereby:

5.3.1. The ORDERING PARTY is obliged to inform NTT about the planned inspection within 14 days before its planned date, together with the data of the persons to carry out the inspection;

5.3.2. The CONTRACTING AUTHORITY shall ensure that the persons conducting the inspection on behalf of the CONTRACTING AUTHORITY will comply with all rules applicable at NTT in relation to access to the specified premises in which the inspection will be carried out and, if required by NTT, undertake to maintain the confidentiality of the information obtained in connection with the admission of such person to conduct the inspection. In the event of failure to comply with the assurances referred to in this sub-clause, NTT shall be entitled to remove the person concerned from the inspection;

5.3.3. The CONTRACTING AUTHORITY undertakes to take all reasonable steps to minimize the impact of the inspection on NTT's operations and to cooperate with NTT in good faith in this regard.

5.4. In the course of the performance of the Agreement, NTT undertakes to provide the Supervisory Authorities with all information requested by them regarding the Services provided, as well as, at the request of the Supervisory Authority, to enable the Supervisory Authority to inspect the premises where the Services are provided and to provide the Supervisory Authority with documentation related to the processing of the ORDERING PARTY's information, processes and procedures, organization and management, and compliance confirmations.

5.5. The right of audit or control performed by the ORDERING PARTY or the relevant Supervisory Authority includes the right to access the full range of relevant equipment, systems, networks, information and data used to provide NTT's Services, including related financial, personnel and external auditor information.

5.6. In the event that the exercise of the audit right by the EMPLOYER or the Supervisory Authority has a negative impact on the provision of the Services by NTT, NTT shall inform the EMPLOYER of the impact of the audit on the Services provided and shall be exempt from liability to the EMPLOYER in this respect in the event of non-performance or improper performance of the Agreement.

5.7. In the event that the exercise of the right to audit by the EMPLOYER or the Supervisory Authority requires significant involvement on the part of NTT, NTT will inform the EMPLOYER of the estimated costs of such involvement, and the EMPLOYER – in the event of an audit – is obliged to reimburse NTT for the costs incurred, in accordance with the information provided and documented, within 7 days.

ICT SECURITY TRAINING

5.8. At the request of the ORDERING PARTY, submitted no later than 14 days before the scheduled date of the training, NTT is obliged to delegate the relevant NTT personnel or Subcontractors – participating in the provision of the Services – to participate in a training course on digital operational resilience organized by the ORDERING AUTHORITY or an entity designated by the ORDERING PARTY, or in any other event aimed at raising awareness of ICT security.

5.9. Participation in the training or event in question by delegated NTT staff members or the Subcontractor shall be at the expense of the EMPLOYER, on terms and conditions specifically agreed by the PARTIES prior to the commencement of the training or event.

REPORTING AND MONITORING OF SERVICE DELIVERY PERFORMANCE

5.10. NTT is obliged to provide the ORDERING PARTY with reports on the provision of Services specified in the Agreement, within the deadlines specified in the Agreement.

5.11. Regardless of the reports received, the ORDERING PARTY is entitled to monitor on its own the results of the provision of Services by NTT, in particular their compliance with the Agreement. If necessary, NTT shall cooperate with the ORDERING PARTY in order to enable effective monitoring of the level of Services provided, on terms and conditions specifically agreed between the PARTIES.

INSURANCE

5.12. NTT declares that it has insurance for its business activity up to the sum insured not lower than PLN 5,000,000.00 and undertakes to maintain the insurance at a not lower level throughout the entire period of provision of the Services.

STANDARDS OF PROVIDED SERVICES

5.13. In the event of changes in the standards of the Services provided:

5.13.1. if the change concerns a Service provided directly by NTT – NTT is obliged to inform the ORDERING PARTY about the planned change at least 14 days before its implementation;

5.13.2. if the change concerns a Service provided by a Subcontractor – NTT is obliged to inform the ORDERING PARTY about the change within 14 days of receiving such information from the Subcontractor,

– NTT shall inform the ORDERING PARTY in a documentary form, with a clear indication that the information relates to a change in the standards of the Services provided.

TESTING AND CONTINGENCY PLANS (BUSINESS CONTINUITY)

5.14. NTT is required to have in place and test – at least every 12 months – a contingency plan for the Services provided. If the ORDERING PARTY has detailed requirements for contingency plans, it will provide them to NTT, and the PARTIES will jointly agree on the date and conditions of their implementation. By contingency plan, the PARTIES also mean a business continuity plan.

5.15. At the request of the ORDERING PARTY, notified at least 14 days in advance, NTT is obliged to participate in the TLPT and provide the ORDERING PARTY with support in this regard on terms and conditions specifically agreed by the PARTIES.

DOCUMENTATION

5.16. The Agreement/Order specifies the place where the technical documentation is stored and updated – together with configuration instructions, if applicable – regarding the Services provided along with the rules of access of the PARTIES to this documentation.

5.17. The Agreement/Order precisely defines the scope of documentation and all information that NTT is obliged to make available to the ORDERING PARTY in connection with the provision of the Services.

INTELLECTUAL PROPERTY

5.18. The Agreement/Order specifies in detail the scope of the ORDERING PARTY's rights to use the works made available to it by NTT in connection with the provision of the Services, as well as the rules for performing security updates of the software used in the provision of the Services.

6. LIABILITY, LIQUIDATED DAMAGES AND FORCE MAJEURE

RESPONSIBILITY

6.1. NTT's liability to the CLIENT, including the CLIENT's customers, in connection with the performance of the Agreement is limited to the limit specified in the Agreement/Order, as the limit of NTT's liability.

6.2. The PARTIES exclude NTT's liability under the warranty for physical and legal defects of the results of work delivered to the ORDERING PARTY in the course of performance of the Agreement.

CONTRACTUAL PENALTIES

6.3. In the event of non-performance or improper performance of the Agreement by one of the PARTIES, the other PARTY shall be entitled to charge the PARTY in breach of the Agreement with a contractual penalty – in the cases and in the amount specified in detail in the Agreement. The contractual penalty shall be payable upon the first demand, within 14 days from the date of delivery of the written request to the PARTY obliged to pay by the other PARTY.

FORCE MAJEURE

6.4. Neither PARTY shall be liable for the non-performance or improper performance of its obligations under the Agreement if the non-performance or improper performance of such obligations is the result of Force Majeure.

6.5. If the inability of one PARTY to perform its obligations as a result of Force Majeure materially affects the other PARTY's ability to perform its obligations under the Agreement, that PARTY shall also not be liable for the failure to perform its obligations. The PARTY that has notified the Force Majeure event shall not be liable to the other PARTY for any loss or damage suffered by the other PARTY from the date of the Force Majeure event, provided that the notification is made in writing, no later than 14 days after the Force Majeure circumstance ceases, otherwise the rights under this provision will be forfeited.

6.6. Notwithstanding the obligation under pt. 6.5 of the Appendix, the PARTY affected by the Force Majeure shall notify the other PARTY of the occurrence of the Force Majeure immediately after its occurrence, as soon as it is possible, and together with such notification, provide the following information (if known or ascertainable to the PARTY):

6.6.1. information on what the Force Majeure event is;

6.6.2. information about the start time and estimated duration of the Force Majeure;

6.7. If the performance of part or all of any obligation under the Agreement is delayed due to Force Majeure for a period exceeding 60 days from the time limits under the Agreement, the Parties shall meet and consider in good faith the advisability and conditions of termination of the Agreement.

7. TERMINATION OF THE CONTRACT AND EXIT PLAN

7.1. Each PARTY is entitled to terminate the Agreement/Order if the Agreement provides for such a right and with the notice period indicated therein.

7.2. Notwithstanding other provisions of the Contract/Order, the ORDERING PARTY is entitled to terminate the Agreement:

7.2.1. with a 3-month notice period – in the event that the Supervisory Authority issues a decision ordering the ORDERING PARTY to terminate the Contract. In such a case, the termination shall be effective upon delivery of the notice of termination to NTT, together with a copy of the Supervisory Authority's termination decision;

7.2.2. with 1 month's notice period – if the EMPLOYER has applied to NTT for termination or amendment of the contract with a specific Subcontractor due to a violation or threat to the material interest of the EMPLOYER (in accordance with point 1). 3.3 of the Appendix) and the PARTIES have not reached an agreement within 30 days to amend such an agreement with the Subcontractor or terminate it;

7.2.3. with 1 month's notice period – in case NTT has entrusted the provision of Services to a Subcontractor who has not obtained the approval of the EMPLOYER in accordance with chapter 3 Annex;

7.2.4. with 1 month's notice period – in the event that NTT in connection with the provision of Services violates the laws or regulations applicable to the ORDERING PARTY, and the ORDERING PARTY has called on NTT to cease the violations, setting an appropriate deadline for this purpose, which has expired ineffectively;

7.2.5. with 1 month's notice – if NTT breaches the Agreement in a way that poses a threat to the EMPLOYER's information security and fails to cease the breach within the appropriate period of time set by the EMPLOYER;

7.3. Notwithstanding any other provision of the Agreement, NTT shall be entitled to terminate the Agreement:

7.3.1. with a 1-month notice period – in the event of failure to reach an agreement by the PARTIES on the admission of a specific Subcontractor to provide Services, in accordance with point 1 of the Contractor Act. 3.4 Annex;

7.3.2. with 1 month's notice – in the event of failure to reach an agreement by the PARTIES as to the location of the provision of Services or the processing or storage of data related to the Service, in accordance with point 1 of the Tax Code. 4.2 Annex;

TRANSITION PERIOD

7.4. Upon termination of the Agreement by either PARTY, as well as the declaration of bankruptcy or liquidation of NTT, a transition period ("**Transition Period**") begins. The transition period lasts for the duration of the notice period, and if the Agreement has been terminated immediately – for a period of 1 month.

7.5. During the Transition Period, NTT shall provide the Services in full and in accordance with the Agreement, unless otherwise agreed in writing by the PARTIES, otherwise they shall be null and void.

7.6. During the Transition Period, NTT is required to:

7.6.1. to enable the ORDERING PARTY, upon its request, access to the data – including personal data – entrusted to NTT by the ORDERING PARTY in connection with the provision of the Services, and

7.6.2. to provide the ORDERING PARTY, at its request, with the data – including personal data – entrusted to NTT by the ORDERING PARTY in connection with the provision of the Services, in an easily accessible format and in the form agreed by the PARTIES,

– no later than within 1 month from the submission of such a request by the ORDERING PARTY.

7.7. Upon issuance of the data, NTT shall be entitled to reimbursement of the costs of the work carried out for the issuance of the data in accordance with this provision, including the reimbursement of the costs of the media on which the data were issued to the ORDERING PARTY.

7.8. During the Transition Period, the following detailed rules of cooperation apply:

7.8.1. NTT shall assist the ORDERING Party in enabling the ORDERING Party or a third party to take over the provision of the Services, in exchange for remuneration specified in a separate agreement.

7.9. During the Transition Period, NTT shall, at the request of the EMPLOYER expressed in writing under pain of nullity, permanently delete all information entrusted to NTT by the EMPLOYER in connection with the provision of the Services, which is in NTT's possession and obliges the Subcontractors to delete it. The removal of information will be carried out no later than within 14

days from the date of such a request by the ORDERING PARTY and will be confirmed by an appropriate protocol issued to the ORDERING PARTY by NTT.

7.10. Notwithstanding anything to the contrary in the Agreement or the Annex, NTT is entitled to retain a single copy of the ORDERING PARTY's data processed or stored in connection with the conclusion and performance of the Agreement for the assertion of NTT's claims or for the defence against any claims asserted against NTT, provided that NTT is not entitled to use such data for any purpose other than to protect NTT's rights.

8. FINAL PROVISIONS

8.1. The contract is concluded under Polish law.

8.2. Any disputes arising out of or in connection with this agreement shall be finally resolved on the basis of the Arbitration Rules of the Court of Arbitration at the Polish Chamber of Commerce in Warsaw, in force on the date of commencement of the proceedings, by an arbitrator or arbitrators appointed in accordance with these Rules.

8.3. The Agreement sets out a detailed procedure for the PARTIES to amend the Agreement, including changes in the parameters of the Services provided by NTT.