

Outsourcing Supplement to Purchase

1. SUBJECT MATTER OF THE OUTSOURCING SUPPLEMENT

- 1.1. NTT Poland sp. z o.o. („**NTT**” or simply we) provides ICT services to its Clients who are financial entities according to Article 2 of DORA. DORA and applicable national regulations impose obligations and promotes good practices for both financial entities and ICT service providers.
- 1.2. Because our vendors (“**Vendor**” or simply you) act as our subcontractors, certain regulatory obligations and best practices are binding upon our contractual relationships. These obligations and best practices are reflected in this document, implementing outsourcing regulations to our contract (“**Outsourcing Supplement**”).
- 1.3. The Outsourcing Supplement outlines your obligations arising from DORA and applicable national regulations, in connection with the Applicable Order.
- 1.4. This Outsourcing Supplement and its binding terms are attached to an Applicable Order concluded in writing or in equivalent form.
- 1.5. In the event of any discrepancies between the Applicable Order, the Agreement and the Outsourcing Supplement, the following order of precedence shall apply:
 - 1.5.1. Applicable Order;
 - 1.5.2. Outsourcing Supplement;
 - 1.5.3. Agreement.

2. DEFINITIONS

- 2.1. The terms below have the following meaning:
 - 2.1.1. **Agreement:** the Vendor Agreement which regulated relationships established between NTT and our vendors through the signing of the Applicable Order
 - 2.1.2. **Authority:** any public authority supervising the activities of NTT, including the Financial Supervision Authority (KNF), the National Bank of Poland (NBP), the General Inspector for Personal Data Protection (GIODO), the General Inspector of Financial Information (GIIF), and the European Supervisory Authorities (EUN) as defined in point 7 of DORA.
 - 2.1.3. **DORA:** 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.
 - 2.1.4. **FSC Communication:** communication of the Office of the Financial Supervision Commission regarding the processing of supervised entities’ information in public or hybrid cloud computing dated January 23, 2020.

- 2.1.5. **ICT:** information and communication technology.
- 2.1.6. **RTO:** Recovery Time Objective, the time from a failure of an IT system until its recovery.
- 2.1.7. **RPO:** Recovery Point Objective, maximum length of time from the last data backup until a failure of the cloud service. This also means a potential risk (accepted by the supervised entity) that the results of information processing might be lost for a specified duration of time

2.2. Other terms written with capital letters have the same meaning as in the Agreement.

3. APPLICABLE REGULATIONS

3.1. Each party to the Applicable Order will comply with the laws and relevant guidelines and recommendations issued by the Authorities, to the extent that they apply to the Applicable Order, in particular with:

3.1.1. DORA

3.1.2. guidelines of the European Banking Authority on outsourcing dated February 25, 2019 (EBA/GL/2019/02);

3.1.3. communication of the Office of the Financial Supervision Commission regarding the processing of supervised entities' information in public or hybrid cloud computing dated January 23, 2020.

3.2. If new laws come into effect or new guidelines or recommendations of the Authorities are issued during the term of the Applicable Order, we will comply with them. If this requires a change to the Applicable Order or the way it is executed, we will immediately enter into good-faith negotiations to implement the appropriate changes.

4. LOCATION

4.1. Contracted or subcontracted functions and ICT services, as well as data processing and storage locations are specified in the Applicable Order. If the location is not specified in the Applicable Order, the contracted or subcontracted services and data storage should occur within the EEA area.

4.2. If you intend to change location of performing ICT services, data processing or its storage, you must provide us with advance notice. The notice must be provided in written form with a minimum of one month's notice period.

4.3. We reserve the right to object to the change in the location within 2 weeks of receiving your notice. In such a situation, we will initiate bilateral negotiations. If we fail to reach an agreement, NTT is entitled to terminate the Applicable Order within an immediate effect.

5. CONTROL AND AUDIT RIGHTS

- 5.1. NTT, Clients and Authority are entitled to audit and inspect you during the term of the Applicable Order.
- 5.2. The frequency of audits and inspections as well as the areas to be audited has been specified in the Applicable Order.
- 5.3. If the frequency of audits is not specified in the Applicable Order the audit or inspection can be conducted by NTT or Client once per every quarter. However, in the event of reasonable suspicion of non-performance or improper performance of the Applicable Order an audit or inspection may be conducted at any time.
- 5.4. If the scope of the audit is not specified in the Applicable Order, NTT and Client are entitled to audit and inspect every area of the services provided by you under the Applicable Order.
- 5.5. During an audit or inspection, Authorities are entitled to check the premises and the documentation pertaining to the processing of information, the processes and procedures, the organisation, management, and certificates of compliance – in connection with the Applicable Order.
- 5.6. In the event of an audit or inspection, you will provide full cooperation to NTT or Client and individuals delegated by them, as well as to the Authority and individuals delegated by the Authority. You are obligated to adhere to post-audit or post-inspection instructions and guidelines.
- 5.7. You are obliged to promptly inform us of any changes that may impact the proper execution of your obligations covered by the Applicable Order.
- 5.8. In the event that you conduct an internal audit or a third-party audit, you are obligated to promptly inform us about:
 - 5.8.1. the occurrence of such audit or inspection - no later than 7 days from the commencement of the audit or inspection, and
 - 5.8.2. the results of the audit or inspection - no later than 7 days from the completion of the audit or inspection.
- 5.9. You are obligated to fully cooperate with the competent Authorities as well as with the persons appointed by Client or NTT.

6. BUSSINES CONTINGENCY

- 6.1. Upon entering into the Applicable Order, NTT will provide you with the business contingency plan established between NTT and Client. In case of an update to the plan, we will promptly provide it to you.
- 6.2. You are obligated to implement and test business contingency plan of yours, that is compatible with NTT's and Client's plans and have in place ICT security measures, tools and

policies that provide an appropriate level of security of the provision of services by Client in line with its regulatory framework.

- 6.3. Your business contingency plan will cover full scope of services provided under the Applicable Order.
- 6.4. You are obligated to participate, upon request, in NTT's or Client's business contingency plan tests.
- 6.5. You declare that you have a good financial standing, enabling the uninterrupted conduct of the activities covered by the Applicable Order.
- 6.6. You will provide a copy of your business contingency plan upon request, without undue delay. You will inform NTT of the result of business contingency plan tests immediately after they were conducted.

7. IT SECURITY

- 7.1. You are obligated to comply with appropriate, most up-to-date, and highest quality information security standards.
- 7.2. You will execute the Applicable Order with due regard to ensuring the availability, authenticity, integrity, and confidentiality in relation to the protection of NTT's and Clients' data.
- 7.3. Throughout the duration of the Applicable Order, you are required to maintain up-to-date and suitable action plans, detailing strategies for recovering data stored or processed under the terms of the Applicable Order to mitigate the risk of data loss resulting from unforeseen circumstances. You are expected to promptly provide the updated plans when requested.
- 7.4. In the event of an ICT incident related to the ICT service provided by you to NTT you are obligated to provide assistance to NTT and NTT's Client without additional cost.
- 7.5. You ensure that the personnel delegated to execute the Applicable Order will participate in ICT security awareness programs and digital operational resilience training organized by NTT or Client. NTT will inform you about the training in advance and facilitate participation of delegated personnel.

8. USE OF SUBCONTRACTORS

- 8.1. In the application for NNT consent to use a subcontractor, you are obligated to:
 - 8.1.1. identify the subcontractor in a way that allows NTT to carry out verification procedures;
 - 8.1.2. submit to NTT copy of the confidentiality agreement concluded with the subcontractor;
 - 8.1.3. clearly outline the scope of services to be executed by the subcontractor, specifying the services in which the subcontractor will be involved and detailing the activities that the subcontractor it to carry out;

- 8.1.4. submit to NTT the draft contract with the subcontractor, if it exists.
- 8.2. NTT may request additional information in any time, and you shall provide requested information without undue delay.
- 8.3. You will notify us about any change or termination in your contract with the subcontractor, as well as any case of the subcontractor ceasing to provide services. Notice shall be provided immediately, but no later than within 1 day from the event's occurrence.

9. SERVICE LEVEL

- 9.1. Service level descriptions, including updates and revisions are described in the Applicable Order.

10. FUNCTIONS AND ICT SERVICES

- 10.1. The complete and clear description of all functions and ICT services that you are providing is included in the Applicable Order.

11. LIABILITY

- 11.1. You are fully liable for any damages incurred by Client's customers in connection with your execution of the Applicable Order. Any limitation of your liability does not apply in such cases.

12. VALIDITY, TERMINATION AND EXIT PLAN

- 12.1. This Outsourcing Supplement goes into effect upon it being delivered to you as an attachment to the Applicable Order with the Applicable Order's date becoming the effective date of the Outsourcing Supplement.
- 12.2. We have the right to terminate the Applicable Order at any time without the further notice in any of the following circumstances:
 - 12.2.1. significant breach of applicable laws, regulations or contractual terms of the Applicable Order, Agreement or this Outsourcing Supplement;
 - 12.2.2. circumstances identified throughout the monitoring of ICT risk that are deemed capable of altering the performance of the functions provided through the Applicable Order, including material changes that affect the Applicable Order or you;
 - 12.2.3. weaknesses pertaining to your overall ICT risk management and in particular in the way you ensure the availability, authenticity, integrity and confidentiality of data, whether personal or otherwise sensitive data, or non-personal data;
 - 12.2.4. where the competent Authority can no longer effectively supervise Client because of the conditions of, or circumstances related to the Applicable Order;
 - 12.2.5. termination of the agreement (concerning the Applicable Order) between NTT and Client by the Authority, NTT or Client.

- 12.3. The exit strategies, including the mandatory adequate transition period has been specified in the Applicable Order.
- 12.4. During the mandatory transition period you will continue providing the respective functions or ICT services with a view to reducing the risk of disruption services provided to and by NTT and Client or to ensure its effective resolution and restructuring.
- 12.5. During the mandatory transition period, upon request you are obligated to make available NTT data to us, in format customarily used by the Parties or in easily accessible form, and enable us the migration to another service provider or the change to in-house solutions consistent with the complexity of the service provided. On NTT's request you will delete our data.

13. ICT SERVICES SUPPORTING CRITICAL OR IMPORTANT FUNCTIONS

- 13.1. The following provisions apply to you if the Applicable Order specifies that your ICT services support Client's critical or important functions. If following provisions are applicable and there are any discrepancies between this Section 13 and other terms of this Outsourcing Supplement, the following provisions will apply.
- 13.2. Service level descriptions, including updated and revisions with precise quantitative and qualitative performance targets within the agreed service levels are included in the Applicable Order.
- 13.3. You are obligated to promptly notify NTT about any development that might have a material impact on your ability to effectively provide the ICT services supporting critical or important functions of Client in line with agreed services levels. Specific notice periods can be described in the Applicable Order.
- 13.4. You are obligated to participate and fully cooperate in the NTT's Client threat-led penetration testing as referred to in Article 26 and 27 of DORA.
- 13.5. NTT and Client have the right to monitor, on an ongoing basis, your performance, which entails the following:
 - 13.5.1. unrestricted rights of access, inspection and audit by NTT and Client, or an appointed third party, and by the competent authority, and the right to take copies of relevant documentation on-site if they are critical to the operations of your service, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies;
 - 13.5.2. the right to agree on alternative assurance levels if the Client's customers' rights are affected;
 - 13.5.3. your obligation to fully cooperate during the onsite inspections and audits performed by the competent Authorities, Client or an appointed third party; and
 - 13.5.4. your obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits.

- 13.6. You are obliged to have in place ICT security measures, tools and policies that provide an appropriate level of security for the provision of services.

14. CLOUD SERVICES

- 14.1. The following provisions apply to you if the Applicable Order specifies that the FSC Communication applies to the services you provide.
- 14.2. The clear distribution of responsibility for information security, considering the service model, the service continuity (including the RTO and RPO parameters, where appropriate) and declared SLA together with the measurement and reporting method applies when specified in the Applicable Order.
- 14.3. During the term of the Applicable Order and after its termination (expiration, dissolution), the ownership of information remains with NTT or Client accordingly.
- 14.4. The Applicable Order specifies Vendor's obligations regarding provision of the information on the expected changes in the standards applicable to the relevant cloud services (including technical changes).
- 14.5. The Applicable Order specifies Vendor's obligations regarding delivery of technical documentation, cloud service configuration manuals and declarations of conformity.
- 14.6. Independently of NTT's and the Client's rights to conduct audits and inspections (specified in Section 5 of this Outsourcing Supplement), NTT and Client have the right to conduct inspections at locations where data are processed in connection with the Applicable Order, including the right to conduct an audit of the other party or third party at the request of Client or NTT.
- 14.7. If applicable, the licensing rules (including the right to update the security of software or its components) and intellectual property rights, including the right to handle information which is being processed are specified in the Applicable Order.
- 14.8. The technical parameters of the services performed under the Applicable Order can be modified only in cases and according to the procedure specified in the Applicable Order.
- 14.9. The rules and time limits for deleting information which is being processed are specified in the Applicable Order. If the rules and time limits are not specified, the information will be deleted under rules and within the time limits indicated by NTT.
- 14.10. The Applicable Order specifies the standards and norms that the Vendor adheres to, such as PN-ISO/IEC ISO 20000, PN-EN ISO/IEC 27001, PN-EN ISO 22301, ISO/IEC 27017, ISO/IEC 27018 or other.
- 14.11. You will implement rules protecting against unauthorized access to information by your staff and subcontractors, including:
 - 14.11.1. default rule of no access to information processed by NTT or Client,

- 14.11.2. default rule of no administrator or user account on virtual machines dedicated to NTT or Client or in any cloud services that are being launched,
 - 14.11.3. the rule of the 'necessary minimum' requirements for service account rights, is to be granted only where it is necessary to perform operations required by NTT or Client (e.g. troubleshooting) and only for the duration of such operations, based on a service request made by NTT or Client; the whole management and execution process may be carried out after log-in; The applicable operation procedures may also be confirmed by a relevant certificate (e.g. SOC7 2 Type 2) issued by an independent certification body accredited in line with the European accreditation standards.
- 14.12. You will also protect the information against unauthorized access through adhering to available guidelines, model configuration, descriptions of rules, etc., which should clearly define separation in information processing and indicate methods of verifying the correctness of configuration and through launching a new default environment (or cloud service) separated from other tenants, with 'secure-by-default' settings.
- 14.13. The information processed in the cloud must be encrypted in accordance with the below rules:
- 14.13.1. you should provide NTT access to up-to-date detailed cloud configuration manuals and methods of verification of the correctness of configuration and operation, in particular in the area of encryption;
 - 14.13.2. your personnel should have adequate competences to set up proper configuration of cloud services in line with the guidelines submitted by the cloud service provider, including in terms of encryption;
 - 14.13.3. you should use dedicated configuration settings – or settings recommended by the cloud service provider – that increase the safety of the cloud services concerned;
 - 14.13.4. the information protected by law must be encrypted both as data 'at rest' and data 'in transit.'
- 14.14. You will provide the following information to NTT:
- 14.14.1. up-to-date detailed cloud configuration manuals and methods of verification of the correctness of configuration and operation, in particular in the area of encryption;
 - 14.14.2. guidelines for the proper configuration of cloud services;
 - 14.14.3. recommendations regarding configuration settings that increase the safety of the cloud services.
- 14.15. You will protect the logs against unauthorised access, modification or deletion for a period of time specified in the security rules following from the risk assessment and the applicable special rules.
- 14.16. If you have remote access to the cloud services used by NTT or Client, you ensure that:

- 14.16.1. only authorised staff has access to specific IT systems and/or specific parts of the IT structure;
- 14.16.2. your staff use multi-factor authentication (MFA), with the type and scope being determined by the results of the risk assessment;
- 14.16.3. the administrative and privileged user access is restricted to trusted networks of NTT or Client and/or you and controlled (including by recording sessions and session parameters, and then by analysing the correctness and purpose of each operation), unless the risk assessment has shown that this is not necessary.