Commissioned Data Processing Agreement for City Cloud Services

1. Scope and Order of Precedence

The Customer agreeing to these terms ("Customer") concerning the Processing of Personal Data as part of City Network Hosting AB's (org. no. 556630-7806, "City Network") cloud services "City Cloud" (the "Services"), as further specified in (i) the applicable master agreement, (ii) the order between Customer and City Network, (iii) the General Terms and Conditions, and (iv) all documents, appendices, and amendments incorporated therein (collectively the "Agreement") by and between the Customer entity and City Network subsidiary listed in your order for Services.

This agreement (the "Data Processing Agreement") is subject to the terms of the Agreement and is annexed as an appendix to the Agreement. In the event of any conflict between the terms of the Agreement and the terms of this Data Processing Agreement, the relevant terms of this Data Processing Agreement shall prevail.

The parties acknowledge and agree that City Network is a processor of Personal Data under the European data protection legislation; Customer is a controller or processor, as applicable, of the Customer's Personal Data under the European data protection legislation; and each party will comply with the obligations applicable to it under the European data protection legislation with respect to the processing of the Customer's Personal Data.

This Data Processing Agreement is valid and in effect from signing of the Agreement ("Effective Date") and shall replace any previously applicable data processing agreement, or any terms applicable to privacy, data processing and/or data security, for the services period of any Supplier cloud order placed under the Agreement.

This Data Processing Agreement is only applicable to City Cloud Data Centers within the European Union subject to European data protection legislation. For City Cloud Data Centers outside the European Union, or if the Customer requests to store or transfer Personal Data out of the EU and the EEA and the European data protection legislation applies to such transfers, a separate agreement mirroring the EU Model Contract Clauses is required.

2. Definitions

This Data Processing Agreement has the following definitions:

Terms	Explanation
Affiliates	Any subsidiaries of City Network that may assist in the performance of the Services.
Agreement	Consisting of (i) the applicable master agreement, (ii) the order between Customer and City Network, (iii) the General Terms and Conditions, and (iv) all documents, appendices, and amendments incorporated therein.
Processing	Any operation which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Personal Data	Any information relating to an identified or identifiable natural person (i.e. Data Subject).
Controller	The natural or legal person, which alone or jointly with other, determines the purpose and means of the processing of Personal Data.
Processor	A natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.
Data Incident	means a breach of City Network's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by City Network. "Data

	Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
Data Subject	An identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identify or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person.
Data Protection Authority	An independent public authority which the is established by a Member State. In Sweden the appointed authority is the Swedish Data Protection Authority (Sw. Datainspektionen).
Technical and organisational security measures	Measures to protect personal data against unintentional or unlawful extinction, accidental sealed, changes, unauthorized disclosure or access, in particular when processing involves transmission of data over a network and against all other unlawful form of processing.
Sub Data Processor	A natural or legal person, public authority, agency or body other than the Data Subject, Controller, Processor and person who, under the direct authority of the Controller or Processor, are authorised to process Personal Data.

3. Duration of Data Processing Agreement

This Data Processing Agreement will take effect on the Effective Date and, notwithstanding expiry of the Term, remain in effect until, and automatically expire upon, deletion of all Personal Data by City Network as described in this Data Processing Agreement.

4. Categories of Personal Data

In order to execute the Agreement, and in particular to perform the Services on behalf of Customer, the Customer authorizes and requests that City Network Process, for example but not limited to, the following Personal Data: user IDs, personal contact information such as name, home address, home telephone or mobile number, email address, and passwords; social security details and business contact details; financial details; documents; presentations; images; calendar entries; tasks; and goods and services provided.

5. Categories of Data Subjects:

Data subjects include Customer's representatives and end users, such as employees, contractors, collaborators, partners, and customers of the Customer. Data subjects also may include individuals attempting to communicate or transfer Personal Data to users of the Services.

Customer is responsible as the Controller for that all Personal Data stored in the Service not containing any illegal obtain information or information used to preform illegal activity. The Customer also agree to hold City Network harmless in any case such illegal information is processed.

6. Nature and Purpose of the Processing

City Network will process Customer's Personal Data submitted, stored, sent or received by Customer, its affiliates or end users via the Services for the purposes of providing the Services and related technical support to Customer in accordance with this Data Processing Amendment

By entering into this Data Protection Agreement, Customer instructs City Network to Process Personal Data only with applicable law: (a) to provide the Services and related technical support; (b) as further instructed via the Customer's use of the Services (including the admin console and other functionality of the Services) and related technical support; (c) as documented in any other written form of the applicable Agreement, including this Data Processing Agreement; (and (d) as further documented in any other written instructions given by Customer and acknowledged by City Network as constituting instructions for processing for purposes of this Data Protection Agreement.

City Network shall not otherwise disclose such Personal Data to third parties other than City Network's affiliates or its Sub Data Processors for the aforementioned purposes or as required by law.

7. Customer's Instructions

During the term of the Agreement of any order for Services, Customer may provide instructions to City Network in addition to those specified in the Data Processing Agreement with regard to processing of Personal Data. City Network will comply with all such instructions to the extent necessary for City Network to comply with laws applicable to City Network as a Processor in the performance of the Services.

City Network is entitled to compensation from the Customer to comply with the Customer's written instructions if the requested action is not otherwise apparent from the Data Processing Agreement. If the costs of complying with the Customer's additional instruction are beyond reasonable and disproportionate in relation to the service fee for the Service, City Network shall be entitled to terminate the Agreement (including this Data Processing Agreement) with 30 days' notice.

City Network will inform Customer if, in City Network's opinion, an instruction breaches data protection regulations. Customer understands that City Network is not obligated to perform legal research and/or to provide legal advice to Customer.

8. Confidentiality

The Processor agrees to not disclose or transfer any information regarding the processing of the Personal Data or any other information received under this Agreement to any third party. These obligations do not apply for; (i) information which a party can show was known for the public at the time of receipt, or (ii) information that a party issued to submit to the authority.

The Parties shall disclose Confidential information only to employees or subcontract personnel who need to know the Confidential information for their work in connection with the approved purpose or employees in the legal unit that is part of the same group as the Recipient, and who need to know the Confidential information for their work in connection with the performance of the Agreement. The confidentiality obligation shall survive the Agreement.

9. The Controller's Security Responsibilities and Assessment

The control of Personal Data remains with Customer, and as between Customer and City Network, Customer will at all times remain the Controller for the purposes of the Services, the Agreement, and this Data Processing Agreement.

Customer is responsible for compliance with its obligations as Controller under data protection laws, in particular for justification of any transmission of Personal Data to City Network (including providing any required notices and obtaining any required consents from Data Subjects), and for its decisions concerning the Processing and use of the Personal Data.

Customer is solely responsible for its use of the Services, including: (a) making appropriate use of the Services and the additional security controls to ensure a level of security appropriate to the risk in respect of the Customer's Personal Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Services; and (c) backing up its Customer Data.

City Network has no obligation to protect Customer's Personal Data that Customer elects to store or transfer outside of City Network's and its Subprocessors' systems (for example, offline or on premise storage), or to protect Customer's Personal Data by implementing or maintaining additional security controls except to the extent Customer has opted to use them.

The Controller shall without delay inform the Processor about changes in the Processing which will affect the Processor's obligations. Controller shall also inform the Processor about third parties, such as Data Protection Authority and Data Subjects means in regard to the Processing.

Customer's Security Assessment: (a) Customer is solely responsible for reviewing the security documentation and evaluating for itself whether the Services, City Network's applicable security measures, and City Network's commitments under this Section 13 (Technical and Organizational Measures) will meet Customer's needs, including with respect to any security obligations of Customer under the European data protection legislation and/or non-European data protection legislation, as applicable; (b) Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer's Personal Data as well as the risks to individuals) the security measures implemented and maintained by City Network as set out in Section 13 (Technical and Organizational Measures) provide a level of security appropriate to the risk in respect of the Customer's Personal Data.

10. Rights of Data Subjects

During the applicable Term, City Network will grant Customer electronic access to Customer's Services environment that holds Personal Data to permit Customer to rectify, delete, release, correct or block access to specific Personal Data or, if that is not practicable and to the extent permitted by applicable law, follow Customer's detailed written instructions to rectify, delete, release, correct or block access to Personal Data. Customer agrees to pay City Network's reasonable fees associated with the performance of any such deletion, release, correction or blocking of access to data.

Customer's Responsibility for Data Subject Requests. During the applicable Term, if City Network receives any request from a Data Subject in relation to Customer's Personal Data, City Network shall advise the data subject to submit her/his request to Customer, and Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

11. Data Processing within the EU/EEA

With respect to Processing of Personal Data originating from the European Union (EU) and the European Economic Area (EEA), City Network Hosting AB will at all times maintain established Customer's Personal Data during the performance of the Services in its data centres located within the EU/EEA.

12. Sub Data Processors

Some or all of City Network's obligations under the Agreement may be performed by City Network Affiliates. In such an event, City Network and City Network's Affiliates have subscribed to the intra-company agreement, under which a City Network subsidiary handling Personal Data adopts safeguards consistent with those of the City Network subsidiary contracting with a customer for City Network's Services. City Network Affiliate contracting with the Customer is responsible for City Network's compliance and the City Network Affiliates compliance with this requirement. If the Processor, with the Controller's authorization, transfer its obligation, according to this Agreement, in whole or partly to a subcontractor, shall a written agreement the concluded between the Processor and such Sub Data Processors, imposing the same Processors obligations under this Data Processing Agreement. City Network shall remain responsible at all times for compliance with the terms of the Agreement and this Data Processing Agreement by City Network Affiliates and Sub Data Processors.

City Network maintains a list of Sub Data Processors that the Customer has approved to Process the Personal Data of City Network's Service customers and will provide a copy of that list to Customer upon request. All Sub Data Processors are required to abide by substantially the same obligations as City Network under this Data Processing Agreement as applicable to their performance of the Services.

Customer may request that City Network audit the Sub Data Processors or provide confirmation that such an audit has occurred (or, where available, obtain or assist customer in obtaining a third-party audit report concerning Sub Data Processors' operations) to ensure compliance with such obligations. Customer also will be entitled, upon written request, to receive copies of the relevant terms of City Network's agreement with Sub Data Processors that may Process Personal Data, unless the agreement contains confidential information, in which case City Network may provide a redacted version of such agreement.

13. Technical and Organizational Measures

City Network will implement and maintain compliance with necessary and appropriate technical and organizational measures to protect the Processing of Personal Data against unauthorized access, destruction and alteration. City Network may update or modify its security measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

To prevent unauthorized persons from gaining access to data processing systems in which Personal Data is Processed (physical access control), City Network shall take measures to prevent physical access, such as security personnel and secured buildings and factory premises.

To prevent data processing systems from being used without authorization (system access control), the following may be applied depending upon the particular Services ordered: authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes, and logging of access on several levels.

For Services hosted at City Network, (i) logins to services environments by City Network employees and Sub Data Processors are logged; (ii) logical access to the data centres is restricted and protected by firewall/VLAN; and (iii) the following security processes are applied: intrusion detection system, centralized logging and alerting, and firewalls.

To ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access, and that Personal Data cannot be read, copied, modified or removed without authorization in the course of Processing and/or after storage (data access control), Personal Data is accessible and manageable only by properly authorized staff, contractors and sub processors, direct database query access is restricted, and application access rights are established and enforced.

To ensure that Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which entities the transfer of Personal Data by means of data transmission facilities is envisaged (transmission control), City Network will comply with the following requirements: Except as otherwise specified for the Services, transfers of data outside the Service environment may be encrypted. Activating this is the Customer responsibility. The content of communications (including sender and recipient addresses) sent through some email or messaging services may not be encrypted once received through such services.

To ensure that it is possible to check and establish whether and by whom Personal Data have been entered into data processing systems, modified or removed (input control), City Network will comply with the following requirements: The

Personal Data source is under the control of the Customer, and Personal Data integration into the system is managed by secured file transfer (i.e., via web services or entered into the application) from the Customer.

To ensure that Personal Data is Processed strictly in accordance with the instructions of the Customer, City Network must comply with the instructions of the Customer concerning Processing of Personal Data; such instructions are specified in the Agreement and in this Data Processing Agreement, and may additionally be provided by Customer in writing from time to time.

To ensure that Personal Data is protected against accidental destruction or loss, for Services hosted by City Network: back-ups can be taken on a regular basis but activating this is the responsibility of the Customer; back-ups are encrypted and are secured. It is the Customers responsibility to ensure that back-ups are taken in a manner that meets all legal requirements. Further information on back-up can be read in the General Terms and Condition (https://citycontrolpanel.com/files/City_Network_General_Terms_And_Conditions_City_Cloud.pdf) for this Service.

To ensure that Personal Data which is collected for different purposes may be Processed separately, data from different City Network's customers' environments is logically segregated on City Network's systems.

The Controller has the final responsibility to assess which safety measure need to be implemented. However, upon the effectiveness of the General Data Protection Act ("GDPR") on 25 May 2018, the Processor will have its own responsibility to safeguard that essential security measures for processing is implemented and if necessary implement further technical and safety measures. Should this further technical and organizational measures increase cost for the Processor shall this be paid separately by the Controller.

Security Certifications and Reports. City Network will maintain the ISO 27001 Certification to evaluate and help ensure the continued effectiveness of the security measures.

Impact Assessments and Consultations. Customer agrees that City Network will (taking into account the nature of the processing and the information available to City Network) assist Customer in ensuring compliance with any obligations of Customer in respect of data protection impact assessments and prior consultation, including if applicable Customer's obligations pursuant to Articles 35 and 36 of the GDPR.

City Network is entitled to compensation from the Customer for assistance with Impact Assessments and Consultations if the requested action is not otherwise apparent from the Data Processing Agreement.

14. Audit Rights

City Network shall provide the Customer with certificates of compliance with data protection and cloud security applicable to the Services, upon the Customer's request. Customer may audit City Network's compliance with the terms of the Agreement and this Data Processing Agreement up to once per year. Customer may perform more frequent audits of the Service computer systems that Process Personal Data to the extent required by laws applicable to Customer. If a third party is to conduct the audit, the third party must be mutually agreed to by Customer and City Network and must execute a written confidentiality agreement acceptable to City Network before conducting the audit.

To request an audit, Customer must submit a detailed audit plan at least two weeks in advance of the proposed audit date to City Network describing the proposed scope, duration, and start date of the audit. City Network will review the audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise City Network security, privacy, or employment policies). Customer will provide City Network any audit reports generated in connection with any audit under this section, unless prohibited by law. Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of the Agreement and this Data Processing Agreement. The audit reports are Confidential Information of the parties under the terms of this Data Processing Agreement.

City Network will provide at least one (1) opportunity for Customers to perform audits free of charge within a 12 months period. The time and date of this opportunity will be determined by City Network. Any additional audits are at the Customer's expense. Any request for City Network to provide assistance with an audit is considered a separate service if such audit assistance requires the use of different or additional resources. City Network will seek the Customer's written approval and agreement to pay any related fees before performing such audit assistance.

15. Incident Management and Notification

Incident Notification. If City Network becomes aware of a Data Incident, City Network will: (a) notify Customer of the Data Incident promptly and without undue delay; and (b) promptly take reasonable steps to minimize harm and secure Customer Data. The Parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected Data Subjects.

Details of Data Incident. Notifications made pursuant to this section will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps City Network recommends Customer take to address the Data Incident.

Delivery of Notification. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address or, at City Network's discretion, by direct communication (for example, by phone call or an in-person meeting). Customer is solely responsible for ensuring that the Notification Email Address is current and valid.

No Assessment of Customer Data by City Network. City Network will not assess the contents of Customer Data in order to identify information subject to any specific legal requirements. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Data Incident(s).

No Acknowledgment of Fault by City Network. City Network's notification of or response to a Data Incident under this Section 15 will not be construed as an acknowledgement by City Network of any fault or liability with respect to the Data Incident.

16. Return and Deletion of Personal Data Upon End of Services or at Customer's Request ("Data Portability")

Following termination or expiry of this Data Processing Agreement and depending on what the Controller decide, the Processor shall, and shall make any potential Sub Data Processor to, either return or otherwise make available for retrieval Customer's Personal Data and copies in the services environment. Following the deletion or return of the data, or as otherwise agreed, City Network will comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless EU or EU Member State law requires storage.

Customer acknowledges and agrees that Customer will be responsible for exporting, before the applicable Term expires, any of its Personal Data it wishes to retain afterwards.

17. Legally Required Disclosures

Except as otherwise required by law, City Network will promptly notify Customer of any subpoena, judicial, administrative or arbitral order of an executive or administrative agency or other governmental authority ("Demand") that it receives and which relates to the Personal Data City Network is Processing on Customer's behalf.

At Customer's request, and to the extent permitted by law, City Network will provide Customer with reasonable information in its possession that may be responsive to the Demand and any assistance reasonably required for Customer to respond to the demand in a timely manner.

Upon the effectiveness of the GDPR, the Processor is obligated, on request, to collaborate with the Data Protection Authority. This provision will take precedence to any confidentiality obligations which the Processor concluded with the Controller.

Processing Records. Customer acknowledges that City Network is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which City Network is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly, if the GDPR applies to the processing of Customer's Personal Data, Customer will, where requested, provide such information to City Network via the admin console or other means provided by City Network, and will use the admin console or such other means to ensure that all information provided is kept accurate and up-to-date.

18. Warranties and Indemnification

Customer warrants that the use of the Service will not be misused. For the purpose of this section, misused shall mean: (i) acting non-compliant with applicable laws on Personal Data and data security; (ii) spreading information which can be seen as illegal or seeks to be used for illegal activities; (iii) irresponsible spreading of collected or complied Personal Data; (iv) or in any way engaging in acting which can cause harm to City Network, City Networks System or City Networks other customers.

Customer shall indemnify and hold City Network harmless in case Customer should breach any of its obligations in Section 18 above.

Customer shall further indemnify City Network in the event that the Parties are subject to an administrative fee, claim or award for damages arising out of the Agreement.

19. Effect of Amendment.

To the extent of any conflict or inconsistency between the terms of this Data Processing Amendment and the remainder of the applicable Agreement, the terms of this Data Processing Amendment will govern. Subject to the amendments in this Data Processing Amendment, such Agreement remains in full force and effect. For clarity, if Customer has entered more than one Agreement, this Data Processing Amendment will amend each of the Agreements separately.