

DATA PROCESSING AGREEMENT

1. INTRODUCTION

- 1.1. This data processing agreement (the "DPA") sets out Customer's rights and obligations as controller ("Data Controller") and Quinyx' rights and obligations as processor ("Data Processor") when Quinyx processes Personal Data on Customer's behalf in providing the Services, and forms part of the Agreement. Capitalised terms not defined in this DPA have the meaning given in the Agreement.
- 1.2. Nothing in this DPA affects either party's exclusions or limitations of liability under the Agreement, unless this DPA expressly provides otherwise.
- 1.3. In this DPA, the terms:
 - a) "controller", "data subject", "processing", "processor" and "personal data" have the meanings given in the applicable data protection laws. A reference to "Personal Data" shall for the purposes of this DPA be deemed to be a reference to personal data provided by Data Controller or its Users under the Agreement;
 - b) "data protection laws" means all laws and regulations applicable to the processing of Personal Data under this DPA, including the General Data Protection Regulation ("GDPR") and, where relevant, the UK GDPR; and
 - c) "EEA" means the European Economic Area.

2. PROCESSING OF PERSONAL DATA

- 2.1. Data Processor shall process Personal Data only on Data Controller's documented instructions, unless required otherwise by data protection laws, in which case Data Processor shall, unless prohibited by law, inform Data Controller of that legal requirement before processing. Data Processor shall immediately inform Data Controller if, in its opinion, an instruction infringes data protection laws. Data Controller's initial instructions to Data Processor regarding the subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data and categories of data subjects are set forth in this DPA and in Appendix 1A. Other than instructions given under this clause 2.1, the obligations of Data Processor set out in this DPA (including its appendices) constitute the full instructions to Data Processor. Changes to these instructions require the parties' written agreement.
- 2.2. Data Controller warrants to Data Processor that:
 - a) it has, and will maintain, all rights, licences, consents and authorisations needed to transmit the Personal Data to Data Processor and to have it processed and used for the purposes contemplated by the Agreement;
 - b) any data (including Personal Data) which it transmits to Data Processor will be accurate and up to date, and Data Controller is responsible for the legality, reliability, integrity, accuracy and quality of that data; and
 - c) it complies with, and will comply with, all data protection laws, including transparency requirements, and will ensure that its instructions to Data Processor also comply with such laws.
- 2.3. Data Processor shall, to the extent required by data

protection laws, assist Data Controller in fulfilling its legal obligations under such laws, in accordance with Data Controller's written instructions.

3. EXERCISE OF ACCESS RIGHTS

- 3.1. If data subjects, competent authorities or other third parties request information or seek to exercise rights under data protection law from Data Processor regarding the processing of Personal Data ("Requests"), Data Processor shall refer the Request to Data Controller unless prevented by law. Subject to clause 3.2, Data Processor may not respond to a Request on behalf of, or as a representative of, Data Controller, nor disclose Personal Data or related information to a third party in connection with a Request, without Data Controller's prior instructions. Data Controller is solely responsible for responding substantively to Requests.
- 3.2. If Data Processor cannot determine the applicable data controller from a Request, it may contact the data subject for further information. If Data Processor is required by law to disclose Personal Data it processes on Data Controller's behalf, it shall immediately inform Data Controller and request confidentiality regarding the disclosure, unless prevented by law from doing so.
- 3.3. A party subject to a claim from a data subject arising out of or in connection with this DPA shall without undue delay notify the other party in writing, if the claim relates to the other party's alleged acts or omissions.

4. SUB-PROCESSORS AND THIRD COUNTRY TRANSFERS

- 4.1. Subject to clause 4.2, Data Processor may engage additional or replacement sub-processors without further specific authorisation from Data Controller.
- 4.2. Data Processor will inform Data Controller in an appropriate manner (typically via a release note) at least 30 days prior to engaging any new sub-processor to carry out processing activities under this DPA ("Initial Notice"), and shall, on request, provide information reasonably needed to assess the proposed sub-processor. Data Controller may object to such engagement, but agrees to do so only to the extent it considers (and can reasonably demonstrate to Data Processor) that compliance with this DPA and the data protection laws will not be maintained through the proposed sub-processor. If the parties cannot reach a mutually acceptable solution following such objection, Data Controller's shall as sole consequence be entitled to suspend or terminate the Agreement with immediate effect on written notice and without liability provided such notice is given within 30 days of the Initial Notice. If Data Controller has not objected to the new sub-processor within 30 days from the Initial Notice, the new sub-processor shall be considered approved.
- 4.3. Where Data Processor authorises a sub-processor under clauses 4.1 and 4.2, Data Processor shall impose data processing obligations on the sub-processor substantially equivalent to those in this DPA by written contract, and remain accountable to Data Controller for the sub-processor's acts and omissions as if they were Data Processor's own.

4.4. A list of approved sub-processors as of the effective date is available on <https://legal.quinyx.com/sub-processors>. Sub-processors engaged solely for a specific Data Controller (for example, implementation or integration partners) may instead be notified individually to Data Controller. Sub-processors approved under an earlier data processing agreement between the parties remain approved under this DPA. Data Processor may update the list of approved sub-processors from time to time in accordance with clauses 4.1 and 4.2.

4.5. Notwithstanding clauses 4.3 and 7.1, Data Controller accepts that Data Processor's engagement of Amazon Web Services ("Amazon") as an approved sub-processor is governed by a data processing agreement with Amazon based on Amazon's standards for data processing agreements, and Data Processor shall not be obligated to enforce on Amazon other obligations regarding the processing of Personal Data beyond that agreement and Amazon's terms of service entered into between Amazon and Data Processor.

4.6. Data Processor shall not transfer any Personal Data outside of the EEA (or, where UK GDPR applies, outside of the UK) unless:

- a) the Personal Data is processed in a territory recognised by the European Commission or the UK's Information Commissioner's Office (as applicable) as providing adequate protection; or
- b) a valid cross-border transfer mechanism is in place under data protection laws, such as standard contractual clauses ("SCCs").

5. INFORMATION SECURITY AND CONFIDENTIALITY

5.1. Data Processor shall comply with its legal obligations on information security under data protection laws, including taking appropriate technical and organisational measures to protect Personal Data processed.

5.2. Data Processor shall maintain a level of security for the Services in accordance with industry practice and data protection laws, including reasonable administrative, physical, technical, organisational and other security measures to protect against unauthorised access, loss, destruction, unavailability or alteration of Personal Data. Data Processor's security measures are described in the latest version of the "Quinyx Security Overview", available at quinyx.com/policies. Data Processor may update the security measures from time to time, provided that the overall level of security is not degraded.

5.3. Data Processor may only disclose Personal Data processed under this DPA (a) to its own personnel and to sub-processors engaged in accordance with this DPA (and their personnel), to the extent such disclosure is reasonably required for the purposes of the Agreement and provided that such recipients are bound by a statutory or contractual confidentiality obligation; or (b) as compelled by law.

6. PERSONAL DATA BREACH NOTIFICATIONS

6.1. Data Processor shall inform Data Controller without undue delay after becoming aware of a breach of security leading to accidental or unlawful destruction, loss, alteration, or

unauthorised disclosure of or access to, Personal Data ("Personal Data Breach").

6.2. Data Processor shall assist Data Controller providing Data Controller with any information reasonably required to fulfil its Personal Data Breach notification requirements.

7. AUDIT RIGHTS

7.1. Data Controller shall be entitled to take measures necessary to verify that Data Processor is in compliance with its obligations under this DPA. Data Processor undertakes to make available to the Data Controller all information and all assistance reasonably necessary to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller. Where possible, Data Processor may satisfy an audit request under this clause by making available information and relevant third-party certifications or audit reports (such as ISO 27001 or SOC 2) in lieu of an on-site inspection. Any audit or inspection under this clause shall be limited to the processing of Data Controller's own Personal Data and shall not extend to any data or confidential information of Data Processor's other customers.

8. MEASURES UPON COMPLETION OF PROCESSING OF PERSONAL DATA

8.1. Upon expiry or termination of this DPA, Data Processor will, unless instructed otherwise in writing by Data Controller, erase any Personal Data processed under this DPA within 90 days after the expiry date or effective date of termination, remaining bound by this DPA for that limited purpose.

8.2. Upon request by Data Controller, Data Processor shall provide a written notice of the measures taken regarding the Personal Data set out in clause 8.1.

9. CHARGES

9.1. As a general principle, Data Processor may not charge for any assistance provided to Data Controller under clauses 2.3, 3.1 or 6.2, or in connection with audits under clause 7.1, or measures required by Data Controller upon completion of processing under clause 8.1 (together, "Assistance"). Data Processor may charge reasonable costs on a time and materials basis for Assistance only to the extent Data Controller's request goes above and beyond what is reasonable to expect from a data processor under the data protection laws, typically requests requiring extensive resources and/or repeated requests not part of the standard Service. Data Processor shall in such event inform Data Controller in writing of its intention to charge, including the estimated costs, enabling the Data Controller to assess the costs involved.

9.2. In case of changed instructions under clause 2.1, Data Processor shall be entitled to charge for any reasonable and documented additional costs for the performance of the Services which are due to the change, unless the change is caused by general demands on the Services that cannot be specifically attributed to Data Controller, e.g. amendments or changes to applicable legislation or industry standards.

APPENDIX 1A – DATA PROCESSING INSTRUCTIONS

Purposes

- a) Provisioning of (i) automated personnel administrative workforce management services such as scheduling of shifts, time recording, task management and preparation of input for salary calculations etc. relating to employees or contractors, (ii) automated personnel administrative, operational and communication management services such as task management, store operations, company communications and directives, approval processes, compliance reporting etc. relating to stores and employees or contractors, and/or (iii) workforce optimisation solutions to improve strategic planning, demand forecasting, and labour optimisation.
- b) Professional services and administrative activities in connection with a) above.
- c) System development, analysis and testing to ensure quality of Services provided to Data Controller in accordance with a) above.

Categories of data

Name, employee profile image, login ID, employee number, card number (for time punching), birth date, sex, address, phone number, e-mail address, employee category, store/unit/department, performance ranking, social security number, next of kin, skills and certifications, schedule details, task details, salary details, absence details, employment contract details, employment type, employment period, employment percentage employee messages, and any other categories of data submitted by Data Controller to Data Processor from time to time for purposes of the Services.

Categories of Data Subjects

Employees, former employees, emergency contact(s), and any other categories of data subjects submitted by Data Controller to Data Processor from time to time for purposes of the Services.

Processing Operations

Collection, registration, storing, processing, deletion, automated translations, analysis, anonymisation or pseudonymisation and distribution.

Location of Processing Operations

Processing operations are primarily located in the EEA and UK, with hosting in Frankfurt and Dublin through Amazon. For customers based in North America, processing operations are primarily located in the US, with hosting in North Virginia and Oregon through Amazon.

Information Security

In accordance with the latest version of Quinyx Security Overview document, available from time to time at quinyx.com/policies.