Xurrent DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "**Addendum**") is made and entered into by and between Xurrent, Inc., a Delaware corporation ("**Xurrent**") and the customer specified in the table below ("**Customer**").

Xurrent, Inc.	**Customer:**
Signature:	Signature:
Name:	Name:
Title:	Title:
Date signed:	Date signed:
Address: 8 W. Victoria Street Santa Barbara, CA 93101 U.S.A.	Address:

This Addendum is an addendum to the Xurrent Customer Agreement available at https://www.xurrent.com/agreement, as updated from time to time between Customer and Xurrent, or other agreement between Customer and Xurrent governing Customer's use of the Service (the "**Agreement**"). Unless otherwise defined in this Addendum or in the Agreement, all capitalized terms used in this Addendum will have the meaning given to them in Section 17 (Definitions) of this Addendum. All of the terms of the Agreement shall apply to this Addendum. In the event of conflict between the terms of this Addendum and the Agreement, as regards data protection this Addendum shall prevail.

1. Data Processing.

1.1. Scope and Roles. This Addendum applies when Customer Personal Data is processed by Xurrent. The parties acknowledge that in relation to all Customer Personal Data, as between the parties, Customer is the Controller or Responsible Party of Customer Data, and Xurrent is acting as a Processor or Operator on behalf of the Customer in the course of providing the Service.

1.2. The purpose, subject matter and duration of the Processing carried out by Xurrent on behalf of the Customer, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects are described in **Schedule 1** attached hereto.

1.3. Customer Controls. The Service provides Customer with a number of controls, including security features and functionalities, that Customer may use to access, rectify, erase or restrict processing of Customer Personal Data. Customer may use these controls as technical and organizational measures to assist it in connection with its obligations under data protection legislation including its obligations relating to responding to requests from data subject.

1.4. Compliance with Laws. Each party will comply with all applicable Data Protection Legislation in processing Customer Personal Data under the Agreement and this Addendum.

1.5. Access or Use. Xurrent will not access or use Customer Data, except as necessary to maintain or provide the Service.

1.6. AI Processing. Xurrent does not use Customer Data to train AI models. Xurrent is providing AI functions by utilizing pre-trained models offered by AWS Bedrock in the same Processing Region as the Customer's Data is located. AI functions are clearly marked and can be disabled by the Customer.

2. **Customer Instructions.** Xurrent will process Customer Personal Data only in accordance with Customer's instructions. The parties agree that this Addendum with Appendixes is Customer's complete and final documented instruction to Xurrent in relation to Customer Personal Data. Additional instructions outside the scope of this Addendum (if any) require prior written agreement between Xurrent and Customer, including agreement on any additional fees payable by Customer to Xurrent for carrying out such instructions. Customer is entitled to terminate this Addendum and the Agreement if Xurrent declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this Addendum. Customer shall ensure that its instructions comply with all laws, rules and regulations applicable in relation to the Customer Personal Data.

3. **Law Enforcement.** In the event Xurrent receives an order from a law enforcement agency for compelled disclosure of any Customer Personal Data, Xurrent shall use reasonable effort to:

   (a) redirect the law enforcement agency directly to the Data Controller;
   (b) promptly notify the Data Controller (if permitted);
   (c) if possible and commercially viable, challenge the order for disclosure on the basis of any legal defences available under the laws of the requesting party or any relevant conflicts with the law of the European Union, applicable Member State law or Customer's local law.

4. **Confidentiality of Processing.** Xurrent restricts any person from processing Customer Data without authorization by Xurrent as described in the Xurrent Technical and Organizational Measures. Xurrent imposes appropriate contractual obligations upon its staff, agents and subprocessors, including relevant obligations regarding confidentiality, data protection and data security.

5. **Subprocessing.**

   5.1. Authorized Subprocessors. Customer agrees that Xurrent may use subprocessors to fulfill its contractual obligations under this Addendum or to provide certain services on its behalf, such as providing support services. **Schedule 3** attached hereto (as updated from time to time on Xurrent's website at https://www.xurrent.com/subprocessors/) lists the subprocessors that are engaged by Xurrent to carry out specific processing activities on behalf of Customer. At least thirty (30) days before Xurrent authorizes and permits a new subprocessor to access any Customer Personal Data, Xurrent will proactively inform Customer. Customer can object to a new subprocessor by notifying Xurrent promptly in writing within thirty (30) days after the announcement to engage the new subprocessor. Such notice shall explain the reasonable grounds for the objection. In the event Customer objects to a new subprocessor, Xurrent will use commercially reasonable efforts to make available to Customer a change in the Service or recommend a commercially reasonable change to Customer's configuration or use of the Service to avoid processing of Customer Personal Data by the objected-to new subprocessor without unreasonably burdening Customer. If Xurrent is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, either party may terminate without penalty the applicable order form(s) with respect only to those Service element(s) which cannot be provided by Xurrent without the use of the objected-to new subprocessor by providing written notice to Xurrent. Xurrent will refund Customer any prepaid fees covering the remainder of the term of such order form(s) following the effective date of termination with respect to such terminated element(s) of the Service, without imposing a penalty for such termination on Customer. Except as set forth in this Section, or as Customer may otherwise authorize, Xurrent will not permit any subprocessor to carry out specific processing activities on behalf of Customer.

   5.2. Subprocessor Obligations. Where Xurrent appoints any subprocessor as described in Section 5.1:

   i. Xurrent will restrict the access of subprocessor to Customer Data only to what is necessary to maintain the Service or to provide the Service to Customer. Xurrent will prohibit the subprocessor from accessing Customer Data for any other purpose;

   ii. Xurrent will enter into a written agreement with the subprocessor and, to the extent that the subprocessor is performing the same data processing services that are being provided by Xurrent under this Addendum, Xurrent will impose on the subprocessor the same contractual obligations that Xurrent has under this Addendum; and

iii. Xurrent will remain responsible for its compliance with the obligations of this Addendum and for any acts or omissions of the subprocessor that cause Xurrent to breach any of Xurrent's obligations under this Addendum.

6. Customer Personal Data Transfers

6.1. Where the GDPR, UK GDPR or the Swiss FADP is applicable, if the Processing of Customer Personal Data by Xurrent (or by a subprocessor) includes transfer of Customer Personal Data (either directly or through an onward transfer) to a third country outside the EEA, the UK, or Switzerland that is not an Adequate Country, such transfer shall only occur if an appropriate safeguard approved by the applicable Data Protection Law (the GDPR (Article 46), UK GDPR (Article 46) or Swiss FADP (as applicable) for the lawful transfer of Customer Personal Data is in place.

6.2. If Xurrent or its subprocessor relies on the Standard Contractual Clauses to facilitate a transfer to a third country that is not an Adequate Country, then:

i. Transfer of Personal Data from the EEA the terms set forth in **Schedule 4** shall apply.

ii. Transfer of Personal Data from the UK, the terms set forth in **Schedule 5** shall apply; and

iii. Transfer of Personal Data from Switzerland, the terms set forth in **Schedule 6** shall apply.

If Customer is based In California, the provisions of **Schedule 7** shall apply.

7. Data Subject Rights. Xurrent shall assist the Customer, taking into account the nature of the processing and the information available to it, in complying with the obligations set out in Articles 32 to 36 GDPR. Xurrent offers Customer certain controls as described in Section 1.2 (Customer Controls) and Section 9 (Customer Security Controls) that Customer may elect to use to comply with its obligations towards data subjects.

7.1. Access, Rectification, Erase, Restrict, Portability. Xurrent will, in a manner consistent with the functionality of the Service, enable Customer to access, rectify, erase and restrict processing of Customer Personal Data, including via the erasure functionality provided by Xurrent as described in Section 8 (Erasure During Term), and to export Customer Data.

7.2. Data Subject Requests.

i. Customer's Responsibility for Requests. When Xurrent receives any request from a data subject in relation to Customer Personal Data, Xurrent will advise the data subject to submit their request to Customer, and Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Service.

ii. Xurrent Assistance. Customer agrees that (taking into account the nature of the processing of Customer Personal Data) Xurrent will assist Customer in fulfilling any obligation to respond to requests by data subjects, including, if applicable, Customer's obligation to respond to requests for exercising the data subject's rights (see Section 17 (Definitions)), by:

(a) providing the Customer Security Controls in accordance with Section 9.3 (Customer Security Controls)

(b) complying with the commitments for rectification, erase, restrict, portability) and supporting Customer's responsibility for requests).

Should a data subject contact Xurrent with regards to correction or deletion of their personal data, Xurrent will use commercially reasonable efforts to forward such requests to Customer without delay.

8. Data Erasure.

8.1. Erasure During Term of the Agreement. Xurrent will enable Customer and/or End Users to erase Customer Data during the term of the Agreement in a manner consistent with the functionality of the Service. If Customer uses the Service to erase any Customer Data during the term of the Agreement and the Customer Data cannot be recovered by Customer, this use will constitute an instruction to Xurrent to erase the relevant Customer Data from Xurrent's systems in accordance with applicable law. Xurrent will comply with this instruction as soon as reasonably practicable and within a maximum period of 30 days, unless applicable law

requires storage or there are any contractual retention obligations to the contrary. Xurrent will inform the Customer when the data erasure will be completed.

8.2. Erasure on Expiry or Termination of the Agreement. On expiry or termination of the Agreement, Customer instructs Xurrent to erase all Customer Data (including existing copies) from Xurrent's systems in accordance with applicable law. Xurrent will comply with this instruction as soon as reasonably practicable and within a maximum period of 30 days after the account is settled, unless applicable law requires storage or there are any contractual retention obligations to the contrary. Without prejudice to Section 7.1 (Access, Rectification, Erase, Restrict, Portability), Customer acknowledges and agrees that Customer will be responsible for exporting, before the end of the 30 days period mentioned above, any Customer Data it wishes to retain afterwards. Xurrent will inform the Customer when the data erasure will be completed.

9. Technical and Organizational Measures, Compliance and Controls.

9.1. Xurrent Technical and Organizational Measures. Xurrent shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality, integrity and availability of Customer Data, as set forth in the Xurrent TOMs. Xurrent regularly reviews compliance with these TOMs as well as subprocessors' compliance with their technical and organizational measures. Xurrent may update or modify the Xurrent TOMs from time to time provided that such updates and modifications do not materially decrease the overall security of the Service.

9.2. TOMs Compliance by Xurrent Staff. Xurrent will take appropriate steps to ensure compliance with the Xurrent TOMs by its staff, contractors and subprocessors to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

9.3. Customer Security Controls. Xurrent provides Customer with information about securing, accessing and using Customer Data, and makes available a number of security controls that Customer may elect to use. Customer is responsible for (a) properly configuring the Services, (b) using the controls available in connection with the Service (including the security controls) to ensure the ongoing confidentiality and integrity of Customer Data, and (c) taking such steps as Customer considers adequate to maintain appropriate security, protection, and erasure of Customer Data, which includes measures to control access rights to Customer Data.

10. Security Incident Response.

10.1. Incident Notification. If Xurrent becomes aware of a Security Incident impacting Customer's operation or unauthorized access to Customer data, Xurrent will without undue delay (within 48 hours where possible):
(a) notify Customer of the Security Incident; and
(b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident. The notification shall include information about:
(a) the time and nature of the incident;
(b) the time of discovery;
(c) the data subjects and affected Controller Data, including an estimate of the number of affected data subjects and Controller Data;
(d) likely consequences of the data security incident and/or personal data breach;
(e) measures already adopted or proposed by the Processor to address or mitigate its possible adverse effects, where applicable.

10.2. No Assessment of Customer Data by Xurrent. Xurrent 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 Security Incident(s).

10.3. Unsuccessful Security Incidents. Customer agrees that Xurrent assesses whether the personal data processed for the Customer is affected by a security incident. If not, this Security Incident will not be subject to this Section 10. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data

or to any of Xurrent's equipment or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful access attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

10.4. No Acknowledgement of Fault by Xurrent. Xurrent's obligation to report or respond to a Security Incident under this Section 10 is not and will not be construed as an acknowledgement by Xurrent of any fault or liability of Xurrent with respect to the Security Incident.

10.5. Communication. Notifications of Security Incidents, if any, as well as other security and compliance related communication mentioned in this Data Processing Addendum, will be delivered to Customer's representative (if applicable) and/or Customer's data protection/security officer by any means Xurrent selects, including via email. It is Customer's sole responsibility to ensure Customer's Xurrent account owner maintains accurate contact information within the Xurrent Settings console section "Legal & Compliance", and secure transmission at all times.

10.6. Privacy Impact Assessment and Prior Consultation. The information made available by Xurrent under this Section 10 is intended to assist Customer in complying with Customer's obligations under applicable data protection law with respect to data protection impact assessments and prior consultation. Xurrent will provide Customer with additional documentation for Customer's compliance obligations if deemed necessary by Customer and if distribution is permitted for the requested documentation.

11. Certifications and Audits.

11.1. Xurrent Audits.

i. Xurrent engages accredited external auditors to verify the adequacy of the Xurrent TOMs. This audit: (a) will be performed at least annually; (b) will be performed according to industry standards; (c) will be performed by independent third-party security professionals at Xurrent's selection and expense; and (d) will result in the generation of an audit report ("Report"), which will be Xurrent's Confidential Information. If Customer's agreement with Xurrent for the Service does not include a provision protecting Xurrent Confidential Information, then Reports will be made available to Customer subject to a mutually agreed upon non-disclosure agreement covering the Report (an "NDA").

ii. Xurrent engages independent entities to conduct regular application-level and infrastructure-level penetration tests. Results of these tests are shared with Xurrent management. Xurrent's security team reviews and prioritizes the reported findings and tracks them to resolution. Customers wishing to conduct their own penetration test of the Service may request to do so and should contact their account representative to obtain permission from both Xurrent and Xurrent's hosting provider.

i. Xurrent's SaaS platform is compliant with the requirements of SOC 2 Type 2 for information security, availability and privacy, as well as ISO 27001:2013 and ISO 27018:2019. To evaluate and help ensure the continued effectiveness of the TOMs, Xurrent will update the SOC 2 report at least once every 12 months and will undergo yearly surveillance audits and a recertification audit after three years for the ISO certifications. Xurrent will notify Customer if there is any change in its audit strategy or if a significant finding/deviation during an audit will prevent Xurrent from continuing the above-mentioned compliance strategy and therefore maintaining the mentioned certifications.

11.2. Audit Reports. At Customer's written request, Xurrent will provide Customer with a confidential Report so that Customer can reasonably verify Xurrent's compliance with its obligations under this Addendum. The Report will constitute Xurrent's Confidential Information under the confidentiality provisions of the Agreement or the NDA, as applicable.

11.3. Independent Determination. Customer is responsible for reviewing the information made available by Xurrent relating to data security and making an independent determination as to whether the Services meets Customer's requirements and legal obligations as well as Customer's obligations under this Addendum.

11.4. Regulator Audits. Xurrent grants Regulators the unrestricted rights of inspection and auditing related to the Services (hereinafter "Audit Rights") to enable them to monitor the Service and to ensure compliance with all

applicable regulatory and contractual requirements. This Audit Right comprises, but is not limited to, the direct right to examine the Service, including the right to conduct an on-premise assessment and examination at Xurrent's offices and/or the right to copy relevant documents for this purpose. For this purpose, any person or entity exercising an internal or external audit function at Xurrent is released from any obligation of confidentiality and/or professional secrecy with respect to Customer to the extent required to comply with these Audit Rights.

11.5. Customer Audits. Xurrent also grants Audit Rights described in 11.4 of this Addendum to Customer and any other person or legal entity appointed by each of them with respect to the Service, but only to the extent necessary to comply with laws and regulatory requirements of any applicable jurisdiction. Customer may exercise this Audit Right annually upon reasonable notice to Xurrent (being not less than 30 days). The costs of the audit shall be borne by the Customer. If Xurrent declines to follow any instruction requested by Customer regarding audits or inspections, Customer is entitled to terminate this Addendum and the Agreement.

12. Personal Data Locations.

12.1. Storage Locations. Customer Personal Data in the main Xurrent Service is stored and processed either within the European Economic Area (EEA), the United Kingdom, Switzerland, Australia or the United States of America depending on the Customer's data processing location decision. Customer Personal Data in the Xurrent Workflow Automation Service is stored and processed either in the European Economic Area (for all Xurrent locations except USA) or in the United States of America.

13. Data Protection Team and Processing Records.

13.1. Data Protection Team. Xurrent's Data Protection Team can be contacted by Customer's Xurrent account administrators via privacy@Xurrent.com and/or by Customer by providing a notice to Xurrent as described in the Agreement.

13.2. Processing Records. Customer acknowledges that Xurrent is required under applicable data processing laws 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 Xurrent 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, Customer will, where requested, provide such information to Xurrent in the "Legal & Compliance" section that is available in the Settings console of the Service when logged in as the owner of Customer's Xurrent accounts, or other means provided by Xurrent, and will use the Settings console or such other means to ensure that all information provided is kept accurate and up-to-date.

14. Entire Agreement; Conflict. This Addendum supersedes and replaces all prior or contemporaneous representations, understandings, agreements, or communications between Customer and Xurrent, whether written or verbal, regarding the subject matter of this Addendum. Except as amended by this Addendum, the Agreement will remain in full force and effect. In case there is a conflict between this Addendum and the Standard Contractual Clauses, the applicable Standard Contractual Clauses will control.

15. Effective Date. This Addendum shall become effective between the respective Controller and Processor when the Addendum is signed. This Addendum may be executed in counterparts and by electronic signature, each of which shall be deemed an original, but all of which together shall be deemed to be one and the same agreement. An electronically signed copy of this Addendum delivered by e-mail as a PDF shall be deemed to have the same legal effect as delivery of an original signed copy of this Addendum.

16. Termination of the Addendum. This Addendum shall continue in force until the termination of the Agreement.

17. Definitions. Unless otherwise defined in the Agreement, all capitalized terms used in this Addendum will have the meanings given to them below:

"Adequate Country" is a country that has received an adequacy decision from the European Commission, the UK or other jurisdiction which applies the same or similar policy, as applicable.
"**Xurrent Infrastructure**" means data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are within Xurrent's control and are used to provide the Service.
"**Xurrent TOMs**" means the technical and organizational measures set out in **Schedule 2**.

"**CCPA**" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. Seq.
"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by UK, Swiss, Union or Member State law, the controller or the specific criteria for its nomination may be provided for by UK, Swiss, Union or Member State law.
"Customer Data" means data that is uploaded to the Service in Customer's Xurrent accounts and may include Customer Personal Data.
"Customer Personal Data" means the "personal data" (as defined in the GDPR and other Data Protection Legislation) contained within the Customer Data.
"Data Controller, Data Processor, Data Subject, Personal Data, Data Breach, Processing, Processed and Process and appropriate technical and organizational measures" shall have the meaning as defined in the Data Protection Legislation.
"Data Protection Legislation" means any and all applicable privacy and data protection laws and regulations, including, where applicable, the EU Data Protection Law, Swiss Data Protection Laws, the UK Data Protection Law, the POPIA, the Canadian Personal Information Protection and Electronic Documents Act, The Privacy Act 1988 in Australia and the CCPA, as all may be amended or superseded from time to time.
"Data Subject's Rights" according to Chapter III of the GDPR and section 5 of POPIA.
"EU Data Protection Law" or "**GDPR**" means the (i) EU General Data Protection Regulation (Regulation 2016/679) ("**GDPR**"); (ii) Regulation 2018/1725; (iii) the EU e-Privacy Directive (Directive 2002/58/EC), as amended (**e-Privacy Law**); (iv) any national data protection laws made under, pursuant to, replacing or succeeding (i) – (iii); and (iv) any legislation replacing or updating any of the foregoing.
"**EEA**" means the European Economic Area.
"Operator" means a person or company who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party according to POPIA.
"POPIA" means The Protection of Personal Information Act, 2013 (Act 4 of 2013) of South Africa with regard to processing of personal data, including juristic personal information.
"**Processing**" has the meaning given to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.
"Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
"Responsible Party" is the public or private body or any other person, which alone or in conjunction with others, determines the purpose of and means for processing personal information according to POPIA
"**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of Personal Data to third countries pursuant to the GDPR, as adopted by the European Commission **Decision 2021/914** of June 4, 2021 which is available at: https://eur-ex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN.
"**Security Incident**" means a breach of security of the Xurrent Technical and Organizational Measures leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data. "Security Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful access attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
"SOC 2 Report" means a confidential Service Organization Control (SOC) 2 Report (or a comparable report) on Xurrent's systems examining logical security controls, physical security controls, and privacy controls, as produced by Xurrent's third-party auditor in relation to the audited Service.
"Swiss Data Protection Laws" or **"FADP"** means the Swiss Federal Act on Data Protection of June 19, 1992, SR 235.1, and any other applicable data protection or privacy laws of the Swiss Confederation as amended, revised, consolidated, re-enacted or replaced from time to time, to the extent applicable to the processing of Personal Data under this Agreement.
"**Swiss SCC"** shall mean the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner.
"UK Data Protection Laws" means the Data Protection Act 2018 (DPA 2018), as amended, and the EU General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, as incorporated into UK law as the UK GDPR, and any other applicable UK data protection laws, or regulatory Codes of Conduct or other guidance that may be issued from time to time
"**UK SCC**" means the UK 'International data transfer addendum to the European Commission's standard contractual clauses for international data transfers', available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf as adopted, amended or updated by the UK's Information Commissioner's Office, Parliament or Secretary of State.

SCHEDULE 1

DETAILS OF DATA PROCESSING.

i. Subject Matter. The subject matter of the data processing under this Addendum is the Customer Personal Data.

ii. Duration. As between Customer and Xurrent, the duration of the data processing under this Addendum is determined by Customer. In general processing is happening as long as the Customer is actively using the Service.

iii. Purpose. The purpose of the data processing under the Addendum is the provision of an Enterprise Service Management System, among other things for use as a ticket system for incident problem and change management.

iv. Nature of the Processing. Storage and other processing necessary to provide, maintain and improve the Service (as described in the Agreement).

v. Categories of Data. The Customer Personal Data uploaded to the Service in Customer's accounts which may include, but not limited to, name and contact information, technical data, organizational data (structures and teams), roles and authorizations and content of tickets as well as juristic personal information.

vi. Categories of Data Subjects. The data subjects may include Customer's employees and contractors, customers, partners, suppliers, end users, and any person who uploads data via the Service, including individuals collaborating and communicating with end users.

SCHEDULE 2

Xurrent TECHNICAL AND ORGANIZATIONAL MEASURES

Xurrent will implement and maintain the Xurrent TOMs set out in this Schedule 2 to the Data Processing Addendum. Xurrent may update or modify the Xurrent TOMs from time to time provided that such updates and modifications do not materially decrease the overall security of the Service.

1. **Information Security Program.** Xurrent will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) satisfy the Xurrent Information Security Policy, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the Xurrent Infrastructure, and (c) minimize security risks, including through risk assessment and regular testing. Xurrent will designate one or more staff to coordinate and be accountable for the information security program. The information security program will include the following measures:

   1.1. **Data Centers.** Xurrent relies on the secure cloud infrastructure provided by its subprocessor AWS to store and process all Customer Data logically across multiple availability zones within the Customer selected region, protecting the Services from loss of connectivity, power infrastructure and other common location-specific failures.

   1.2. **Physical Security.** All data centers that run the Service are secured and monitored 24/7 and physical access to the data centers is strictly limited to select AWS staff who have a legitimate business need for such access privileges. No staff of Xurrent has, nor will be permitted to have, physical access to the data centers. This measure survives the end of the contract a staff member has with Xurrent.

   1.3. **Infrastructure Security.** The Xurrent Infrastructure will be electronically accessible to Xurrent staff, contractors and any other person as necessary to provide the Service. Xurrent will maintain access controls and policies to manage what access is allowed to the Xurrent Infrastructure from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Xurrent will maintain corrective action and incident response plans to respond to potential security threats.

   1.4. **Instance Security.** Xurrent takes all necessary precautions to ensure that every layer involved in data transfer is secured by best-of-breed technologies. The Service is based on a security-oriented bare minimal, lightweight operating system, preventing the exploitation of entire classes of zero-day and other vulnerabilities.

   1.5. **Customer Data Security.** The Service supports the latest recommended secure cipher suites and protocols to encrypt all data traffic in transit. All Customer Data is encrypted at rest – including, but not limited to: databases, search indexes, files storage, memory caches, log data, backups, and all disks.

   1.6. **Access Security.**

      i. **Infrastructure Security Staff.** Xurrent has, and maintains, a security policy for its staff, and requires security training as part of the training package for its staff. Xurrent's infrastructure security staff are responsible for the ongoing monitoring of Xurrent's security infrastructure, the review of the Service, and responding to security incidents.

      ii. **Customer Access.** In addition to the Technical and Organizational Measures Xurrent employs for its processes, systems and staff, Xurrent provides administrators of Xurrent accounts capabilities to enable their own users to protect their Customer Data. This includes controls such as role-based access, single sign on, SCIM provisioning, multi-factor authentication, password policies, visibility into audit trails and access logs, data retention settings, and capabilities to rectify, erase and restrict processing of Customer Personal Data.

      iii. **Internal Data Access.** Xurrent's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process Customer Data. Xurrent aims to design its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that Customer Data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. Xurrent employs a centralized access management system to control staff access to

production systems, and only provides access to a limited number of authorized staff. All access mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Xurrent requires the use of unique user IDs, strong passwords, two-factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized staff's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with Xurrent's internal data access policies and training. Approvals are managed by Xurrent that maintain audit trails of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication, password policies that follow at least industry standard practices are implemented. These standards include password expiry, restrictions on password reuse and sufficient password strength.

1.7. Personnel Security. Xurrent staff members are required to conduct themselves in a manner consistent with the Xurrent's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Xurrent conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations. Staff members are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Xurrent's security and privacy policies. Staff members are provided with security training annually and privacy training bi-annually. Xurrent staff members will not process Customer Data without authorization.

1.8. Subprocessor Security. Before using a subprocessor, Xurrent conducts an audit of the security and privacy practices of the subprocessor to ensure the subprocessor provides a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. This is also verified annually by Xurrent. Once Xurrent has assessed the risks presented by the subprocessor, then subject always to the requirements set out in Section 5 (subprocessing) of this Data Processing Addendum, the subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

2. Additional measures. Following the decision of European Court of Justice No. 311/18 (Schrems II) Xurrent certifies that (1) it has not purposefully created back doors or similar programming that could be used to access the system and/or personal data (2) it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and (3) that national law or government policy does not require the Processor to create or maintain back doors or to facilitate access to personal data or systems or for the Processor to be in possession or to hand over the encryption key.

3. Continued Evaluation. Xurrent will conduct periodic reviews of the security of its Xurrent Infrastructure and adequacy of its information security program as measured against industry security standards and its policies and procedures. Xurrent will continually evaluate the security of its Xurrent Infrastructure and associated Service to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

SCHEDULE 3

LIST OF SUB-PROCESSORS

The controller has authorized the use of the following subprocessors:

1. Name: Amazon Web Services
   Address: 410 Terry Ave North
   Seattle, WA 98109-5210
   U.S.A.
   Attention: General Counsel

   Description of processing: Facilitating the Virtual Private Cloud Infrastructure (local data centers) to enable the Processor to provide the Service.
   Location of processing in Europe: Ireland and Germany
   Subprocessor authorization: 2010

2. Name: Workato, Inc.
   Address: 215 Castro Street, Suite 300
   Mountain View, CA 94041
   U.S.A.
   Attention: Chief Information Security Officer, privacy@workato.com

   Description of processing: Workato provides a flexible business integration and automation service which is used by the Processor to provide the Xurrent Workflow Automator Service.
   Location of processing in Europe: Germany
   Subprocessor authorization: 2023

SCHEDULE 4

EEA INTERNATIONAL TRANSFERS AND SCCs

1. The parties agree that the terms of the Standard Contractual Clauses are hereby incorporated by reference and shall apply to transfer of Customer Personal Data from the EEA to other countries that are not deemed as Adequate Countries.

2. Module Two (Controller to Processor) of the Standard Contractual Clauses shall apply where the transfer is effectuated by Customer as the data Controller of the Personal Data and Xurrent is the data Processor of the Personal Data.

3. The Parties agree that for the purpose of transfer of Customer Personal Data between Customer (as Data Exporter) and the Xurrent (as Data Importer), the following shall apply:

   3.1. Clause 7 of the Standard Contractual Clauses shall not be applicable.

   3.2. In Clause 9, option 2 (general written authorization) shall apply and the method for appointing and time period for prior notice of subprocessor changes shall be as set forth in the subprocessing Section 5 of the Addendum.

   3.3. In Clause 11, the optional language will not apply, and data subjects shall not be able to lodge a complaint with an independent dispute resolution body.

   3.4. In Clause 17, option 1 shall apply. The parties agree that the Standard Contractual Clauses shall be governed by the laws of the EU Member State in which the Customer is established (where applicable).

   3.5. In Clause 18(b) the parties choose the courts of the Republic of Ireland, as their choice of forum and jurisdiction.

4. **Annex I.A** of the Standard Contractual Clauses shall be completed as follows:

   4.1.1. "**Data Exporter**": Customer
   4.1.2. "**Data Importer**": Xurrent
   4.1.3. Roles: (A) With respect to Module Two: (i) Data Exporter is a data controller and (ii) the Data Importer is a data processor.
   4.1.4. Data Exporter and Data Importer Contact details: As detailed in the Agreement and Addendum.
   4.1.5. Signature and Date: By entering into the Agreement and Addendum, Data Exporter and Data Importer are deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

5. **Annex I.B** of the Standard Contractual Clauses shall be completed as follows:

   5.1. The purpose of the processing, nature of the processing, categories of data subjects, categories of personal data and the parties' intention with respect to the transfer of special categories are as described in **Schedule 1** (Details of Processing) of Addendum.

   5.2. The frequency of the transfer and the retention period of the personal data is as described in **Schedule 1** (Details of Processing) of the Addendum.

   5.3. The subprocessors which Personal Data is transferred to are listed in **Schedule 3**.

6. **Annex I.C** of the Standard Contractual Clauses shall be completed as follows: the competent supervisory authority in accordance with Clause 13 is the supervisory authority in the Member State stipulated in Section 3 above.

7. **Schedule 2** of this Addendum (Xurrent TOMs) serves as **Annex II** of the Standard Contractual Clauses.

8. **Schedule 3** of this Addendum (List of Sub-processors) serves as **Annex III** of the Standard Contractual Clauses.

SCHEDULE 5

UK INTERNATIONAL TRANSFERS AND SCCs

1. The parties agree that the terms of the Standard Contractual Clauses as amended by the UK Standard Contractual Clauses, and as amended in this Schedule 5, are hereby incorporated by reference and shall apply to transfer of Customer Personal Data from the UK to other countries that are not deemed as Adequate Countries.

2. This Schedule 5 is intended to provide appropriate safeguards for the purposes of transfers of Customer Personal Data to a third country in reliance on Article 46 of the UK GDPR and with respect to Customer Personal Data transfers from controllers to processors or from the processor to its subprocessors.

3. Terms used in this Schedule 5 that are defined in the Standard Contractual Clauses, shall have the same meaning as in the Standard Contractual Clauses.

4. This Schedule 5 shall (i) be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that if fulfills the intention for it to provide the appropriate safeguards as required by Article 46 of the UK GDPR, and (ii) not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.

5. Amendments to the UK Standard Contractual Clauses:

5.1. Part 1: Tables

5.1.1. Table 1 Parties: shall be completed as set forth in the Addendum above.

5.1.2. Table 2 Selected SCCs, Modules and Selected Clauses: shall be completed as set forth in Section 2 and 3 within Schedule 4 above.

5.1.3. Table 3 Appendix Information:

Annex 1A: List of Parties: shall be completed as set forth in the Addendum above.

Annex 1B: Description of Transfer: shall be completed as set forth in Schedule 1 above.

Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: shall be completed as set forth in Schedule 2 above.

Annex III: List of Sub processors: shall be completed as set forth in Schedule 3 above.

5.1.4. Table 4 Ending this Addendum when the Approved Addendum Changes: shall be completed as “neither party”.

SCHEDULE 6

SUPPLEMENTARY TERMS FOR SWISS DATA PROTECTION LAW TRANSFERS ONLY

The following terms supplement the Clauses only if and to the extent the Clauses apply with respect to data transfers subject to Swiss Data Protection Law, and specifically the FDPA:

- The term 'Member State' will be interpreted in such a way as to allow data subjects in Switzerland to exercise their rights under the Clauses in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Clauses.

- The clauses in the Addendum protect the Customer Personal Data of legal entities until the entry into force of the Revised Swiss FDPA.

- All references in this Addendum to the GDPR should be understood as references to the FDPA insofar as the data transfers are subject to the FDPA.

- References to the "competent supervisory authority", "competent courts" and "governing law" shall be interpreted as Swiss Data Protection Laws and Swiss Information Commissioner, the competent courts in Switzerland, and the laws of Switzerland (for Restricted Transfers from Switzerland).

- In respect of Customer Personal Data transfers governed by Swiss Data Protection Laws and Regulations, the EU SCCs will also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Customer Personal Data under Swiss Data Protection Laws and Regulations until such laws are amended to no longer apply to a legal entity.

- The competent supervisory authority is the Swiss Federal Data Protection Information Commissioner.

SCHEDULE 7

CCPA ADDENDUM

In addition to the requirements set forth under the Addendum, which shall apply to the collection, processing, use, sharing, sale, and retention of California residents' Personal Information, the obligations set forth under this Schedule 7 ("**CCPA Addendum**") shall further apply. All terms used but not defined in this CCPA Addendum.

1. For the purpose of the CCPA, Customer is the Business and Xurrent is the Service Provider.

2. Xurrent shall process Personal Information on behalf of the Customer as a Service Provider under the CCPA and shall not: (1) sell or share the Personal Information; (2) retain, use or disclose the Personal Information for any purpose other than for Customer purpose specified in the Agreement; or (3) combine the Personal Information that Xurrent receives from, or on behalf of, Customer with other Personal Information that it receives from, or on behalf of, another customer, or collects from its own interaction with California residents, expect as otherwise permitted by the CCPA.

3. Xurrent permits Customer to monitor its compliance with this CCPA Addendum subject to Section 11 in the Addendum "Audit Rights".

4. Xurrent agrees to notify the Customer if Xurrent makes a determination that it can no longer meet its obligations under this Addendum or CCPA requirements.

5. Xurrent shall assist Customer in respect of a consumer request to limit the use of Sensitive Personal Information ("**SPI**"), Xurrent shall provide assistance and procure that its subcontractors will provide assistance as Customer may request, where applicable, in connection with any obligation by Customer to respond to requests for exercising the rights of a consumer under the CCPA. Xurrent shall (a) promptly notify Customer; (b) only act upon the consumer's request with the prior written consent of the Customer; and (c) make available to Customer all needed information which is necessary to demonstrate compliance.

6. Xurrent acknowledges and confirms that it does not receive or process any Personal Information as consideration for the Service or other items that Xurrent provides to Customer under the Agreement.

7. Xurrent certifies that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from selling (as such term is defined in the CCPA) any Personal Information.