



DATA PROCESSING ADDENDUM

This Data Processing Addendum (“DPA”) forms part of the applicable subscription and services agreement (the “Agreement”), entered into by and between the Customer named below and Xactly Corporation (“Xactly”), pursuant to which Customer has purchased subscriptions to Xactly’s application services (“Services”). The purpose of this DPA is to reflect the parties’ agreement with regard to the Processing of Personal Data, in accordance with the requirements of Data Protection Laws and Regulations. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

HOW TO EXECUTE THIS DPA:

A. This DPA consists of two parts: the main body of the DPA, and the Standard Contractual Clauses in Attachment 1 (including Appendices 1 and 2). The DPA and the Standard Contractual Clauses have been pre-signed on behalf of Xactly.

B. To complete this DPA, Customer must:

1. Complete the information in the signature box and sign on Page 6.
2. Complete the information regarding the data exporter on Page 7 and 14.
3. Complete the information in the signature box and sign on Page 13 and 15.
4. Submit the completed and signed DPA, without changes to any printed terms, to Xactly at the following email address: legalcontracts@xactlycorp.com. Upon receipt of the validly completed DPA at the above email address, this DPA will become legally binding.

HOW THIS DPA APPLIES

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement.

If the Customer entity signing this DPA has entered into an order form or statement of work with Xactly pursuant to the Agreement (an “Ordering Document”), but is not itself a party to the Agreement, this DPA is an addendum to that Ordering Document and applicable renewal Ordering Documents.

If the Customer entity signing this DPA is neither a party to an Ordering Document nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity that is a party to the Agreement executes this DPA, and Affiliates of such Customer entity will benefit under this DPA via Section 9.1.2 below.

DATA PROCESSING TERMS

For the duration of the Agreement and in the course of providing the Services to Customer pursuant to the Agreement, Xactly may Process Personal Data on behalf of Customer. Xactly and Customer each agree to comply with the following provisions with respect to any Personal Data submitted by or for Customer to the Services or collected and Processed by or for Customer through the Services.

1. DEFINITIONS

“CCPA” means the California Consumer Privacy Act.

“Data Controller” means the entity that determines the purposes and means of the Processing of Personal Data.

“Data Processor” means the entity that Processes Personal Data on behalf of the Data Controller.



“Data Protection Laws and Regulations” means all local, state, national and/or foreign law, treaties, and/or regulations, including the CCPA, the laws and regulations of the European Union, the European Economic Area and their member states, and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR, applicable to either (i) Xactly in its role as service provider Processing data under the Agreement or (ii) Customer and its Affiliates, as the case may be. For the avoidance of doubt, each party is only responsible for the local, state, national and/or foreign law, treaties, and/or regulations applicable to it. As an example for illustrative purposes, Xactly is responsible for complying with local, state, national and/or foreign law, treaties, and/or regulations applicable to Xactly but not those laws applicable to Customer or its Affiliates.

“Data Subject” means the individual to whom Personal Data relates.

“GDPR” means EU General Data Protection Regulation 2016/679.

“Personal Data” means any information relating to an identified or identifiable person that has been provided by or for Customer to the Services or collected and Processed by or for Customer through the Services as well as information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer, household, or device, or as otherwise defined under applicable law, whichever is more restrictive.

“Processing” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

“Standard Contractual Clauses” means the agreement pursuant to the European Commission’s decision of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, executed by and between Customer and Xactly and attached hereto as Attachment 1.

“Sub-processor” means any Data Processor engaged by Xactly to process Personal Data under the Agreement and/or this DPA.

“Supervisory Authority” means an independent public authority which is established by a member state pursuant to Article 51 of the GDPR.

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer and/or its Affiliates is the Data Controller, Xactly is a Data Processor and that Xactly will engage Sub-processors pursuant to the requirements set forth in Section 5 “Sub-processors” below.

2.2 Customer’s Processing of Personal Data. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer’s instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer shall ensure that the Customer is entitled to transfer the relevant Personal Data to Xactly so that Xactly and its Sub-processors may lawfully use, process and transfer the Personal Data in accordance with this DPA and the Agreement on Customer’s and its Affiliates’ behalf.

2.3 Instructions. This DPA (including the Standard Contractual Clauses) and the Agreement are Customer’s complete and final instructions to Xactly for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. Xactly undertakes to document in writing any such further instruction given by Customer.



2.4 Xactly's Processing of Personal Data. Xactly shall only Process the Personal Data specified in Appendix 1 to the Standard Contractual Clauses. Xactly shall Process Personal Data on behalf of and in accordance with Customer's instructions and shall treat Personal Data as Confidential Information. Customer instructs Xactly to Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and applicable Ordering Document, which includes updating the Services and preventing or addressing service or technical issues; (ii) Processing initiated by Customer's Subscribers in their use of the Services; and (iii) Processing to comply with other reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

3. RIGHTS OF DATA SUBJECTS

3.1 Assistance. Taking into account the nature of the processing, Xactly assists the Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter 3 (Art. 12-23) of the GDPR;

3.2 Correction, Blocking and Deletion. To the extent Customer, in its use of the Services, does not have the ability to correct, amend, block or delete Personal Data, as required by Data Protection Laws and Regulations, Xactly shall comply with any commercially reasonable request by Customer to facilitate such actions to the extent Xactly is legally permitted to do so. To the extent legally permitted, Customer shall be responsible for any costs arising from Xactly's provision of such assistance.

3.3 Data Subject Requests. Xactly shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for access to, correction, amendment or deletion of that person's Personal Data. Xactly shall not respond to any such Data Subject request without Customer's prior written consent except to confirm that the request relates to Customer. Xactly shall provide Customer with commercially reasonable cooperation and assistance in relation to handling of a Data Subject's request for access to that person's Personal Data, to the extent legally permitted and to the extent Customer does not have access to such Personal Data through its use of the Services. If legally permitted, Customer shall be responsible for any costs arising from Xactly's provision of such assistance.

4. XACTLY PERSONNEL

4.1 Confidentiality. Xactly shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Xactly shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2 Reliability. Xactly shall take commercially reasonable steps to ensure the reliability of any Xactly personnel engaged in the Processing of Personal Data.

4.3 Limitation of Access. Xactly shall ensure that Xactly's access to Personal Data is limited to those personnel who require such access to perform the Agreement.

5. SUB-PROCESSORS AND TRANSFERS OF PERSONAL DATA

5.1 Appointment of Sub-processors. Customer acknowledges and agrees that Xactly's Affiliates may be retained as Sub-processors, and Xactly and Xactly's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services, in each case (a) anywhere in the world where Xactly, its Affiliates or its or their Sub-processors maintain data processing operations, and (b) subject to a written agreement requiring the Sub-processor to comply with the requirements of applicable Data Protection Laws and Regulations and to abide by terms no less protective of the Personal Data than those provided in this DPA to the extent applicable to the nature of the services provided by such Sub-processor. For transfers of Personal Data under this DPA from the European Economic Area and Switzerland to countries that do not ensure an adequate level of data protection within the meaning of applicable Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such applicable Data Protection Laws and Regulations, the Standard Contractual Clauses set forth in Attachment 1



and this DPA will apply, together with this Section 5. Xactly shall be liable for the acts and omissions of its Sub-processors to the same extent Xactly would be liable if performing the services of each Sub-processor directly under the terms of this DPA and the Agreement.

5.2 Notification of New Sub-processors. Xactly's current list of Sub-processors for the applicable Services is available at <https://trust.xactlycorp.com/privacy-policy/> ("Sub-processor List"). Customer may subscribe to updates to the relevant Sub-processor List and shall provide such updates at least thirty (30) days prior to authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the Services.

5.3 Objection Right for New Sub-processors. This Section 5.3 shall apply only where and to the extent Customer is established with the European Economic Area or Switzerland or where otherwise required by Data Protection Laws and Regulations applicable to Customer. If Customer has a reasonable basis to object to Xactly's use of a new Sub-processor, Customer shall notify Xactly in writing within 10 business days after receipt of Xactly's notice. In the event Customer objects to a new Sub-processor(s) on reasonable grounds, and Xactly chooses to retain the objected-to new Sub-processor, Xactly will notify the Customer in writing and Customer may terminate the applicable Ordering Document(s) in respect only to those Services which cannot be provided by Xactly without the use of the objected-to new Sub-processor, by providing written notice to Xactly, and Customer shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated Services.

6. SECURITY

6.1 Controls for the Protection of Personal Data. Xactly shall maintain a comprehensive information security program that includes administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Personal Data that are appropriate to (a) the size, scope and type of Xactly's business; (b) the amount of resources available to Xactly; (c) the type of information that Xactly will store; and (d) the need for security and confidentiality of such information. Xactly shall regularly monitor compliance with these safeguards. At a minimum, Xactly will implement and maintain the technical and organizational measures as set forth by Appendix 2 of the Standard Contractual Clauses.

6.2 Third-Party Audits. At least once per year during the term of the Agreement, Xactly shall have an audit of its operations performed by an independent auditing firm. This audit will include an evaluation that tests and validates key controls relating to the security of Personal Data at each site (currently a SSAE 18 report ("Security Report")). Upon request, and subject to the Confidentiality provisions of the Agreement, Xactly shall make a copy of the then-current Security Report available to Customer for evaluation.

7. SECURITY BREACH MANAGEMENT AND NOTIFICATION

Xactly maintains security incident management policies and procedures and shall, to the extent permitted by law, promptly notify Customer's designated contact as set forth by Customer in the signature block below, of any actual or reasonably suspected unauthorized disclosure of Personal Data by Xactly or its Sub-processors of which Xactly becomes aware (a "Security Breach"). To the extent such Security Breach is caused by a violation of the requirements of this DPA by Xactly, Xactly shall make reasonable efforts to identify and remediate the cause of such Security Breach.

In addition, as of 25 May 2018, GDPR provides for additional requirements for Personal Data breach notification. Xactly shall notify the Data Controller without undue delay but in any event within 72 hours after becoming aware of a Personal Data breach, and Xactly will assist the Data Controller in accordance with Art. 28 paragraph 3 of GDPR with the compliance of its reporting obligations, including by providing at least the following information:

- a) a description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;



- b) the name and contact details of the data protection officer or other contact point where more information can be obtained;
- c) a description of the likely consequences of the personal data breach;
- d) a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

8. RETURN AND DELETION OF PERSONAL DATA

Xactly shall make Personal Data available for export by Customer upon request made within thirty (30) days of the date of termination/expiration of the Agreement. Within one hundred twenty (120) days after the termination/expiration of the Agreement, Xactly shall securely destroy all Personal Data in its possession or control.

9. ADDITIONAL TERMS FOR EU PERSONAL DATA

9.1 Application of Standard Contractual Clauses. The Standard Contractual Clauses in Attachment 1 and the additional terms in this Section 9 will apply to the Processing of Personal Data by Xactly in the course of providing the Services:

9.1.1 The Standard Contractual Clauses apply only to Personal Data that is transferred from the European Economic Area (EEA) to outside the EEA, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Directive), and (ii) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for personal data, including but not limited to Binding Corporate Rules for Processors.

9.1.2 The Standard Contractual Clauses apply to (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all Affiliates of Customer established within the European Economic Area (EEA) and Switzerland that have purchased Services on the basis of an Ordering Document. For the purpose of the Standard Contractual Clauses and this Section 9, the aforementioned entities shall be deemed “Data Exporters”.

9.2 Objective and Duration. The objective of Processing of Personal Data by Xactly is the performance of the Services pursuant to the Agreement during the term of the Agreement.

9.3 Sub-processors. Pursuant to Clause 5(h) of the Standard Contractual Clauses, the Data Exporter acknowledges and expressly agrees that Xactly’s Affiliates may be retained as Sub-processors; and (b) Xactly and Xactly’s Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. The parties agree that the copies of the Sub-processor agreements that must be sent by the Data Importer to the Data Exporter pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by the Data Importer beforehand, and that such copies will be provided by Data Importer only upon reasonable request by Data Exporter.

9.4 Audits. The parties agree that the audits described in Clause 5(f), Clause 11 and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications: Upon Data Exporter’s request, and subject to the confidentiality obligations set forth in the Agreement or otherwise agreed by the parties, Data Importer shall make available to Data Exporter (or Data Exporter’s independent, third-party auditor that is not a competitor of Xactly (“Data Exporter’s Auditor”)) information regarding Xactly’s compliance with the obligations set forth in this DPA, and shall allow for and contribute to audits and inspections, by Data Exporter or Data Exporter’s Auditor. The foregoing requirements may be satisfied by provision of Xactly’s most recent annual Security Report. In the event a supervisory authority requests access to Xactly’s data processing facilities pursuant to Clause 12(2), Customer shall reimburse Data Importer for any time expended for any such on-site audit at Xactly’s then-current professional services rates, which shall be made available to Data Exporter upon request. Before the commencement of any such on-site audit, Data Exporter and Data Importer shall mutually agree upon the scope, timing, and duration



of the audit in addition to the reimbursement rate for which Data Exporter shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Data Importer. Data Exporter shall promptly notify Data Importer with information regarding any non-compliance discovered during the course of an audit.

9.5 Certification of Deletion. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) shall be provided by the Data Importer to the Data Exporter only upon Data Exporter's request.


9.6 Data Protection Impact Assessment and Prior Consultation. Data Importer shall provide reasonable assistance to Data Exporter with any data protection impact assessments, and prior consultations with any Supervisory Authority or other competent data privacy authorities, which Data Exporter reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Laws and Regulations, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, the Data Importer.

9.7 Conflict. In the event of any conflict or inconsistency between the GDPR, this DPA and the Standard Contractual Clauses in Attachment 1, the conflict or inconsistency shall be resolved by giving precedence in the following order: (i) the terms of the GDPR; (ii) the Standard Contractual Clauses; and (iii) this DPA.

10. LEGAL EFFECT

This DPA shall only become legally binding between the eligible Customer and Xactly when each of the steps set out in the Section "HOW TO EXECUTE THIS DPA" above have been fully completed. The terms of this DPA will end simultaneously and automatically with the termination of the Agreement, provided however any obligation imposed on Xactly under this DPA in relation to the Processing of Personal Data shall survive any termination or expiration of the Agreement. This DPA is part of and subject to the terms of the Agreement. Customer's remedies (including those of its Affiliates) with respect to any breach by Xactly of the terms of this Agreement will be subject to any aggregate limitation of liability that applies to the Customer under the Agreement. With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and the Agreement, the provisions of this DPA shall prevail with regard to the parties' data protection obligations.

IN WITNESS WHEREOF, the parties' authorized signatories have duly executed this Agreement:

CUSTOMER:	XACTLY CORPORATION
By:	By: 
Name:	Name: Ron Rasmussen <small>4768860669E444...</small>
Title:	Title: Chief Technology Officer
Date:	Date: 11/27/2019
Customer's Email Contact (for breach notifications):	

Attachment 1
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection,

Name of the data exporting organisation:

Address:

Tel.:

E-mail:

Other information needed to identify the organisation:

(the data exporter)

And

Name of the data importing organisation: Xactly Corporation

Address: 505 S. Market Street, San Jose, CA 95113, USA

Tel.: +1 (408) 977-3132

E-mail:

Other information needed to identify the organisation: None

(the data importer)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

- (a) ‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘supervisory authority’ shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data();
- (b) ‘the data exporter’ means the controller who transfers the personal data;
- (c) ‘the data importer’ means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) ‘the sub-processor’ means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data

exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) ‘the applicable data protection law’ means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) ‘technical and organisational security measures’ means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter’s behalf and in accordance with the applicable data protection law and the Clauses;

- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
 - (ii) any accidental or unauthorised access; and

- (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so:
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent

and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature _____

(stamp of organisation)


On behalf of the data importer: Xactly Corporation

Name (written out in full): Ron Rasmussen

Position: Chief Technology Officer

Address: 505 S. Market Street, San Jose, CA 95113

Other information necessary in order for the contract to be binding (if any): None

Signature  _____
17C2860CF69E444...

(stamp of organisation)

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data Exporter

The Data Exporter is (please specify briefly your activities relevant to the transfer):

Data Exporter is _____ and its Affiliates (as defined in the Agreement) established within the European Economic Area (EEA) and Switzerland that have purchased Services pursuant to one or more Ordering Documents.

Data Importer

The data importer is (please specify briefly activities relevant to the transfer):

The Data Importer is Xactly Corporation, a provider of hosted incentive compensation, performance management and territory optimization software applications, which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

Data Subjects

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

Data exporter's employees, agents, advisors, and contractors who are natural persons, and data exporter's users authorized by data exporter to use the Services

Categories of data

The personal data transferred concern the following categories of data (please specify):

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

Names and contact details, e-mail and telephone details, job title, unit/department, location, supervisor(s) and subordinate(s), employee identification number, employment status and type, compensation information, including bonus and sales commission eligibility, quotas, commission rates and on target earnings, objectives, coaching and job performance information.

Special categories of data (if appropriate):

The personal data transferred concern the following special categories of data (please specify):

- None

Purposes of the transfer / Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The objective of Processing of Personal Data by data importer is the performance of the Services pursuant to the Agreement. Data importer shall only Process Personal Data in accordance with the instructions as set out by section 2.4 of the DPA.

DATA EXPORTER

Name:

Authorised Signature

DATA IMPORTER: Xactly Corporation

Name: Ron Rasmussen

Authorised Signature

DocuSigned by:
Ron Rasmussen
17C2860CF69E444...

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data Importer maintains and enforces various policies, standards and processes designed to secure personal data and other data to which Data Importer employees are provided access, and updates such policies, standards and processes from time to time consistent with industry standards. Following is a description of some of the core technical and organisational security measures implemented by Data Importer as of the date of signature:

1. General Security Procedures

1.1 Data Importer shall be responsible for establishing and maintaining an information security program that is designed to: (i) protect the security and confidentiality of Personal Data; (ii) protect against anticipated threats or hazards to the security or integrity of the Personal Data; (iii) protect against unauthorized access to or use of the Personal Data; (iv) ensure the proper disposal of Personal Data, as further defined herein; and, (v) ensure that all employees and subcontractors of Data Importer, if any, comply with all of the foregoing. Data Importer shall designate an individual to be responsible for the information security program. Such individual shall respond to Data Exporter inquiries regarding computer security and to be responsible for notifying Data Exporter-designated contact(s) if a breach or an incident occurs, as further described herein.

1.2 Data Importer shall conduct formal privacy and security awareness training for all personnel and contractors as soon as reasonably practicable after the time of hiring and/or prior to being appointed to work on Personal Data and annually recertified thereafter. Documentation of security awareness training shall be retained by Data Importer, confirming that this training and subsequent annual recertification process have been completed.

1.3 Data Exporter shall have the right to review an overview of Data Importer's information security program prior to the commencement of Service and annually thereafter upon Data Exporter request.

1.4 In the event of any apparent or actual theft, unauthorized use or disclosure of any Personal Data, Data Importer shall immediately commence all reasonable efforts to investigate and correct the causes and remediate the results thereof, and within one (1) business day following confirmation of any such event, provide Data Exporter notice thereof, and such further information and assistance as may be reasonably requested. Upon Data Exporter request, remediation actions and reasonable assurance of resolution of discovered issues shall be provided to Data Exporter.

1.5 Data Importer shall not transmit any unencrypted Personal Data over the internet or any unsecured network, and shall not store any Personal Data on any mobile computing device, such as a laptop computer, USB drive or portable data device, except where there is a business necessity and then only if the mobile computing device is protected by industry-standard encryption software. Data Importer shall encrypt Personal Data in transit into and out of the Services over public networks using industry standard protocols.

2. Network and Communications Security

2.1 All Data Importer connectivity to Data Exporter computing systems and/or networks and all attempts at same shall be only through Data Exporter's security gateways/firewalls and only through Data Exporter-approved security procedures.

2.2 Data Importer shall not access, and will not permit unauthorized persons or entities to access Data Exporter computing systems and/or networks without Data Exporter's express written authorization and any such actual or attempted access shall be consistent with any such authorization.

2.3 Data Importer shall take appropriate measures to ensure that Data Importer's systems connecting to Data Exporter's systems and anything provided to Data Exporter through such systems does not contain any computer code, programs, mechanisms or programming devices designed to, or that would enable, the disruption, modification, deletion, damage, deactivation, disabling, harm or otherwise be an impediment, in any manner, to the operation of Data Exporter's systems.

2.4 Data Importer shall maintain technical and organisational measures for data protection including: (i) firewalls and threat detections systems to identify malicious connection attempts, to block spam, viruses and unauthorized intrusion; (ii) physical networking technology designed to resist attacks by malicious users or malicious code; and (iii) encrypted data in transit over public networks using industry standard protocols.

3. Personal Data Handling Procedures

3.1 Disposal of Personal Data on paper shall be done in a secure manner, to include shredders or secure shredding bins within Data Importer space from which Personal Data is handled or accessed ("Data Exporter Work Area"). Shredding must take place within the Data Exporter Work Area before disposal or transit outside of the Data Exporter Work Area or be performed offsite by a reputable third party under contract with Data Importer.

3.2 Erasure of Information and Destruction of Electronic Storage Media. All electronic storage media containing Personal Data must be wiped or degaussed for physical destruction or disposal, in a manner meeting forensic industry standards such as the NIST SP800-88 Guidelines for Media Sanitization, prior to departing Data Exporter Work Area(s), with the exception of encrypted Personal Data residing on portable media for the express purpose of providing service to the Data Exporter. Data Importer shall maintain commercially reasonable documented evidence of data erasure and destruction for infrastructure level resources. This evidence must be available for review at the request of Data Exporter.

3.3 Data Importer shall maintain authorization and authentication technologies and processes to ensure that only authorized persons access Personal Data, including: (i) granting access rights on the basis of the need-to-know-principle; (ii) reviewing and maintaining records of employees who have been authorized or who can grant, alter or cancel authorized access to systems; (iii) requiring personalized, individual access accounts to use passwords that meet complexity, length and duration requirements; (iv) storing passwords in a manner that makes them undecipherable if used incorrectly or recovered in isolation; (v) encrypting, logging and auditing all access sessions to systems containing Personal Data; and (vi) instructing employees on safe administration methods when computers may be unattended such as use of password protected screen savers and session time limits.

3.4 Data Importer shall maintain logical controls to segregate Personal Data from other data, including the data of other customers.

3.5 Data Importer shall maintain measures to provide for separate processing of data for different purposes including: (i) provisioning Data Exporter within its own application-level security domain, which creates logical separation and isolation of security principles between customers; and (ii) isolating test or development environments from live or production environments.

4. Physical Security

4.1. Xactly Incent Enterprise, Xactly Objectives, Xactly Insights. The terms set forth in 4.1A, 4.1B, and 4.1C are applicable solely to Xactly Incent Enterprise, Xactly Objectives and Xactly Insights product offerings:

A. All backup and archival media containing Personal Data must be contained in secure, environmentally-controlled storage areas owned, operated, or contracted for by Data Importer. All backup and archival media containing Personal Data must be encrypted.

B. Technical and organisational measures to control access to data center premises and facilities are in place and include: (i) staffed reception desks or security officers to restrict access to identified, authorized individuals; (ii) visitor screening on arrival to verify identity; (iii) all access doors, including equipment cages, secured with automatic door locking systems with access control systems that record and retain access histories; (iv) monitoring and recording of all areas using CCTV digital camera coverage, motion detecting alarm systems and detailed surveillance and audit logs; (v) intruder alarms present on all external emergency doors with one-way internal exit doors; and (vi) segregation of shipping and receiving areas with equipment checks upon arrival.

C. Data Importer shall maintain measures to protect against accidental destruction or loss of Personal Data including: (i) fire detection and suppression, including a multi-zoned, dry-pipe, double-interlock, pre-action fire suppression system and a Very Early Smoke Detection and Alarm (VESDA); (ii) redundant on-site electricity generators with adequate supply of generator fuel and contracts with multiple fuel providers; (iii) heating, ventilation, and air conditioning (HVAC) systems that provide stable airflow, temperature and humidity, with minimum N+1 redundancy for all major equipment and N+2 redundancy for chillers and thermal energy storage; and (iv) physical systems used for the storage and transport of data utilizing fault tolerant designs with multiple levels of redundancy.

4.2. Xactly Incent Express. Customer acknowledges that the Xactly Incent Express product offering is hosted on Xactly's subprocessor's platform. The administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services are described in the Security, Privacy and Architecture Documentation applicable to Salesforce.com's platform and accessible via <http://help.salesforce.com> or otherwise made reasonably available by Xactly.

4.3. Xactly AlignStar for SalesForce. Customer acknowledges that the Xactly AlignStar for SalesForce product offering is hosted on the Amazon Web Services and Salesforce.com platforms. The administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services are described in (a) the Security, Privacy and Architecture Documentation applicable to Salesforce.com's platform and accessible via <https://trust.salesforce.com/en/security/> or otherwise made reasonably available by Xactly and (b) the documentation applicable to Amazon Web Services and accessible via <https://aws.amazon.com/security/> and <http://aws.amazon.com/security/sharing-the-security-responsibility/> or otherwise made reasonably available by Xactly.

4.4. Xactly SimplyComp, Xactly Sales Planning. Customer acknowledges that the Xactly SimplyComp and Xactly Sales Planning product offerings are hosted on the Amazon Web Services platform. The administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services are described in the Security, Privacy and Architecture Documentation applicable to Amazon Web Services and accessible via <https://aws.amazon.com/security/> and <http://aws.amazon.com/security/sharing-the-security-responsibility/> or otherwise made reasonably available by Xactly.

4.5. Xactly Inspire. Customer acknowledges that the Xactly Inspire product offering is hosted by SalesHood. The administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services shall be made reasonably available by Xactly, upon request.

4.6. Xactly Commission Expense Accounting, Obero SPM, Xactly Advanced Quota Planning. Customer acknowledges that the Xactly Commission Expense Accounting, Obero SPM and Xactly Advanced Quota Planning product offerings are hosted on the Microsoft Azure platform. The administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services are described in the Security, Privacy and Architecture Documentation applicable to Microsoft Azure and accessible via <https://www.microsoft.com/en-us/trustcenter> or otherwise made reasonably available by Xactly.

5. Security Testing

During the performance of Services under the Agreement, Data Importer shall engage, at its own expense and at least one time per year, a third party vendor (“Testing Company”) to perform penetration and vulnerability testing (“Security Tests”) with respect to Data Importer’s systems containing and/or storing Personal Data. The foregoing shall not apply to the Xactly Inspire product offering which is hosted by Saleshood.

The objective of such Security Tests shall be to identify design and/or functionality issues in applications or infrastructure of the Data Importer systems containing and/or storing Personal Data, which could expose Data Exporter’s assets to risks from malicious activities. Security Tests shall probe for weaknesses in applications, network perimeters or other infrastructure elements as well as weaknesses in process or technical countermeasures relating to the Data Importer systems containing and/or storing Personal Data that could be exploited by a malicious party.

Security Tests shall identify, at a minimum, the following security vulnerabilities: invalidated or un-sanitized input; broken or excessive access controls; broken authentication and session management; cross-site scripting (XSS) flaws; buffer overflows; injection flaws; improper error handling; insecure storage; common denial of service vulnerabilities; insecure or inconsistent configuration management; improper use of SSL/TLS; proper use of encryption; and anti-virus reliability and testing.

Within a reasonable period after the Security Test has been performed, Data Importer shall notify Data Exporter in writing of any critical security issues that were revealed during such Security Test which have not been remediated. To the extent that critical security issues were revealed during a particular Security Test, Data Importer shall subsequently engage, at its own expense, the Testing Company to perform an additional Security Test to ensure resolution of identified security issues. Results thereof shall be made available to the Data Exporter upon request.

6. Security Audit

Data Importer, and all subcontracted entities (as appropriate) shall conduct at least annually an SSAE 18 (or higher) audit covering all systems and/or facilities utilized to provide the Service (excluding any Service related to Xactly Inspire) to the Data Exporter, and will furnish to Data Exporter the results thereof promptly following Data Exporter’s written request. If, after reviewing such audit results, Data Exporter reasonably determines that security issues exist relating to the Service, Data Exporter will notify Data Importer, in writing, and Data Importer will promptly discuss and where commercially feasible, address the identified issues. Any remaining issues shall be documented, tracked and addressed at such time as agreed upon by both Data Importer and the Data Exporter.