Visier Data Privacy Addendum

Last Updated: March 11, 2025

This Visier Data Privacy Addendum ("DPA") is applicable to the Processing of Personal Data by Visier for the purpose of providing the Services under the Agreement. This DPA is made part of the Agreement. If there is any conflict between this DPA and any other part of the Agreement, this DPA will control with respect to matters within its scope. Except as set forth in this DPA, this DPA will be effective upon execution by the parties to the Agreement (the "Effective Date") and will automatically terminate upon termination of the Agreement. Should a party execute this DPA as "Customer" that is not party to the Agreement, this DPA will be void and not legally binding.

1. Definitions

1.1. "Agreement" means collectively the MSA, the Order(s), and all amendments, addendums and supplements thereto including, without limitation, this DPA, entered into by and between Visier and Customer for the provision of Services.

1.2. "Data Protection Law" means legislation protecting the right to privacy of natural persons (including consumers and households) that is applicable to the Processing of Personal Data under the Agreement.

1.3. "Data Subject" means the identified or identifiable person who is the subject of Personal Data.

1.4. "EEA" means the European Economic Area and its member states.

1.5. "EEA/UK/Swiss/California Data" means any Personal Data collected about individuals located in the EEA, United Kingdom, Switzerland or California, respectively.

1.6. "MSA" means "MSA" means the Visier Master Software as a Services Agreement, including (i) all schedules and exhibits expressly referenced therein and (ii) all addendums and amendments that expressly amend or are incorporated into the MSA and are properly executed by the parties thereto (or their permitted successors).

1.7. "Personal Data" means any information that is subject to Data Protection Law and relates to an identified or identifiable natural person (Data Subject, consumer or household); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.8. "Personal Data Breach" means a Security Incident (as defined in the Safeguards Policy) leading to the accidental or unlawful destruction, loss, alteration or unauthorized disclosure of or access to Personal Data that Visier Processes in the course of providing the Services.

1.9. "Process" means (and its variants "Processes" and "Processing" similarly refer to) any operation or set of operations performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.10. "Safeguards Policy" means Visier's Customer Data Safeguards Policy available at Visier's Trust Site.

1.11. "Services" means, for the purposes of this DPA only, the SaaS Services and any professional service offerings made available by Visier to the extent that processing of Personal Data is required.

1.12. "Standard Contractual Clauses" means the standard contractual clauses for the transfer of Personal Data to third countries adopted by the European Commission, Commission Implementing Decision 2021/914 of 4 June 2021.

1.13. "Subprocessors" means (i) Visier's Affiliates; and (ii) third-party subprocessors retained by Visier in connection with the provision of the Services.

1.14. "Supervisory Authority" means a competent body in the jurisdiction charged with the enforcement of Data Protection Law.

1.15. "UK Addendum" means the UK Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office under s. 119A(1) of the Data Protection Act 2018.

1.16. All other capitalized terms used but not defined in this DPA have the meanings ascribed to them in the Agreement.

2. Roles, Scope of Processing, and Customer Instructions

2.1. Roles and Responsibilities. Customer shall determine the purposes and means of Processing with respect to Personal Data transferred to Visier in connection with the Services. Visier shall act as the processor or service provider only with respect to such Personal Data. Each party will comply with the obligations applicable to it under Data Protection Law as those obligations relate to this DPA and the Agreement.

2.2. Scope of Processing. The subject matter of the Processing is the performance of the Services. Visier's Processing will be carried out for the term of the Agreement. Schedule 1 to this DPA sets out further details about the Processing conducted by Visier. Customer can directly access and control end user access to its Personal Data stored in the Services.

2.3. Customer Instructions.

a. Visier will Process Personal Data in accordance with Customer's instructions. The Agreement and this DPA will be considered Customer's complete and final set of instructions to Visier pertaining to the Processing of Personal Data. Additional instructions outside the scope of this DPA (if any) require prior written agreement between Visier and Customer. The foregoing notwithstanding, Visier may Process the Personal Data if required under Data Protection Law, provided that Visier will first inform Customer of such required Processing unless prohibited by Data Protection Law. Both parties are responsible to store copies of all written instructions along with a copy of the Agreement and this DPA.

b. Customer will ensure that its instructions at all times comply with Data Protection Law and acknowledges that Visier is not responsible to determine: (i) which laws or regulations are applicable to Customer's business; (ii) whether Visier's Processing of Personal Data will meet the requirements of such laws; or (iii) whether Customer's instruction(s) comply with applicable law. Visier will inform Customer if it becomes aware or reasonably believes that Customer's instructions infringe Data Protection Law.

3. Processing of Personal Data

3.1. Visier will maintain technical and organizational measures designed for the protection of the security, confidentiality and integrity of the Personal Data, as set forth in the Safeguards Policy. These measures take into account the state of the art, the costs of implementation and the nature, scope, context and purpose of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons and demonstrates Visier's implementation of appropriate technical and organizational measures. In addition, these measures take into account the sensitivity of the Personal Data in respect of the harm to the Data Subject that might result from unauthorized or unlawful Processing, loss, destruction of, or damage to, the Personal Data, including, but not limited to measures designed to:

a. prevent the use of Personal Data for any purpose other than Processing in accordance with the Agreement and this DPA or as otherwise instructed by Customer;

b. prevent the disclosure of Personal Data to third parties except to the extent permitted under the Agreement and this DPA, or as otherwise instructed by Customer, or in compliance with a legal obligation to disclose;

c. prevent unauthorized access, duplication, modification and/or deletion of Personal Data during electronic transmission and storage;

d. limit access to Personal Data to personnel who are trained in data protection and confidentiality requirements and bound to uphold Visier's data protection and confidentiality obligations;

e. limit access to Personal Data on a "need to know" basis and ensuring that all such persons to whom Visier discloses the Personal Data are aware of and compliant with these obligations; and

f. logically separate Personal Data from the Personal Data of Visier's other customers.

3.2. Visier has appointed a data protection officer who is responsible for overseeing the management of data protection within Visier.

3.3. Except as otherwise permitted or required under Data Protection Law, Visier will not: (a) retain, use or disclose Personal Data for any purpose other than providing the Services specified in the Agreement or as otherwise permitted or required by the Agreement; nor (b) retain, use, or disclose Personal Data except where permitted under the Agreement.

3.4. Upon request, Visier will assist Customer as reasonably necessary for Customer to meet its obligations to the competent Supervisory Authority in connection with the Processing of Personal Data hereunder. Additional Customer requests that fall outside the scope of such reasonable assistance will require the prior written agreement of Visier and Customer, including agreement on any additional fees related to such requests.

3.5. Taking into account the nature of the Processing, Visier will assist Customer by appropriate technical and organizational measures, insofar as this is possible, in fulfilment of Customer's obligations to respond to the requests of Data Subjects to exercise their rights under Data Protection Law. Visier will promptly forward to Customer the request of a Data Subject where the Data Subject applies directly to Visier to exercise such rights.

3.6. Schedule 1 hereto describes the Personal Data and its Processing via the Services.

4. Conflicts of Law

4.1. The parties will promptly inform each other and cooperate in good faith to find a mutually agreeable resolution, which may include additions or modifications to this DPA or the Agreement executed in writing by the duly authorized representatives of both parties, in the event that a change in Data Protection Law, or ruling, finding, or decision of a competent judicial body or Supervisory Authority:

a. prevents either of the parties from performing their obligations under this DPA in compliance with Data Protection Law;

b. means that the Processing of any Personal Data by Visier is no longer compliant with Data Protection Law; and/or

c. requires further actions to be carried out or documents to be executed by either party in order to comply with Data Protection Law.

5. Notifications

In the event of a Personal Data Breach, Visier will notify Customer without undue delay and within twenty-four hours in accordance with the Safeguards Policy. Visier will provide commercially reasonable cooperation to assist Customer in Customer's obligations under Data Protection Law respecting notifications in the event of a Personal Data Breach by making available to Customer such information about a Personal Data Breach as Visier can disclose, taking into account the nature of the Services, the information available to Visier, and any restrictions on disclosing the information, such as obligations of confidentiality.

6. Audit

6.1. Customer hereby directs Visier to audit its technical and organizational measures described in this DPA at least annually by retaining qualified independent third party auditors at Visier's selection and expense and to produce an audit report detailing its findings in the form of a SOC2 Type II (or equivalent) audit report (the "Audit Report").

6.2. Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, Visier will make available to Customer the Audit Report so that Customer can reasonably verify Visier's compliance with its obligations under this DPA. The Audit Report forms part of Visier's Confidential Information in accordance with the confidentiality provisions of the Agreement.

6.3. Where Customer is required by Data Protection Law to verify compliance under this DPA by means other than Customer's instructions in Section 6.1 and subsequent to a review of the Audit Report, Customer may conduct, no more than once per year (unless otherwise mandated by Data Protection Law), an audit of the architecture and procedures relevant to the protection of Personal Data. Such audit will be conducted at Customer's expense by Customer or Customer's independent, third-party auditor reasonably acceptable to Visier that executes a nondisclosure agreement acceptable to Visier prior to any audit, in accordance with

Visier's then-available audit timetable. Customer acknowledges and agrees that: (a) Visier will only provide existing documents as evidence in support of the audit; (b) the audit cannot interfere with individual rights and data protection requirements under Data Protection Law; and (c) if interviews are required, Visier will have sole discretion to select its personnel to be interviewed. Customer shall schedule each audit with Visier at least ninety (90) days in advance unless a shorter period is required by Data Protection Law, or mandated by an applicable Supervisory Authority, in which event the parties will adhere to the shorter period. Before the commencement of any audit, Customer and Visier shall mutually agree upon the scope, timing, and duration of the audit in addition to the fees to be paid by Customer. Customer shall promptly provide Visier with information regarding any non-compliance discovered during an audit. If Visier and Customer, after making good faith efforts, are unable to agree upon the scope, timing, and duration of the audit and the fees to be paid by Customer, then Customer may terminate this DPA and the Agreement upon thirty (30) days' prior written notice to Visier.

6.4. The information available to Customer or any person acting on Customer's behalf by operation of this Section 6: (a) is intended to allow Customer to assess Visier's compliance with those processor obligations required under Data Protection Law, including audits and inspections, and to comply with Customer's obligations in respect of data protection impact assessments and prior consultation mandated by Data Protection Law; and (b) shall be considered Visier Confidential Information in accordance with the confidentiality provisions of the Agreement.

7. Authorized and Compelled Disclosure

Visier may disclose Personal Data to its security auditors to the extent necessary to support the security-related investigations and audits described in this DPA, provided that such security auditors are bound to confidentiality and security obligations consistent with those required by this DPA and the Agreement. Visier may also disclose Personal Data to the extent necessary to comply with a legal obligation to disclose, provided that, Visier will first, if legally permissible, provide Customer with notice of such pending disclosure so that Customer may seek to contest or limit such disclosure.

8. Customer Affiliates

Customer acknowledges and agrees that it is entering into this DPA to enable the provision of the Services by Visier as set forth under the Agreement. Customer shall be responsible to direct, make, and receive all communications on behalf of its Affiliates. Visier and Affiliates will not engage in direct communication unless Customer is prohibited by Data Protection Law from communicating on Affiliate's behalf. Save where prohibited by Data Protection Law, Customer shall have the sole entitlement to exercise any right or seek any remedy on behalf of its Affiliates.

9. Data Transfer Adequacy Mechanisms

9.1. Customer acknowledges and agrees that Visier may Process Personal Data, including by using Subprocessors, in accordance with this DPA outside of the country in which Customer is located, as permitted by Data Protection Law. Where Visier's Processing of EEA/UK/Swiss Data is to take place in a third country outside of the EEA, United Kingdom or Switzerland, Visier makes available the following transfer mechanisms, presented in order of precedence:

a. transfer to a third country deemed by the European Commission or its UK or Swiss equivalent (or competent authority) to have an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data; and

b. the Standard Contractual Clauses as the same may apply to EEA, UK or Swiss Data as set out in this Section 9.

9.2. For transfers of EEA Data, Module 2 (Controller to Processor) of the Standard Contractual Clauses are hereby signed, dated, and entered into (and incorporated into this DPA by this reference) by and between Visier and Customer as of the date of this DPA. The parties agree that the Standard Contractual Clauses are completed as follows:

a. optional clauses not expressly identified in this Section 9.2 of the DPA as accepted by the parties are not included;

b. the parties agree that for purposes of Clause 9 of the Standard Contractual Clauses, Option 2 (General Written Authorisation) will apply and the process for provisioning new Subprocessors, including the

notification process, will be as described in Section 10 of this DPA and Customer's acceptance of any Subprocessor pursuant to Section 10 of this DPA will constitute an instruction that Visier may transfer Personal Data to such Subprocessor;

c. the parties agree that any audits permitted under the Standard Contractual Clauses shall be carried out in accordance with Section 6 of this DPA;

d. Visier will return and/or erase Personal Data pursuant to Clause 8.5 of the Standard Contractual Clauses as set forth in Section 11 of this DPA;

e. for the purposes of Clause 13 of the Standard Contractual Clauses, the Supervisory Authority with responsibility for ensuring compliance by Customer with Data Protection Law will be: (i) where Customer is established in an EU Member State, the supervisory authority in the Member State in which Customer is established; (ii) where Customer is not established in an EU Member State, but falls within the territorial scope of application Data Protection Law and has appointed a representative in an EU Member State, the Supervisory Authority of the Member State in which the representative is located; and (iii) where Customer is not established in an EU Member State, but falls within the scope of Data Protection Law without however having to appoint a representative the Supervisory Authority of one of the Member States in which the Data Subjects whose Personal Data is transferred by Customer under the Standard Contractual Clauses are located;

f. for the purposes of Clauses 17 and 18 of the Standard Contractual Clauses, the parties agree that the Standard Contractual Clauses shall be governed by the law of the EU Member State in which Customer is established, and that any dispute arising from the Standard Contractual Clauses shall be resolved by the courts of the EU Member State in which Customer is established;

g. for the purposes of Annex I.A:

   i. Visier will be deemed the 'data importer' (in the role of data processor) and Customer will be deemed the 'data exporter' (in the role of data controller);

   ii. the "contact person" for each party will be deemed to be the person(s) entitled to receive legal notices under the Agreement; and

   iii. the "activities relevant to the data transferred under" the Standard Contractual Clauses are as follows: (1) Customer transfers Personal Data in accordance with the Agreement to Visier to receive the Services, and (2) Visier Processes Personal Data in accordance with the Agreement to provide the Services;

h. for the purposes of Annex I.B, the information set out in Schedule 1 of this DPA is deemed to complete the descriptions of transfer;

i. for the purposes of Annex II, the technical and organizational measures set out in Schedule 2 of this DPA are deemed to complete the technical and organizational security measures; and

j. in the event of a conflict between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

9.3. For transfers of UK Data, the parties agree that the Standard Contractual Clauses will be completed as set out in Schedule 3 of this DPA.

9.4. For transfers of Swiss Data, the parties agree that the Standard Contractual Clauses will be completed as set out in Schedule 3 of this DPA.

9.5. The parties may from time to time agree to other mechanisms for the transfer of EEA/UK/Swiss Data so long as such mechanism remains lawful in accordance with the law of the European Union, the United Kingdom or Switzerland, as applicable. If the mechanism used by the parties for transfers of EEA/UK/Swiss Data should become invalid, the parties will promptly put in place an alternative mechanism for the transfer of EEA/UK/Swiss Data. Customer is responsible for restricting access by its Authorized Users to Personal Data contained in the Services based on geographical location of the user. Accordingly, nothing in the Agreement or this DPA shall be interpreted as creating an obligation on Visier to ascertain the geographic location of any Authorized User or to restrict access to the Services by Customer's Authorized Users based on geographical location.

9.6. For transfers of California Data, the parties agree that the terms set out in Part C of Schedule 3 of this DPA shall apply.

10. Subprocessing

10.1. Customer provides its general authorization for Visier to engage Subprocessors in connection with the provision of the Services. Visier will ensure that: (a) Subprocessors are engaged by Visier solely for the purpose of providing the Services; (b) Subprocessors are bound to data protection obligations that meet the requirements of Data Protection Law, this DPA and the Agreement; (c) a vendor management program is maintained to assess and validate each Subprocessor's capability to meet the data protection obligations of Data Protection Law, this DPA and the Agreement; and (d) if any Subprocessor fails to fulfill its obligations, Visier will remain liable to Customer for such failure as if it were Visier's own.

10.2. Customers may opt in to receive Subprocessor notifications by completing Visier's online subscription form. Contact information provided therein will be used only for the purposes of sending subprocessor notifications. Once subscribed to such notifications, Visier will provide reasonable notice to Customer prior to authorizing any new Subprocessor. Notices will specify Customer's period to object to the authorization of such new Subprocessor and the process for such objection. The parties will work together in good faith to validate and address Customer's objections, if any.

10.3. Visier maintains its current list of Subprocessors at Visier's Trust Site which list may be updated from time to time by Visier in accordance with this Section 10.

11. Deletion of Personal Data.

Upon expiration or termination of the Agreement, Customer instructs Visier to delete all Personal Data within thirty (30) days of such expiration or termination in accordance with the provisions of the Agreement. Backups may be retained by Visier for up to ninety (90) days after the term of the Agreement and thereafter are automatically deleted and/or destroyed in accordance with the Agreement.

12. Remediation

If Visier determines that it can no longer meet one or more of its obligations under this DPA, Visier will promptly notify Customer and take reasonable and appropriate steps to cease Processing the Personal Data and remediate any unauthorized Processing as soon as practicable. If Visier notifies Customer that it will not be able to remediate within a reasonable period of time, Customer may terminate the Agreement or suspend Visier's continued Processing of Personal Data, without penalty, immediately upon written notice to Visier.

13. Limitation of Liability

The liability of a party under this DPA will be subject to the exclusions and limitations of liability set out in the MSA. Any liability to an Affiliate shall be assessed in aggregate for all claims with a party and not apply on an individual or several basis.

14. Construction and Execution

14.1. If a court or other body of competent jurisdiction declares any term of this DPA invalid or unenforceable, then the remaining terms shall continue in full force and effect. The headings in this DPA are for reference purposes only and shall not affect the meaning or construction of the terms and conditions.

14.2. This DPA may be executed by the parties in separate counterparts, each of which when so executed and delivered shall be deemed an original and all such counterparts shall together constitute one and the same agreement.

14.3. This DPA shall survive termination or expiration of the Agreement for a period of thirty (30) days, or for so long as Visier is required to or retains Personal Data in accordance with Data Protection Law, the Agreement and this DPA.

[*Signature Pages Follow*]

Visier and Customer have caused this DPA to be signed by their duly authorized representatives.

CUSTOMER:	VISIER:
	DocuSigned by: Ryan Wong F02C79982DF14FC...
Signature	Signature
	Ryan Wong
Print Name	Print Name
	CEO
Title	Title
	2025-Mar-11
Date	Date
	Visier, Inc.
Company Name	Company Name
	548 Market Street, #62284, San Francisco, CA 94104 USA
Mailing Address	Mailing Address

SCHEDULE 1

Description of Personal Data and Processing

List of Parties

Data exporter(s):

- Name: the Customer entity identified in the Agreement or an applicable Order between the parties
- Address: the Customer's address specified on an applicable Order
- Contact person's name, position and contact details: the Customer's contact specified in the Agreement or on an applicable Order
- Activities relevant to the data transferred under the Standard Contractual Clauses: the data exporter is customer of the data importer and utilizing the data importer's services as described in more detail in the Agreement
- Role (controller/processor): controller

Data importer:

- Name: Visier, Inc.
- Address: 548 Market Street, #62284, San Francisco, CA 94104-5401
- Contact person's name, position and contact details: Visier's contact specified in the Agreement
- Activities relevant to the data transferred under the Standard Contractual Clauses: the data exporter is customer of the data importer and utilizing the data importer's services as described in more detail in the Agreement
- Role (controller/processor): processor

Data Subject Categories

Unless otherwise provided by Customer, the categories of data subjects are Authorized Users, current and former employees, independent contractors, and job applicants of Customer and, if desired by Customer, its affiliated or related entities.

Personal Data Categories Processed and Transferred

Customer, in its sole discretion and control, is responsible for determining the Personal Data elements provided to Visier for Processing by the Services, which may include sensitive data, transferred at a frequency to be determined by the Customer.

Personal Data transferred to Visier may include, and Customer may submit, directly identifying, indirectly identifying, and device identifying information to the Services, the extent of which submission is determined and controlled by the Customer in its sole discretion. Examples of permissible Personal Data include:

- Full or partial name, employee ID number, birthdate, age, and employee photo.
- Work location, including region, country, state or province, city, site, and zip or postal code.
- Home location, including region, country, state or province, city, and zip code or postal code.
- Employment information, such as compensation, tenure, department, and completed training courses.
- Recruitment information, such as the date of application, the job applied for, and the offer date.
- Health data related to workers' compensation claims.
- Organizational Network Analysis (ONA) data.
- Employee engagement results.
- Gender, nationality, and racial or ethnic origin.
- Trade union membership.

The Services do not generally require, and Customer is discouraged from submitting, the following categories of Personal Data to the Services. Visier reserves the right to refuse the submission of any such Personal Data to the Services where Processing of such Personal Data would not align with the Services:

- National identifiers; for example, social security numbers and social insurance numbers.

- Government-issued IDs; for example, drivers' license numbers and passport numbers.
- Credit card numbers and other payment processing information.
- Bank account numbers and other financial account information.
- Any information about an individual who is under the age of 13 or such greater age as may be prohibited by data protection laws or regulations in the jurisdiction where the individual resides—in some countries, the age minimums are as high as 15.

Sensitive Data Transferred (if applicable) and Applied Safeguards

Customer may elect to transfer limited categories of sensitive Personal Data, such as health data related to workers' compensation claims; gender, nationality, and racial or ethnic origin; and trade union membership. Visier does not require Customer to submit sensitive Personal Data to the Services. If Customer elects to submit sensitive Personal Data, the Customer represents and warrants that the Customer has provided all required notices, and obtained and documented all necessary consents as are necessary to transfer such sensitive Personal Data to Visier. Visier implements technical and organisational measures to safeguard sensitive Personal Data as set forth in its Customer Data Safeguards Policy, including:

- Access restrictions for staff, limiting access to those persons who have a need to know information;
- Encrypted storage for Personal Data stored in Visier data centers;
- Keeping a record of (logging) access to Personal Data;
- Submission of Personal Data to the Services is controlled or configured by the Customer, enabling the Customer to control whether sensitive Personal Data is transferred; and
- Specialized data privacy training for all staff who are authorized to access Customer-submitted Personal Data.

Frequency of Transfers

Transfers to Visier are configured by Customer. The Services contain technical options with which Customers can configure transfers to occur on a one-off, occasional, regularly scheduled, or continuous basis.

Nature, Processing Scope and Purpose

Visier provides workforce analytics and planning solutions and Processes Personal Data only to the extent reasonably necessary for the provision of its contracted Services (including without limitation, communication to authorized users of its contracted Services, storage of Personal Data in data centers, and transmission of Personal Data between data centers and to authorized users) or otherwise in accordance with the authorized instructions of Customer (including those instructions set forth in the Agreement and this DPA).

Personal Data Storage and Retention

Personal Data is stored in encrypted disk storage areas in data centers, using multi-tenant architecture. Personal Data is retained as determined by Customer for the purpose of providing the contracted Services and deleted in accordance with Section 11 of this DPA.

Transfers to Subprocessors

For transfers to Subprocessors, the subject matter, nature, and duration of Processing are determined to the extent reasonably necessary for the provision of Visier's contracted Services, as provided for in this DPA and the Agreement, further details of which are available at Visier's Trust Site.

SCHEDULE 2

Visier Security Standards

Description of the technical and organisational security measures implemented by Visier

Visier will maintain technical and organisational security measures for protection of the security, confidentiality and integrity of the Personal Data, which consider the sensitivity of the Personal Data in respect of the harm to the data subject that might result from unauthorized or unlawful Processing, loss, destruction of, or damage to the Personal Data, as described in Section 3 of this DPA, the Agreement and the Safeguards Policy, as same may be applicable to the Processing of Personal Data in Visier's provision of the Services to Customer.

SCHEDULE 3

Standard Contractual Clauses and Jurisdiction-Specific Terms

The Standard Contractual Clauses are available at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

A. Transfers of UK Data

For transfers of UK Data, the parties agree that the UK Addendum is hereby deemed signed, dated, and entered into (and incorporated into this DPA by reference) by and between Visier and Customer as of the date of this DPA, and the Standard Contractual Clauses as completed in accordance with Section 9.2 of this DPA are hereby deemed amended as specified by the UK Addendum in respect of the transfer of such UK Data and are completed as follows:

1. for the purposes of Clause 13 of the Standard Contractual Clauses, the Supervisory Authority with responsibility for ensuring compliance by Customer with Data Protection Law will be the UK Information Commissioner;
2. for the purposes of Table 1 of the UK Addendum, the Start Date is the Effective Date of the Standard Contractual Clauses and the information set out in Schedule 1 of this DPA is deemed to complete the parties, the parties' details and the key contacts;
3. for the purposes of Table 2 of the UK Addendum, the Standard Contractual Clauses, completed as set out in Section 9.2 of this DPA, shall apply to transfers of UK Data;
4. for the purposes of Table 3 of the UK Addendum, the information set out in Schedule 1 of this DPA is deemed to complete Annexes 1A and 1B, the information set out in Schedule 2 of this DPA is deemed to complete Annex II and Option 2 (General Authorization) is deemed to complete Annex III;
5. for the purposes of Table 4 of the UK Addendum, neither party may end the UK Addendum as set out in Section 19 of Part 2 of the UK Addendum; and
6. in the event of a conflict between the UK Addendum and the Standard Contractual Clauses, the UK Addendum shall prevail.

B. Transfers of Swiss Data

For transfers of Swiss Data, the parties agree that the Standard Contractual Clauses as completed in accordance with Section 9.2 of this DPA are hereby deemed amended as specified by the Statement of the Swiss Federal Data Protection and Information Commissioner ("FDPIC") of August 27, 2021 in respect of the transfer of such Swiss Data and are completed as follows:

1. for the purposes of Clause 13 of the Standard Contractual Clauses, the Supervisory Authority with responsibility for ensuring compliance by Customer with Data Protection Law will be the FDPIC;
2. for the purposes of Clauses 17 and 18 of the Standard Contractual Clauses, the parties agree that the Standard Contractual Clauses shall be governed by the law of the EU Member State in which Customer is established, and that any dispute arising from the Standard Contractual Clauses shall be resolved by the courts of the EU Member State in which Customer is established, provided that data subjects in Switzerland may also bring legal proceedings in their place of habitual residence in Switzerland, in accordance with Clause 18(c); and
3. for the purposes of Annex I.B, the information set out in Schedule 1 of this DPA is deemed to complete the descriptions of transfer.

C. Transfers of California Data

For transfers of California Data, and only to the extent that Visier Processes Personal Data that is subject to the California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively the "CCPA"), the parties acknowledge and agree that:

1. Visier is a service provider under the CCPA;
2. the Processing of Personal Data authorized by Customer as set out in Section 2.3 of this DPA is integral to and encompassed by Visier's provision of the Services and the direct business relationship between the parties (the "Business Purpose");
3. except as otherwise permitted or required under Data Protection Law, Visier will not: (a) sell or share the Personal Data; (b) use, retain or disclose Personal Data for any purpose other than the Business Purpose; (c) retain, use or disclose the Personal Data outside of the direct business relationship between the parties; or (d) combine the Personal Data with personal information it receives from or on behalf of another person(s);
4. notwithstanding anything to the contrary in the Agreement, Visier's access to Personal Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement.
5. Visier will notify Customer if it determines that it can no longer meet its obligations under the CCPA; and
6. Customer may take reasonable and appropriate steps to ensure that Visier uses the Personal Data in a manner consistent with Visier's obligations under the CCPA. Upon notice, Customer may take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data.

Visier certifies that it understands the restrictions set out in Section 3 of this Part C and Section 3.3 of the DPA and will comply with them.