

CUSTOMER DATA PROTECTION ADDENDUM

1. Data Processing. This Data Protection Addendum (“DPA”) supplements the underlying services agreement(s) between Cintas Corporation No. 2 (“**Cintas**”) and Cintas’ Customer (“**Customer**”), as set forth in the underlying agreement (“**Agreement**”) pursuant to which Cintas provides functions for or on behalf of Customer (“**Services**”) may involve the processing of “personal information” or “personal data,” as these terms are defined under applicable US, Canadian, EU/EEA, UK, and CH data privacy and/or protections laws, provided by or collected on behalf of Customer (“**Customer Data**”). Customer and Cintas are each a “**Party**” and collectively referred to herein as the “**Parties**.” Schedules 1 and 2 to this DPA sets out certain information regarding Cintas’ Processing of Customer Data.

2. Definitions. The following definitions shall apply for purposes of interpreting this DPA. Capitalized terms used but not defined in this DPA have the meaning given to them in the Agreement or Data Protection Laws.

- a) “**Business Purposes**” means the enumerated Business Purposes set forth in Cal. Civ. Code section 1798.140(d)(1)-(7) and, on or after January 1, 2023, Cal. Civ. Code section 1798.140(e)(1)-(8) that are applicable to the Services as set forth in the Agreement, including but not limited to: performing Services on behalf of Customer, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, or providing similar services on behalf of Customer.
- b) “**Collects,**” “**collected,**” “**collection,**” “**consent,**” “**consumer,**” “**contractor,**” “**controller,**” “**process(ing)(ed),**” “**processor,**” “**personal information,**” “**personal data,**” “**personal data breach,**” “**sell,**” “**sensitive data,**” “**sensitive personal information,**” “**share,**” “**selling,**” “**service provider,**” “**sale,**” “**sold,**” and “**targeted advertising,**” shall have the meanings given to such terms in US Privacy Laws, the GDPR, the UK GDPR, the Swiss DPA, or other applicable Data Protection Laws.
- c) “**Privacy Rights Request(s)**” or “**PRR(s)**” means a communication from a consumer or other data subject requesting to exercise their individual privacy rights under the GDPR, UK GDPR, Swiss DPA, US Privacy Laws, or other applicable Data Protection Laws.
- d) “**Data Protection Law(s)**” means all laws that govern the use of data and privacy relating to identified or identifiable individuals, which may include, among others, and solely to the extent applicable, the GDPR (and any implementing legislation), the Data Protection Act 2018, U.S. Privacy Laws, the Privacy Act, and Directive 2002/58/EC (known as the e-Privacy Directive) (and any implementing legislation), the Swiss DPA, the UK GDPR, PIPEDA, as amended or replaced from time to time and to the extent applicable to a Party.
- e) “**Deidentified Data**” means data, which cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer and where GDPR and/or UK GDPR applies means personal data that has been pseudonymised by being processed in such a manner that it can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

- f) **“EU Standard Contractual Clauses” or “EU SCCs”** means, where the GDPR applies, the standard contractual clauses adopted by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, or any subsequent version thereof released by the European Commission. In the event any subsequent version of such clauses is released that is applicable to the Services, the Parties agree that the then-current version of the clauses will apply, in which case any references in this DPA to specific clauses shall be deemed to refer to equivalent clauses in the then-current version of the clauses, regardless of their enumeration.
- g) **“GDPR”** means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
- h) **“PIPEDA”** means Canada’s Personal Information Protection and Electronic Documents Act (“PIPEDA”).
- i) **“Swiss DPA”** means the Swiss Federal Act on Data Protection 1992 (including as amended or superseded).
- j) **“Swiss Addendum”** means the EU SCCs as recognized and adopted by the Federal Data Protection and Information Commissioner (“**FDPIC**”) under Art. 6 para. 2 and 3 of the Ordinance to the Federal Act on Data Protection DPO, SR. 235.11, as adopted, amended or updated by the FDPIC.
- k) **“Third Country(ies)”** means any country that is neither a member of the European Economic Area (“**EEA**”) or United Kingdom (“**UK**”) nor has an adequacy status (i.e. (i) a status granted by the European Commission to non-EEA countries which provide a level of personal data protection that is comparable to that provided in EU law in accordance with GDPR, or (ii) a status granted by UK Secretary of State to non-UK countries which provide a level of personal data protection that is comparable to that provided in UK law in accordance with UK Data Protection Laws).
- l) **“UK Addendum”** means the UK ‘International data transfer addendum to the European Commission’s standard contractual clauses for international data transfers,’ available at <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>, as adopted, amended or updated by the UK’s Information Commissioner’s Office, Parliament or Secretary of State.
- m) **“UK Data Protection Laws”** means the Data Protection Act 2018 (DPA 2018), as amended, and EU General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as incorporated into UK law (“**UK GDPR**”), as amended, and any other applicable UK data protection laws.
- n) **“US Privacy Law(s)”** means all applicable U.S. federal and/or state security, confidentiality, and/or privacy laws, and regulations that are applicable to Cintas, the Services, Customer Data, and/or any other programs or products provided pursuant to the Agreement, including but not limited to the California Consumer Privacy Act as amended by the California Privacy Rights Act (“**CPRA**”), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Utah Consumer Privacy Act, Connecticut’s Act

Concerning Personal Data Privacy and Online Monitoring, and any implementing regulations thereunder, in each case applicable to this DPA as and when legally effective.

3. Restrictions on Cintas' Processing: Cintas is permitted to process Customer Data solely for purposes of performing the Services and to carry out the Business Purposes under the Agreement, or as otherwise required or permitted by Data Protection Laws of a service provider/processor, or as agreed to or instructed by Customer. Without limiting the generality of the foregoing, except as otherwise permitted by the forgoing sentence, Cintas is prohibited from:

- a) Selling or Sharing Customer Data, the latter of which to the extent the CCPA/CPRA is applicable to processing hereunder, and as Sharing is defined therein;
- b) retaining, using, disclosing, or otherwise processing Customer Data for any purpose other than for the specific purpose of providing Services to Customer and to carry out the Business Purposes under the Agreement;
- c) retaining, using, or disclosing Customer Data for any commercial purpose other than to perform the Services and to carry out the Business Purposes under the Agreement;
- d) retaining, using, disclosing, or processing Customer Data outside of the direct business relationship between Customer and Cintas; and
- e) combining personal data received from or on behalf of Customer with personal data it receives from, or on behalf of, another person(s), or collects from its own interaction with a consumer, except where expressly required to perform the Services.

Cintas certifies it understands and will comply with the provisions of the CCPA/CPRA, to the extent applicable, pertaining to Service Providers.

Cintas shall not provide access to Customer Data to any other entity, unless agreed to or instructed by Customer or required by Data Protection Laws, except it may use subprocessors to perform the Services, provided (i) Cintas provides Customer a reasonable opportunity to object to the engagement of subprocessors and (ii) such subprocessors agree in writing to terms as stringent as those set forth in this DPA. As of the Effective Date of this Addendum, Cintas' subprocessors are set forth in Annex III of Schedule 2, and Customer expressly agrees to Cintas' use of the listed subprocessors.

Notwithstanding anything herein to the contrary, Customer acknowledges that Cintas may retain, use, disclose, or otherwise process Customer Data in manners permitted of a service provider/processor under US Privacy Laws or as otherwise required by Data Protection Laws (e.g., to engage subprocessors, for permitted internal uses such as improving products and services, for security and fraud prevention, compliance with legal obligations, etc.) and may create Deidentified data and Aggregate Consumer Information from Customer Data subject to Section 4(a) below ("**Permitted Cintas Purposes**").

For the purposes of GDPR and/or UK Data Protection Laws, if and to the extent that Cintas acts as controller in relation to processing activities falling within the Permitted Cintas Purposes, Cintas will be an independent controller and will be solely and entirely responsible for its compliance in that capacity with all applicable Data Protection Laws. Where Cintas acts as controller for purposes of GDPR and/or UK Data Protection Laws, the Parties shall enter into EU Standard Contractual Clauses (Module One: Transfers Controller to Controller) and UK Addendum, in each case validly completed

and executed, to ensure that any actual or deemed transfer of Customer Data from Customer to Cintas is in all respects lawful.

4. Cintas' Obligations: Cintas shall, with respect to the Services and the Customer Data:

a) to the extent Cintas receives, or Cintas creates, Deidentified data in connection with this DPA: (i) maintain such information as Deidentified and take reasonable measures to ensure that it cannot be associated with an individual or household (including implementing technical safeguards and business processes to prevent reidentification or inadvertent release of the Deidentified data); (ii) publicly commit to maintain and use the information in Deidentified form and not to attempt to reidentify the information; (iii) not attribute Customer as a source of such data; and (iv) contractually obligate any third parties receiving such information from Cintas to also commit to (i), (ii), and (iv);

b) comply with Data Protection Laws in performing the Services, reasonably assist Customer in meeting its obligations under Data Protection Laws, and make available to Customer information in Cintas' possession necessary to demonstrate compliance with its obligations under Data Protection Laws upon Customer's reasonable request (subject to time and materials charges at standard rates if material efforts are required);

c) ensure the reasonable security of Customer Data including by: (i) providing the same level of privacy protection to Customer Data as is required by Data Protection Laws; and (ii) ensuring each person processing Customer Data is subject to a duty of confidentiality with respect to such Customer Data;

d) notify Customer within the time period required by Data Protection Laws if it determines it can no longer meet its obligations under Data Protection Laws and allow Customer to take reasonable and appropriate steps to stop and remediate unauthorized processing of Customer Data;

e) provide reasonable assistance to enable Customer to fulfill PRRs (subject to time and materials charges at standard rates if material efforts are required), including but not limited to notifying Cintas' subcontractors to delete specified Customer Data in response to a PRR made to Customer, subject to denials and exceptions provided under Data Protection Laws or other applicable law. Customer shall inform Cintas of PRRs for which it needs Cintas' assistance to comply and shall provide Cintas with information necessary to assist Customer to comply with such PRRs;

f) if Cintas receives a PRR from a data subject that might relate to Customer Data it shall respond that it cannot act upon requests made to it as to data it processes as a service provider/processor. If the request specifically identifies Customer in connection with the PRR, Cintas shall inform Customer of such request;

g) notify Customer of a Breach and provide reasonable assistance and information regarding such Breach (as it may be required for the purposes of reporting to the authorities and, where necessary, to the data subjects);

h) provide Customer information to reasonably enable it to conduct and document data protection assessments and prior consultations to the applicable supervisory authority;

i) delete Customer Data at the end of the provision of Services, or as otherwise instructed by Customer, unless retention is (i) required by Data Protection Laws; or (ii) retained as part of backup or record keeping, so long as only used for such purposes and only for as long as reasonably necessary, subject to Data Protection Laws and this DPA; and

j) make available to Customer information necessary to demonstrate compliance with its obligations under this Agreement and under the Data Protection Laws and, not more than once annually (to the extent permitted by Data Protection Laws), allow and cooperate with reasonable assessments by Customer, or its designated assessor (or if mutually agreed and at Cintas' expense, Cintas' qualified assessor), to conduct a reasonable assessment of Cintas' policies and technical and organizational measures in support of the obligations under Data Protection Laws using an appropriate and accepted control standard or framework and assessment procedure for such assessments, and subject to reasonable access and confidentiality restrictions. If Cintas engages its own assessor, it shall provide a report of such assessment to Customer upon request. If Cintas receives instructions from Customer that, in its opinion, infringe Data Protection Laws, it shall immediately inform Customer about it. Any assessments shall be subject to Cintas' reasonable access and confidentiality requirements.

5. Customer Obligations: Customer represents and warrants that Customer Data has been collected in accordance with Data Protection Laws and is transferred to Cintas in connection with this DPA in accordance with Data Protection Laws. Customer acknowledges that it is the controller of Customer Data and shall take all steps necessary to ensure that it has all necessary authority and consent to enable Cintas to use the Customer Data to provide the Services and process Customer

Data consistent with Data Protection Laws, the Agreement, and this DPA, including without limitation timely providing Cintas all instructions for Cintas' processing as may be required by Data Protection Laws (e.g., notice to delete, notice discontinue certain processing, etc.).

Customer agrees to defend, indemnify, and hold harmless Cintas for any and all claims, causes of action, demands, damages, expenses, fines, penalties, and attorneys' fees and costs incurred by Cintas arising out of Cintas' processing of personal data in accordance with Customer's instructions.

In any case where Cintas will act as controller in relation to Customer Data transferred to it, the Parties agree that Cintas will provide Customer with the EU Standard Contractual Clauses (Module 1: Transfers Controller to Controller) completed as follow:

- i. Clause 7 (Optional – Docking Clause) shall be deemed incorporated;
- ii. Clause 9(a): General Written Authorisation and 10 business days;
- iii. For purposes of Clause 11 (Redress), the Parties agree that the optional wording shall not be incorporated herein and therefore shall not be applicable to the Parties;
- iv. For purposes of Clause 17 (Governing law), the Parties agree that the EU Standard Contractual Clauses (Module 1: Transfers Controller to Controller) shall be governed by the laws of Ireland and select Clause 17, “Option 1” to this effect;
- v. For purposes of Clause 18 (Choice of forum and jurisdiction), the Parties agree that any dispute arising from the EU Standard Contractual Clauses (Module 1: Transfers Controller to Controller) shall be resolved by the Courts of Ireland; and

vi. The Cintas shall populate Annexes I, II and II of the EU Standard Contractual Clauses (Module 1: Transfers Controller to Controller);

6. International Data Transfers on a Controller to Processor Basis: For data transfers from the EEA/UK to Third Countries, to the extent such transfers are subject to GDPR (including the UK GDPR) and/or the Swiss DPA, the Parties hereby incorporate the EU Standard Contractual Clauses and/or the UK Addendum as follows:

a) The Parties hereby incorporate the EU Standard Contractual Clauses (Module 2: Transfers Controller to Processor) by reference and as a safeguard for the transfer of personal data to a Third Country. The EU Standard Contractual Clauses (Module 2: Transfers Controller to Processor) will be deemed completed as follows:

i. Clause 7 (Optional – Docking Clause) shall be deemed incorporated;

ii. Clause 9(a): General Written Authorisation and 10 business days;

iii. For purposes of Clause 11 (Redress), the Parties agree that the optional wording shall not be incorporated herein and therefore shall not be applicable to the Parties;

iv. For purposes of Clause 17 (Governing law), the Parties agree that the EU Standard Contractual Clauses (Module 2: Transfers Controller to Processor) shall be governed by the laws of Ireland and select Clause 17, “Option 1” to this effect;

v. For purposes of Clause 18 (Choice of forum and jurisdiction), the Parties agree that any dispute arising from the EU Standard Contractual Clauses (Module 2: Transfers Controller to Processor) shall be resolved by the Courts of Ireland;

vi. Annexes I, II, and III of the EU Standard Contractual Clauses (Module 2: Transfers Controller to Processor) shall be deemed completed with the information set out in **Schedule 2** to this DPA, the contents of which are hereby agreed by the Parties;

vii. For the purposes of Annex I.C., the competent supervisory authority is the data protection authority of Ireland.

b) For the transfer of personal data governed by the UK Data Protection Laws to Third Countries, the Parties hereby incorporate by reference the UK Addendum, which incorporates the EU Standard Contractual Clauses (Module 2: Transfers Controller to Processor). The UK Addendum will be deemed completed as follows:

i. Table 1 shall be deemed completed with the information set out in the **Data Transfer Annex I within Schedule 2**, to the extent applicable, the contents of which are hereby agreed by the Parties;

ii. In Table 2, the Parties select the checkbox that reads: “Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum.” The applicable Approved EU SCCs Module is number 2 (Controller to Processor) and the accompanying UK addendum Table 2 shall be deemed to be completed according to Parties preferences outlined below:

a. Clause 7 (Optional – Docking Clause) shall be deemed incorporated;

b. Clause 9(a): General Written Authorisation and 10 business days;

c. For purposes of Clause 11 (Redress), the Parties agree that the optional wording shall not be incorporated herein and therefore shall not be applicable to the Parties.

iii. Table 3 shall be deemed completed with the information set out in the **Data Transfer Annexes I and III within Schedule 2**, the contents of which are hereby agreed by the Parties, to the extent applicable; and

iv. In Table 4, the Parties agree that only the Exporter may end the UK Addendum as set out in Section 19 of the same.

v. The Information Commissioner’s Office (“ICO”) will be the competent supervisory authority.

c) For the transfer of personal data governed by the Swiss DPA to Third Countries, the Parties hereby incorporate by reference the Swiss Addendum, which incorporates the EU Standard Contractual Clauses (Module 2: Transfers Controller to Processor):

i. The FDPIC will be the competent supervisory authority;

ii. Data subjects in Switzerland may enforce their rights in Switzerland under clause 18c of the EU SCCs, and

iii. References in the EU SCCs to the EU GDPR should be understood as references to Swiss Data Protection Law insofar as the data transfers are subject to Swiss Data Protection Law.

SCHEDULE 1

PROCESSING SCHEDULE

PERSONAL DATA PROCESSING PURPOSES AND DETAILS

Business Purposes: *Providing the Services, as described in the Agreement.*

Personal Data Categories: *Customer employees' names and other business-to-business contact information, such as work e-mail, phone number, address, and, in some cases, garment size.*

Data Subject Types: *Customer employees and other business-to-business contacts.*

Processing Duration: *Cintas will process Customer Data for the duration of the Agreement, or retain it as otherwise required under applicable law.*

Countries where the Provider may receive, access, transfer or store Personal Data: *The United States of America, Canada, and/or Switzerland.*

SCHEDULE 2

DATA TRANSFER ANNEXES

ANNEX 1

Processing on a Controller to Processor Basis

Data Exporter (s)	Capacity of Data Exporter(s)	Data Importer(s) – Identification and contact details	Capacity of Data Importer(s)	Competent Supervisory Authority
The Customer, as set forth in the Agreement	Controller	Cintas, as set forth in the Agreement	Processor; Controller (if applicable)	Ireland for EU transfers; the FDPIC for Swiss transfers; the ICO for UK transfers

A. ACTIVITIES RELEVANT TO THE DATA TRANSFERRED

The activities relevant to the personal data transferred are specified under B of this Annex I.

B. DESCRIPTION OF THE TRANSFERS

1. Categories of data subjects whose personal data is transferred: *Cintas will process Customer Data in accordance with the Agreement and the instructions set forth in this Data Protection Addendum.*
2. Categories of personal data transferred: *Customer employees' names and other business-to-business contact information, such as work e-mail, phone number, address, and, in some cases, garment size.*
3. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: *Not applicable.*
4. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): *Continuous*
5. Nature of the processing (i.e., processing operations): *Providing the Services, as described in the Agreement.*
6. Purpose(s) of the data transfer and further processing: *Providing the Services, as described in the Agreement.*
7. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: *Cintas will retain Customer Data for the duration of the Agreement, or as otherwise required under applicable law.*

8. For transfers to subprocessors, also specify subject matter, nature and duration of the processing: *Cintas will engage subprocessors as identified in the list of Authorized Subprocessors available at www.cintas.com/dataprotectioncenter.*

9. Deidentified Data: *Cintas shall be entitled to create Deidentified data and Aggregate Consumer Information as defined by Data Protection Laws and use such data for its own purposes, subject to Cintas obligations as set forth in the DPA. Notwithstanding the foregoing, with respect to Customer Data which Processing is subject to the GDPR, UK GDPR, or the Swiss DPA, such uses by Cintas are limited to Anonymized data. Customer represents and warrants that it has informed the Customer data subjects that their Personal Data is subject to Anonymization by third parties.*

C. **COMPETENT SUPERVISORY AUTHORITY**

The Supervisory Authority of Ireland for EU transfers; the FDPIC for Swiss transfers; and/or the ICO for UK transfers.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Cintas has implemented and shall maintain the technical and organizational security measures, described in the Technical and Organizational Security Measures in Data Protection Center, found at www.cintas.com/dataprotectioncenter.

ANNEX III

PRE-APPROVED SUB-PROCESSORS

The controller has authorised the use of the sub-processors identified in the authorized sub-processor list in Data Protection Center found at www.cintas.com/dataprotectioncenter.