Explanatory Note as to why there are no SCCs in this DPA: All customers of Momentive located outside the United States contract with Momentive Europe UC. This is an Irish entity based within the European Union. All data transfers occurring through use of our services in Europe to Momentive Europe UC are therefore transfers between two European parties, which does not require a mechanism (e.g. Standard Contractual Clauses) for transfer. Our Momentive Europe UC entity may (depending on the service) export personal data to the United States for onward processing. Momentive Europe UC therefore is a "data exporter" under Standard Contractual Clauses and enters into onward transfer Standard Contractual Clauses with applicable subprocessors "importers".

MOMENTIVE DATA PROCESSING AGREEMENT

HOW THIS DPA APPLIES

This Momentive Data Processing Agreement ("**DPA"**) forms part of your Agreement with Momentive and contains certain terms relating to data protection, privacy, and security in accordance with the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**") and the California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 - 1798.199) ("**CCPA**"), where applicable. In the event (and to the extent only) that there is a conflict between the GDPR and the CCPA, the parties shall comply with the more onerous requirement or higher standard which shall, in the event of a dispute in that regard, be determined solely by Momentive.

This DPA is between the Customer and the applicable Momentive entity determined as follows:

(i) for Customers located in any country other than the United States, Momentive Europe UC shall be the contracting entity;

(ii) for Customers located inside the United States, Momentive Inc. shall be the contracting entity.

This is the latest version of the DPA (dated 16 August 2021).

DATA PROCESSING TERMS

1 Interpretation

In this DPA the following expressions shall, unless the context otherwise requires, have the following meanings:

"**Agreement**" means any agreement between Momentive Inc. or Momentive Europe and a customer for the Services. Such an agreement may have various titles, such as "Order Form", "Sales Order", "Terms of Use" or "Master or Governing Services Agreement".

"**Article 28**" means article 28 of GDPR.

"**Customer**" or "**you**" means the customer that is identified on, and/or is a party to, the Agreement.

"**Customer Data**" means all data (including but not limited to Customer Personal Data and End User data) that is provided to Momentive by, or on behalf of, Customer through Customer's use of the Services, and any data that third parties submit to Customer through the Services.

"**Customer Personal Data**" means all personal data (including that of End Users) that is submitted to the Services by or to Customer, processed by Momentive for the purposes of delivering the Services to the Customer including but not limited to the personal data set out in Appendix 2 to this DPA.

"**Data Protection Legislation**" means:

(i) the GDPR and all other applicable EU, EEA or European single market Member State laws or regulations or any update, amendment or replacement of same that apply to processing of personal data under the Agreement;

(ii) all U.S. laws and regulations that apply to processing of personal data under the Agreement including but not limited to CCPA;

(iii) all laws and regulations that apply to processing of personal data under the Agreement from time to

time in place in the United Kingdom and Canada,

and the terms "controller", "data subject", "data protection impact assessment", "personal data", "process", "processing", "processor", "supervisory authority" have the same meanings as in the GDPR and with respect to CCPA (as defined above), Momentive and Customer hereby agree that Momentive is a "**Service Provider**" and Customer is the "**Business**", as defined under the CCPA and with respect to Personal Information (as defined under the CCPA).

"**End Users**" means, in the case of an Enterprise Customer under our Governing Services Agreement, Customer's employees, agents, independent contractors and other individuals authorized by Customer to access and use the Services.

"**Momentive**" or "**us**" means in the case of Customers in the United States, Momentive Inc. and, in the case of customers outside of the United States, Momentive Europe.

"**Momentive Europe**" means Momentive Europe UC, an Irish company, located at 2 Shelbourne Buildings, Second Floor, Shelbourne Road, Dublin 4, Ireland.

"**Momentive Inc.**" means Momentive Inc., a Delaware corporation located at One Curiosity Way, San Mateo, CA 94403, United States.

"**Momentive Privacy Notice**" means the Momentive Privacy Notice at . https://www.surveymonkey.com/mp/legal/privacy/.

"**Services**" means the services ordered by Customer from Momentive under the Agreement.

"**Standard Contractual Clauses**" means the "Standard Contractual Clauses" annexed to the European Commission Decision of: i) 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to GDPR or ii) (until such times as Momentive has entered into the Standard Contractual Clauses outlined at i)), the 5 February 2010 for the Transfer of Customer Personal Data to Processors established in Third Countries under Directive 95/46/EC).

2 Status of Momentive

In the provision of the Services to the Customer, Momentive is a processor of Customer Personal data for the purposes of GDPR.

3 Term

This DPA shall remain in force until such time as the Agreement is terminated (in accordance with its terms) or expires.

4 Customer's Obligations

Customer shall ensure and hereby warrants and represents that it is entitled to transfer the Customer Data to Momentive so that Momentive may lawfully process and transfer the personal data in accordance with this DPA. Customer shall ensure that any relevant data subjects have been informed of such use, processing, and transfer as required by the Data Protection Legislation and that lawful consents have been obtained (where appropriate). Customer shall ensure that any personal data processed or transferred to Momentive will be done lawfully and properly.

5 Momentive's Obligations

Where Momentive is processing Customer Personal Data for Customer as a processor, Momentive will:

(a) only do so on documented Customer instructions and in accordance with the Data Protection Legislation, including with regard to transfers of personal data to other jurisdictions or an international organization, and the parties agree that the Agreement constitutes such documented instructions of the Customer to Momentive to process Customer Personal Data (including to locations outside of the EEA) along with other reasonable instructions provided by the Customer to Momentive (e.g. via email) where such instructions are consistent with the Agreement;

(b) ensure that all Momentive personnel involved in the processing of Customer Personal Data are subject to confidentiality obligations in respect of the personal data;

(c) make available information necessary for Customer to demonstrate compliance with its Article 28 obligations (if applicable to the Customer) where such information is held by Momentive and is not otherwise

available to Customer through its account and user areas or on Momentive websites, provided that Customer provides Momentive with at least 14 days' written notice of such an information request;

(d) co-operate as reasonably requested by Customer to enable Customer to comply with any exercise of rights by a data subject afforded to data subjects by Data Protection Legislation in respect of personal data processed by Momentive in providing the Services;

(e) provide assistance, where necessary, with requests received directly from a Data Subject in respect of a Data Subject's Personal Data submitted through the Services;

(f) upon deletion by you, not retain Customer Personal Data from within your account other than in order to comply with applicable laws and regulations and as may otherwise be kept in routine backup copies made for disaster recovery and business continuity purposes subject to our retention policies;

(g) cooperate with any supervisory authority or any replacement or successor body from time to time (or, to the extent required by the Customer, any other data protection or privacy regulator under Data Protection Legislation) in the performance of such supervisory authority's tasks where required;

(h) assist Customer as reasonably required where Customer:

(i) conducts a data protection impact assessment involving the Services (which may include by provision of documentation to allow customer to conduct their own assessment); or

(ii) is required to notify a Security Incident (as defined below) to a supervisory authority or a relevant data subject

(i) will not (a) sell any Personal Information (as defined under the CCPA) for a commercial purpose, or (b) collect, retain, use, disclose, or otherwise process Personal Information other than (1) to fulfill its obligations to Customer under the Agreement, (2) on the Customer's behalf, (3) for the Customer's operational purposes, (4) for Momentive's internal use as permitted by Data Protection Legislation, (5) to detect data security incidents or protect against fraudulent or illegal activity, or (6) as otherwise permitted under Data Protection Legislation;

(j) Where required by Data Protection Legislation, Momentive will inform Customer if it comes to its attention that any instructions received by Customer infringe the provisions of Data Protection Legislation. Notwithstanding the foregoing, Momentive shall have no obligation to monitor or review the lawfulness of any instruction received from the Customer; and

(k) Momentive certifies thrat it understands the restrictions and obligations set forth in this DPA and that it will comply with them.

6 Subprocessors

6.1 Subprocessing. Customer provides a general authorization to Momentive to engage onward subprocessors, subject to compliance with the requirements in this Section 6.

6.2 Subprocessor List. Momentive will, subject to the confidentiality provisions of the Agreement or otherwise imposed by Momentive:

(a) make available to Customer a list of the Momentive subcontractors who are involved in processing or subprocessing Customer Personal Data in connection with the provision of the Services ("**Subprocessors**"), together with a description of the nature of services provided by each Subprocessor ("**Subprocessor List**"). A copy of this Subprocessor List may be requested here;

(b) ensure that all Subprocessors on the Subprocessor List are bound by contractual terms that are in all material respects no less onerous than those contained in this DPA; and

(c) be liable for the acts and omissions of its Subprocessors to the same extent Momentive would be liable if performing the services of each of those Subprocessors directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6.3 New / Replacement Subprocessors. Momentive will provide Customer with written notice of the addition of any new Subprocessor or replacement of an existing Subprocessor at any time during the term of the Agreement ("**New Subprocessor Notice**"). The Customer will sign up to a mailing list made available by Momentive through which such notices will be delivered by e-mail or alternatively will check on updates to

the list **here**. If Customer has a reasonable basis to object to Momentive's use of a new or replacement Subprocessor, Customer will notify Momentive promptly in writing and in any event within 30 days after receipt of a New Subprocessor Notice. In the event of such reasonable objection, either Customer or Momentive may terminate the portion of any Agreement relating to the Services that cannot be reasonably provided without the objected-to new Subprocessor (which may, at Momentive's discretion and election, involve termination of the entire Agreement) with immediate effect by providing written notice to the other party. Such termination will be without a right of refund for any fees prepaid by Customer for the period following termination.

7 Security

7.1 Security Measures. Momentive has, taking into account the state of the art, cost of implementation and the nature, scope, context and purposes of the Services and the level of risk, implemented appropriate technical and organizational measures (in accordance with Appendix 1) to ensure a level of security appropriate to the risk of unauthorized or unlawful processing, accidental loss of and/or damage to Customer Data. At reasonable intervals, Momentive tests and evaluates the effectiveness of these technical and organizational measures for ensuring the security of the processing.

7.2 Security Incident and Breach Notification. If Momentive becomes aware of any unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of, Customer Personal Data ("**Security Incident**"), Momentive will take reasonable steps to notify Customer without undue delay. A Security Incident does not include unsuccessful attempts or activities that do not compromise the security of personal data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems. Any notification of a Security Incident to the Customer does not constitute any acceptance of liability by Momentive.

7.3 Momentive will also reasonably cooperate with Customer with respect to any investigations relating to a Security Incident with preparing any required notices, and provide any information reasonably requested by Customer in relation to any Security Incident.

8 Audits

8.1 Audits. Where Momentive is processing Customer Personal Data for Customer as a processor (only), the Customer will provide Momentive with at least one month's prior written notice of any audit, which may be conducted by Customer or an independent auditor appointed by Customer (provided that no person conducting the audit shall be, or shall act on behalf of, a competitor of Momentive) ("**Auditor**"). The scope of an audit will be as follows:

(a) Customer will only be entitled to conduct an audit once per subscription year unless otherwise legally compelled or required by a regulator with established authority over the Customer to perform or facilitate the performance of more than 1 audit in that same year (in which circumstances Customer and Momentive will, in advance of any such audits, agree upon a reasonable reimbursement rate for Momentive's audit expenses).

(b) Momentive agrees, subject to any appropriate and reasonable confidentiality restrictions, to provide evidence of any certifications and compliance standards it maintains and will, on request, make available to Customer an executive summary of Momentive's most recent annual penetration tests, which summary shall include remedial actions taken by Momentive resulting from such penetration tests.

(c) The scope of an audit will be limited to Momentive systems, processes, and documentation relevant to the processing and protection of Customer Personal Data, and Auditors will conduct audits subject to any appropriate and reasonable confidentiality restrictions requested by Momentive.

(d) Customer will promptly notify and provide Momentive on a confidential basis with full details regarding any perceived non-compliance or security concerns discovered during the course of an audit.

8.2 The parties agree that, except as otherwise required by order or other binding decree of a supervisory authority or regulator with authority over the Customer, this Section 8 sets out the entire scope of the Customer's audit rights as against Momentive.

9 International Data Transfers

9.1 To the extent applicable, for transfers of Customer Personal Data from the European Economic Area to locations outside the European Economic Area (either directly or via onward transfer) that do not have

adequate standards of data protection as determined by the European Commission, Momentive relies upon:

(a) the Standard Contractual Clauses; or

(b) such other appropriate safeguards, or derogations (to the limited extent appropriate), specified or permitted under the Data Protection Legislation.

9.2 With respect to Momentive's reliance on the Standard Contractual Clauses for international transfers of Customer Personal Data under the Agreement, Momentive shall act in its capacity as 'data importer' or 'data exporter' (as appropriate) as set out in the relevant modules of the Standard Contractual Clauses (as applicable). Upon written request and in accordance with the provisions of the Standard Contractual Clauses, Momentive will provide copies of the Standard Contractual Clauses entered into with data importers in its capacity as processor to the Customer.

10 General Provisions

10.1 Liability for data processing. Each party's aggregate liability for any and all claims whether in contract, tort (including negligence), breach of statutory duty, or otherwise arising out of or in connection with this DPA shall be as set out in the Agreement, unless otherwise agreed in writing by the parties.

10.2 Conflict. In the case of conflict or ambiguity between: (i) the terms of this DPA and the terms of the Agreement, with respect to the subject matter of this DPA, the terms of this DPA shall prevail; (ii) the terms of any provision contained in this DPA and any provision contained in the Standard Contractual Clauses, the provision in the Standard Contractual Clauses shall prevail.

10.3 Independent Processing. Customer remains exclusively liable for its own compliance with Data Protection Legislation with respect to any independent collection and processing of personal data unrelated to the Services. Customer will provide its own clear and conspicuous privacy notices that accurately describe how it does this and Momentive will not be liable for any treatment of personal data by Customer in those circumstances. Customer hereby indemnifies Momentive in full for any and all claims or liability arising as a result of such collection and use of personal data by it in those circumstances.

10.4 Entire Agreement. The Agreement (which incorporates this DPA) and any Order Form represent the entire agreement between the parties and it supersedes any other prior or contemporaneous agreements or terms and conditions, written or oral, concerning its subject matter. Each of the parties confirms that it has not relied upon any representations not recorded in the Agreement inducing it to enter into the Agreement.

10.5 Severance. If any provision of this DPA is determined to be unenforceable by a court of competent jurisdiction, that provision will be severed and the remainder of terms will remain in full effect. Nothing in this DPA is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, nor authorise any party to make or enter into any commitments for or on behalf of any other party except as expressly provided herein.

10.6 Electronic Copy. This DPA is delivered as an electronic document.

10.7 Governing Law. This DPA shall be governed by the laws of Ireland and the parties submit to the exclusive jurisdiction of the Irish courts (in relation to all contractual and non-contractual disputes) except in the case of any alleged breach or breach of current or future privacy laws, regulations, standards, regulatory guidance, and self-regulatory guidelines at state or federal level in the United States of America, in which case the laws of the State of California shall govern unless otherwise dictated by that law.

Customer[1]

Signature:

Name:

Title:

[1] **Note this must be the person or organization named on the Momentive account (in the case of a person, they are acting in their capacity as an individual) NOT a related person or entity who is not party to the Agreement. If the party that signs here is not a party to an Agreement with Momentive this DPA will not be legally binding on Momentive.**

Date:

Momentive Europe UC	**Momentive, Inc.**
Signature: DocuSigned by: Sally Anne Hinfey	Signature: DocuSigned by: Lora Blum
Name: Sally Anne Hinfey	Name: Lora Blum
Title: Senior Director, Legal	Title: Chief Legal Officer & Secretary
Date: October 27, 2021	Date: October 25, 2021

Appendix 1

Description of the technical and organisational security measures implemented by Momentive

Momentive will maintain appropriate administrative, physical, and technical safeguards ("**Security Safeguards**") for protection of the security, confidentiality and integrity of personal data provided to it for provision of the Services to the Customer.

The Security Safeguards include the following:

(a) Domain: Organization of Information Security.

(i) **Security Roles and Responsibilities.** Momentive personnel with access to data are subject to confidentiality obligations.

(ii) **Risk Management Program.** Momentive performs a risk assessment where appropriate before processing the data.

(b) Domain: Asset Management.

(i) **Asset Handling.**

(1) Momentive has procedures for disposing of printed materials that contain Customer Data.

(2) Momentive maintains an inventory of all hardware on which Customer Data is stored.

(c) Domain: Human Resources Security.

(i) Security Training.

(1) Momentive informs its personnel about relevant security procedures and their respective roles. Momentive also informs its personnel of possible consequences of breaching the security rules and procedures.

(d) Domain: Physical and Environmental Security.

(i) **Physical Access to Facilities.** Momentive limits access to facilities where information systems that process Customer Data are located to identified authorized individuals.

(ii) **Protection from Disruptions.** Momentive uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

(iii) **Component Disposal.** Momentive uses industry standard processes to delete Customer Data when it is no longer needed.

(e) Domain: Communications and Operations Management.

(i) **Operational Policy.** Momentive maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data.

(ii) Data Recovery Procedures.

(1) On a regular and ongoing basis, Momentive creates backup copies of Customer Data from which Customer Data may be recovered in the event of loss of the primary copy.

(2) Momentive stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located.

(3) Momentive has specific procedures in place governing access to copies of Customer Data.

(iii) **Malicious Software.** Momentive has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks.

(iv) Data Beyond Boundaries.

(1) Momentive encrypts Customer Data that is transmitted over public networks.

(v) Event Logging.

(1) Momentive logs the use of its data-processing systems.

(2) Momentive logs access and use of information systems containing Customer Data, registering the access ID, timestamp, and certain relevant activity.

(f) Domain: Information Security Incident Management.

(i) **Incident Response Process.**

(1) Momentive maintains an incident response plan.

(2) Momentive maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and remediation steps, if applicable.

(g) Domain: Business Continuity Management.

(i) Momentive's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original state from before the time it was lost or destroyed.

(h) Access Control to Processing Areas.

Processes to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where the Customer Personal Data are processed or used, to include:

(i) establishing secure areas;

(ii) protection and restriction of access paths;

(iii) securing the mobile/cellular telephones;

(iv) data processing equipment and personal computers;

(v) all access to the data centers where Customer Personal Data are hosted is logged, monitored, and tracked;

(vi) the data centers where Customer Personal Data are hosted is secured by a security alarm system, and other appropriate security measures; and

(vii) the facility is designed to withstand adverse weather and other reasonably predictable natural conditions, is secured by around-the-clock guards, keycard and/or biometric access (as appropriate to level of risk) screening and escort-controlled access, and is also supported by on-site back-up generators in the event of a power failure.

(i) Access Control to Data Processing Systems.

Processes to prevent data processing systems from being used by unauthorized persons, to include:

(i) identification of the terminal and/or the terminal user to the data processor systems;

(ii) automatic time-out after 30 minutes or less of user terminal if left idle, identification and password required to reopen;

(iii) issuing and safeguarding of identification codes;

(iv) password complexity requirements (minimum length, expiry of passwords, etc.); and

(v) protection against external access by means of an industrial standard firewall.

(j) Access Control to Use Specific Areas of Data Processing Systems.

Measures to ensure that persons entitled to use data processing systems are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that Customer Personal Data cannot be read, copied, modified or removed without authorization, to include by:

(i) implementing binding employee policies and providing training in respect of each employee's access rights to the Customer Personal Data;

(ii) effective and measured disciplinary action against individuals who access Customer Personal Data without authorization;

(iii) release of data to only authorized persons;

(iv) implementing principles of least privileged access to information which contains Customer Personal Data strictly on the basis of "need to know" requirements;

(v) production network and data access management governed by VPN, two factor authentication, and role-based access controls;

(vi) application and infrastructure systems log information to centrally managed log facility for troubleshooting, security reviews, and analysis; and

(vii) policies controlling the retention of backup copies which are in accordance with applicable laws and which are appropriate to the nature of the data in question and corresponding risk.

(k) Transmission Control.

Procedures to prevent Customer Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media and to ensure that it is possible to check and establish to which bodies the transfer of Customer Personal Data by means of data transmission facilities is envisaged, to include:

(i) use of firewall and encryption technologies to protect the gateways and pipelines through which the data travels;

(ii) implementation of VPN connections to safeguard the connection to the internal corporate network;

(iii) constant monitoring of infrastructure (e.g. ICMP-Ping at network level, disk space examination at system level, successful delivery of specified test pages at application level); and

(iv) monitoring of the completeness and correctness of the transfer of data (end-to-end check).

(l) Storage Control.

When storing any Customer Personal Data: it will be backed up as part of a designated backup and recovery processes in encrypted form, using a commercially supported encryption solution and all data defined as Customer Personal Data stored on any portable or laptop computing device or any portable storage medium is likewise encrypted. Encryption solutions will be deployed with no less than a 128-bit key for symmetric encryption and a 1024 (or larger) bit key length for asymmetric encryption;

(m) Input Control.

Measures to ensure that it is possible to check and establish whether and by whom Customer Personal Data has been input into data processing systems or removed, to include:

(i) authentication of the authorized personnel;

(ii) protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;

(iii) utilization of user codes (passwords);

(iv) proof established within data importer's organization of the input authorization; and

(v) ensuring that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are locked.

(n) Availability Control.

Measures to ensure that Customer Personal Data are protected from accidental destruction or loss, to include infrastructure redundancy and regular backups performed on database servers.

(o) Segregation of Processing.

Procedures to ensure that data collected for different purposes can be processed separately, to include:

(i) separating data through application security for the appropriate users;

(ii) storing data, at the database level, in different tables, separated by the module or function they support;

(iii) designing interfaces, batch processes and reports for only specific purposes and functions, so data collected for specific purposes is processed separately; and

(iv) barring live data from being used for testing purposes as only dummy data generated for testing purposes may be used for such.

(p) Vulnerability management program.

A program to ensure systems are regularly checked for vulnerabilities and any detected are immediately remedied, to include:

(i) all networks, including test and production environments, regularly scanned; and

(ii) penetration tests are conducted regularly and vulnerabilities are remedied promptly.

(q) Data Destruction.

In the event of expiration or termination of the Agreement by either side or otherwise on request from the Customer following receipt of a request from a data subject or regulatory body:

(i) all Customer data shall be securely destroyed within 3 months; and

(ii) all Customer data shall be purged from all Momentive and/or third party storage devices including backups within 6 months of termination or receipt of a request from Customer unless Momentive is otherwise required by law to retain a category of data for longer periods. Momentive will ensure that all such data which is no longer required is destroyed to a level where it can be assured that it is no longer recoverable.

(r) Standards and Certifications

Data storage solutions and/or locations have at least SOC 1 (SSAE 16) or SOC 2 reports – equivalent or similar certifications or security levels will be examined on a case by case basis.

Appendix 2

Purposes and Nature of Personal Data Processing, Categories of Personal Data, Data Subjects

The parties agree that the purpose and nature of the processing of Customer Personal Data, the types of personal data and categories of data subjects are as set out in this Appendix 2.

Purposes and Nature of Processing	Momentive may process Customer Personal Data as necessary to technically perform the Services, including where applicable: Hosting and storage; Backup and disaster recovery; Technically improve the service; Service change management; Issue resolution; Providing secure, encrypted Services; Applying new product or system versions, patches, updates and upgrades; Monitoring and testing system use and performance; Proactively detect and remove bugs; IT security purposes including incident management; Maintenance and performance of technical support systems and IT infrastructure; Migration, implementation, configuration and performance testing; Making product recommendations; Providing customer support; transferring data, and Assisting with data subject requests (as necessary).
Categories of Personal data	The Customer may submit Customer Personal Data to the Services, and may request for the Customer's respondents to submit personal data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, without limitation: Personal data of all types that may be submitted by the Customer's respondents to the Customer via users of the Services (such as via surveys or other feedback tools). For example: name, geographic location, age, contact details, IP address, profession, gender, financial status, personal preferences, personal shopping or consumer habits, and other preferences and other personal details that the Customer solicits or desires to collect from its respondents. Personal data of all types that may be included in forms and surveys hosted on the Services for the Customer (such as may be included in survey questions). The Customer's respondents may submit special categories of personal data to the Customer via the Services, the extent of which is determined and controlled by the Customer. For clarity, these special categories of Personal data may include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Data Subjects	Data subjects include: Natural persons who submit personal data to Momentive via use of the Services (including via online surveys and forms hosted by Momentive on behalf of the Customer); Natural persons whose personal data may be submitted to the Customer by Respondents via use of the Services; Natural persons who are employees, representatives, or other business contacts of the Customer; The Customer's users who are authorized by the Customer to access and use the Services.

WF-29955762-6