3M PRIVACY EXHIBIT
3M DATA PRIVACY REQUIREMENTS

This 3M Data Privacy Exhibit ("**Privacy Exhibit**") supplements the Agreement any Purchase Order Terms ("**Agreement**") into which it is incorporated. Capitalized terms not defined in this Privacy Exhibit have the meaning ascribed to such terms in the Agreement.

The purpose of this Privacy Exhibit is to establish Supplier's obligations in relation to the Processing of Personal Information where Supplier acts as a **Data Controller.**

A. GENERAL PROVISIONS

1. Order of Precedence. The provisions of this Privacy Exhibit supplement, and in the event of any inconsistency supersede, the provisions of the Agreement relating to the protection of Personal Information, privacy, and confidentiality.

2. Definitions. For purposes of this Privacy Exhibit, the terms "**Controller**" and "**Processor**" each have the meaning ascribed to such or similar terms under Applicable Privacy Laws.

2.1 "**Applicable Privacy Laws**" means all privacy, security, data protection, direct marketing, consumer protection, and workplace privacy laws, rules, requirements, and regulations of any applicable jurisdiction as of the Effective Date or as may become effective and/or amended or replaced from time to time, and any applicable successor provisions, including US State Data Protection Laws, Canadian Data Protection Laws, EU Data Protection Laws, UK GDPR, and PIPL, in each case as applicable to the Processing of Personal Information in connection with the Agreement.

2.2 **"Canadian Data Protection Laws"** means the privacy laws, statutes, rules, guidelines, directions, orders and regulations enacted by the federal, provincial, and territorial Canadian governments, including without limitation, the Federal Personal Information Protection and Electronic Documents Act, the Quebec Act Respecting the Protection of Personal Information in the Private Sector, the British Columbia Personal Information Protection Act, and the Alberta Personal Information Protection Act and any comparable legislation in any other Canadian jurisdiction as each may be amended or replaced from time to time, and any regulations implementing the foregoing.

2.3 "**Cybersecurity Incident**" means an unauthorized incident, or a series of related unauthorized incidents, on or conducted through Supplier's Information Systems that impacts the confidentiality, integrity or availability of the Supplier's Information Systems, including by jeopardizing business operations, finances, legal compliance, or reputation. For example, Cybersecurity Incidents may include malware, cyber-attacks, insider actions, or systemic control failures that allow unauthorized access, theft, exposure, alteration, or destruction of assets or data; or that may cause business interruptions to Supplier or its customers; or that may cause direct or indirect financial impact to Supplier or its customers.

2.4 "**EU Data Protection Laws**" means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("**EU GDPR**"), as it may be amended or replaced from time to time, guidelines from the European Data Protection Board, and any applicable national laws, rules, and regulations implementing the foregoing.

2.5 "**Personal Information**" means information relating to an identified or identifiable natural person (i.e., a person 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) or that is defined as "Personal Information," "Personally Identifiable Information," "Sensitive Personal Information," "Personal Data," or any similar designation by Applicable Privacy Laws, in any form and any media, that Supplier receives, Processes, generates, compiles, or creates in connection with the Agreement.

2.6 "**PIPL**" means the China Personal Information Protection Law.

2.8 "**Privacy Incident**" means any event that involves an unauthorized or unintended exposure, modification, access, disclosure, or other misuse of Personal Information. This could involve accidental sharing of information or a Cybersecurity Incident that involves Personal Information, or any other occurrence that compromises an individual's Personal Information. For example, Privacy Incidents may include misdirected mailings, marketing incidents, or unauthorized disclosure (including loss) of paper files containing Personal Information.

2.9 "**Process**" has the meaning ascribed to it in the Data Security Exhibit.

2.10 "**SCCs**" means (i) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 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 ("**EU SCCs**"), including any

annexes thereto; (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the UK Data Protection Act 2018 ("**UK Addendum**"); and (iii) where the Swiss FADP applies, the EU SCCs as amended by Article 13 of this Privacy Exhibit.

2.11 "**Subprocessor**" means any third party entity that Processes a Controller's Personal Information on behalf of a Processor.

2.12 "**Swiss FADP**" means the Swiss Federal Act on Data Protection dated 25 September 2020 and effective from 1 September 2023.

2.13 "**UK GDPR**" means the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018, subject to the amendments in Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).

2.14 "**US State Data Protection Laws**" means comprehensive consumer privacy laws, statutes, rules, requirements and regulations enacted by states of the United States of America, including the California Consumer Privacy Act of 2018, the California Privacy Rights Act of 2020, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Act Concerning Personal Data Privacy and Online Monitoring, the Utah Consumer Privacy Act, and any comparable legislation in any other states, as each may be amended or replaced from time to time, and any regulations implementing the foregoing.

3. 3M Personal Information Requirements.

3.1 The Parties agree that each Party is, and shall act as, an independent Controller (or similar term under Applicable Privacy Laws) regarding all Personal Information Processed by such Party pursuant to the Agreement. If any situation arises in which the Supplier is, or should be, considered 3M's Processor, the Parties shall implement 3M's standard Processor data privacy requirements and terms.

3.2 The Parties shall Process Personal Information only in accordance with Applicable Privacy Laws, this Privacy Exhibit, and the Data Security Exhibit.

3.3 The Parties acknowledge that Schedule 1 to the Privacy Exhibit sets out details about the Personal Information Processed in connection with the Agreement. Schedule 1 to the Privacy Exhibit is hereby incorporated into the Agreement. Supplier shall provide information specified in the Schedule 1 to the Privacy Exhibit and ensure that the information it provides is fully accurate and comprehensive based on the processing activities it undertakes pursuant to the Agreement.

3.4 The Parties shall notify each other without undue delay if: (i) a Party has a reasonable belief that a particular Processing activity required under the Agreement may infringe Applicable Privacy Laws, or (ii) either Party becomes aware that Personal Information is inaccurate or has become outdated.

3.6 To the extent permitted by applicable law, the Parties shall take reasonable actions to prevent disclosure of Personal Information shared by the other Party to government authorities and/or in response to a legal demand such as subpoena or similar demand.

3.7 To the extent practical and appropriate given their roles as independent Controllers, the Parties shall cooperate with and assist each other in ensuring compliance with Applicable Privacy Laws, including providing notices to and obtaining consents from data subjects, and responding to requests, inquiries, claims, and complaints regarding the Processing of Personal Information.

3.8 The Parties shall ensure that any persons authorized to Process Personal Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.9 The Parties will use best efforts to encrypt all Personal Information, including while in transit and in storage, in accordance with the Data Security Exhibit.

3.11 The Parties agree that no "sale" (as that term is defined under Applicable Privacy Laws) of Personal Information is intended as part of any Agreement, and both Parties will take steps to ensure no sale occurs by, for example, ensuring data subjects are made aware that their Personal Information will be disclosed to the other Party, and that it is clear to the individual that they are using or directing a Party to intentionally disclose Personal Information to, or interact with, the other Party. The Parties agree that any provision of Personal Information by one Party to another under this Agreement is necessary to perform a business purpose and is not part of, and explicitly excluded from, the exchange of consideration, or any other thing of value, between the Parties.

4. Privacy Incidents. In the event a Party experiences a Privacy Incident impacting Personal Information that the other Party disclosed, the Party experiencing the Privacy Incident shall promptly notify the other Party. The Party experiencing the Privacy Incident shall comply with Applicable Privacy Laws including, if applicable, any notice obligations. The Parties shall reasonably cooperate in the resolution of a Privacy Incident as appropriate given their roles as independent Controllers. Neither Party shall provide notice to individuals or other regulatory bodies without the consent of the other Party if the notice would mention, or imply involvement of, the other Party.

5. Technical, Physical and Organizational Security Measures. Supplier shall comply at all times with the Data Security Exhibit, and 3M shall comply with its internal technical, physical, and organizational security measures. All such safeguards shall take into account the nature of the Personal Information Processed pursuant to the Agreement.

6. Subprocessors. The Parties may appoint Subprocessors as are necessary to fulfil the purposes of the Agreement. Such Subprocessors will process any Personal Information on the appointing Party's behalf and direction. The Parties will conduct appropriate due diligence on their Subprocessors and adopt suitable contractual provisions to ensure compliance with all Applicable Privacy Laws.

7. Data Subject Rights.

7.1 The Parties agree that responsibility for complying with requests from data subjects to exercise rights under Applicable Privacy Laws falls to the Party receiving request in respect of the Personal Information held by, and under the responsibility of, that Party when acting as Controller.

7.2 The Parties agree to cooperate and provide reasonable assistance to each other as is necessary, given their roles as independent Controllers, to enable the Parties to comply with data subject requests and respond to any other queries or complaints from data subjects or regulators. The Parties shall bear their respective costs of responding to data subject requests, except that the Party providing assistance to the other Party in responding to a data subject request may charge a reasonable administrative fee as strictly necessary.

8. Cross-Border Data Transfers.

8.1 The Parties will comply with the requirements of Applicable Privacy Laws in relation to international data transfers, including the execution of regulatory data protection agreements such as the SCCs that may be amended from time to time. The SCCs are incorporated into the Privacy Exhibit by this reference.

8.2 To the extent that the Parties Processes Personal Information in a particular jurisdiction, and such Processing would be prohibited by Applicable Privacy Laws (other than EU, UK, and Swiss) in the absence of the implementation of terms comparable to the SCCs, the Parties shall Process all such Personal Information in accordance with such comparable terms and the Parties shall execute additional documents to comply with Applicable Privacy Laws.

8.3 To the extent required by Applicable Privacy Laws, the Supplier acknowledges and agrees to ensure its Subprocessors execute, the SCCs directly with 3M, its affiliates and/or subsidiaries.

8.4 The Parties may, without amending the Agreement:

8.4.1 Append additional document(s) to the SCCs or other contractual arrangements required by Applicable Privacy Laws to comply with Applicable Privacy Laws; and

8.4.2 Replace the SCCs currently appended to this Privacy Exhibit with any newly approved regulatory version of the SCCs.

8.5 If there is any conflict between the terms of this Privacy Exhibit, any SCCs, or other contractual arrangements required by Applicable Privacy Laws in force under the Agreement and any other provisions in the Agreement (or other terms and conditions as may be imposed from time to time, including but not limited to any unilateral terms imposed by Supplier), the terms of the SCCs or other contractual arrangements required by Applicable Privacy Laws shall prevail with respect to such conflicting terms.

9. Supplemental Privacy Terms. When and as reasonably required by 3M from time to time, Supplier shall execute and/or shall cause its affiliates or Subprocessors to execute supplemental data privacy, data protection, and/or data security terms with 3M. Where changes or additions to this Privacy Exhibit are necessary to ensure continued compliance with Applicable Privacy Laws, such changes shall be incorporated into this Privacy Exhibit from the date of 3M's written notice to Supplier and shall take effect immediately and shall be binding on both Parties.

Local Provisions

10. European Economic Area

Where the Parties are Processing Personal Information that is subject to the EU GDPR, the following applies:

10.1 Where either Party receives Personal Information that is subject to the EU GDPR for the performance of this Privacy Exhibit and one Party is located in a country outside the EEA for which the European Commission has not decided that an adequate level of personal data protection exists, the EU SCCs Module One shall be deemed automatically incorporated by reference into this Privacy Exhibit, and binding upon the Parties, including their respective affiliates.

10.2 The following operative provisions and required additional terms to the EU SCCs apply for Module One:

Data exporter	Data importer	Clause 7 (Docking Clause)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Clause 11(a) (Redress)	Clause 13 (Supervision)	Clause 17 (Governing Law)	Clause 18 (Choice of forum and jurisdiction)
3M or Supplier	3M or Supplier	Not applicable	Not applicable	Not applicable	Optional language not applicable	The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.	Option 1 Ireland	Ireland

10.3 With regard to the Appendix of the EU SCCs, the following applies:

(a) The contents of Schedule 1 to this Privacy Exhibit shall be provided by Supplier and shall form Annex I of the Appendix to the EU SCCs.
(b) The contents of the Data Security Exhibit shall form Annex II of the Appendix to the EU SCCs.

11. People's Republic of China

Where Supplier is Processing Personal Information of individuals in the People's Republic of China ("the **PRC**"), the following applies:

11.1 The following definitions apply to this Article 11 of the Privacy Exhibit:

11.1.1. "**Automated Decision-Making**" means the activity of analyzing and evaluating a person's behavioral habits, interests, economic, health, credit status, etc., and making decisions automatically through computer programs.

11.1.2. "**Personal Data Processor**" means an organization or individual that independently determines the purpose and manner of processing of Personal Information processing activities in accordance with PIPL;

11.1.3. "**PRC Standard Contract Clauses**" means the Standard Contracts for Cross-border Transfers of Personal Information as promulgated by the Cyberspace Administration of China.

11.2 Under this Article 11, Personal Information may be transferred by 3M, with respect to Personal Information that is already in the United States, as an onward transfer. Supplier shall Process Personal Information in accordance with the Agreement, the Data Security Exhibit, and this Privacy Exhibit.

11.3 Supplier agrees to comply with Applicable Privacy Laws and this Privacy Exhibit, and to Process Personal Information in accordance with the requirements or instructions of 3M, and to assist 3M in fulfilling its obligations under Applicable Privacy Laws. Supplier shall only use the Personal Information received from 3M pursuant to this Article 11 to fulfill its obligations under the Agreement for the specific purposes and scope agreed upon by both Parties. Without 3M's express approval, Supplier shall not change the purpose of, nor modify, delete, disclose, publicize, store, sell, or transfer the Personal Information in scope.

11.4 Supplier shall (1) only collect and Process Personal Information received from 3M pursuant to this Article 11 in a manner that complies with Applicable Privacy Laws; (2) only grant access to limited personnel, including Supplier's employees or Subprocessors who are necessary to access the Personal Information for the Processing purposes agreed upon by both Parties; (3) ensure that limited personnel are subject to and have been explicitly informed of the same data protection obligations of Supplier under the Privacy Exhibit, the Data Security Exhibit, and this paragraph; (4) keep accurate and up-to-date records of any Personal Information that was Processed for at least 3 years and provide such records to 3M upon 3M's request; (5) provide reasonable assistance to enable 3M to respond to inquiries or requests from individuals exercising their rights under Applicable Privacy Laws with respect to their Personal Information (6) without 3M's express approval, not transfer the Personal Information to another country or region in any form (including but not limited to transfer, sharing, or remote access).

11.5 Supplier acknowledges the Personal Information provided to Supplier contains Personal Information of natural persons residing in the PRC, and 3M is bound to comply with PIPL including the applicable requirements of the PRC Standard Contract Clauses and the PRC Cross-border Data Transfer Security Assessment with respect to the Processing of PRC Personal Data. Supplier understands and agrees to Process the Personal Information in accordance with such applicable requirements, as instructed by 3M and subject to 3M's supervision. If the Cyberspace Administration of China modifies such compliance requirements of Processing PRC Personal Data by issuing new PRC Standard Contract Clauses or a new PRC Cross-border Data Transfer Security Assessment, the

relevant new requirements shall be incorporated into this Privacy Exhibit and be binding on both Parties from the date of 3M's written notice to Supplier.

11.6 Without 3M's express approval, Supplier shall not use any Personal Information received from 3M pursuant to this Article 11 for Automated Decision-Making.

11.7 Supplier shall not provide the Personal Information in scope to any judicial or law enforcement authorities outside the PRC, unless approved by the PRC regulatory authority and with the written approval of 3M.

12. Switzerland

Where either Party is Processing Personal Information that is subject to the Swiss FADP, the following applies:

12.1 If a situation applies as described in Article 10.1 of this Privacy Exhibit, but within the context of the Swiss FADP, the EU SCCs Module One referred to in Article 10.1 of this Privacy Exhibit, as completed with the information set out in Articles 10.2 and 10.3, and as amended by the provisions of Article 12.2, shall be deemed automatically incorporated by reference into this Privacy Exhibit and binding upon the Parties, including their respective affiliates.

12.2 The EU SCCs shall be amended as follows:

(a) The supervisory authority (Clause 13(a)) is the Swiss Federal Data Protection and Information Commissioner.
(b) The applicable law (Clause 17) is the law of Ireland.
(c) Any dispute arising from these Clauses shall be resolved by the courts of Ireland (Clause 18).
(d) The term 'Member State' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of enforcing their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Clauses.
(e) References to the EU GDPR in the EU SCCs are to be understood as references to the Swiss FADP.

13. United Kingdom

Where either Party is Processing Personal Information that is subject to the UK GDPR, the following applies:

13.1 If a situation applies as described in Article 10.1 of this Privacy Exhibit, but within the context of the UK GDPR, the EU SCCs Module One referred to in paragraph 10.1 of this Privacy Exhibit, as amended by the UK Addendum, shall be deemed automatically incorporated by reference into this Privacy Exhibit and binding upon the Parties, including their respective affiliates.

13.2 The UK Addendum shall amend the EU SCCs as follows:

(a) Table 1. The "start date" will be the date the Agreement enters into force. The "Parties" are the Parties set out in Schedule 1 to this Privacy Exhibit. The Parties' "Key Contact" are the key contacts as described in the Agreement.

(b) Table 2.

Addendum EU SCCs		The 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:				
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	Yes	N/A	N/A			
2	No	N/A	N/A	N/A	N/A	
3	No	N/A	N/A	N/A	N/A	
4	No	N/A	N/A			N/A

(c) Table 3. The "Appendix Information" includes:

Annex 1A: List of Parties: **Schedule 1 to this Privacy Exhibit**

Annex 1B: Description of Transfer: **Schedule 1 to this Privacy Exhibit**

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: **Data Security Exhibit**

Annex III: List of Sub processors (Modules 2 and 3 only): **N/A**

(d) Table 4. Neither party may end the UK Addendum as set out in Section 19 of the UK Addendum.

13.4 The Parties may, without amending the Agreement, substitute the appropriate version of any newly approved UK Addendum for the currently incorporated UK Addendum.

SCHEDULE 1 TO THE PRIVACY EXHIBIT

PART A. LIST OF PARTIES

Data exporter(s):

Name: [SUPPLIER] or [3M Company, acting for and on behalf of itself and its affiliates, including those established in the Member States of the European Union].

Address: [SUPPLIER ADDRESS] or [3M Center, St. Paul, MN 55144]

Activities relevant to the data transferred under the Privacy Exhibit: 3M Company is contracting with the Supplier to provide the services set out in the Agreement.

Contact Information: [SUPPLIER CONTACT] or [EU Data Protection Officer, dpo_eu@mmm.com]

Role (Controller)

Data importer(s):

Name: [SUPPLIER] or [3M Company, acting for and on behalf of itself and its affiliates, including those established in the Member States of the European Union].

Address: [SUPPLIER ADDRESS] or [3M Center, St. Paul, MN 55144]

Activities relevant to the data transferred under the Privacy Exhibit: : 3M Company is contracting with the Supplier to provide the services set out in the Agreement.

Contact Information: [SUPPLIER CONTACT] or [EU Data Protection Officer, dpo_eu@mmm.com]

Location of the Processing:

Role (Controller)

PART B. DESCRIPTION OF TRANSFER

Categories of data subjects whose Personal Information is transferred:

Categories of Personal Information transferred:

Categories of sensitive data including additional measures:

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis):

Nature of the Processing:

Purpose(s) of the data transfer and further Processing:

The period for which the Personal Information will be retained, or, if that is not possible, the criteria used to determine that period:

For transfers to (sub-) processors, also specify subject matter, nature and duration of the Processing:

PART C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority (per Clause 13 of the EU SCCs) is the supervisory authority of the EU/EEA Member State where the Data Exporter is established.