

## LEXMARK CLOUD SERVICES DATA PROCESSING ADDENDUM

This **Lexmark Cloud Services Data Processing Addendum** (the “DPA”) shall be incorporated into and form part of the Lexmark Cloud Services Customer Agreement, and/or any other agreement (“Agreement”) by and between **Lexmark International Technology Sàrl** having offices at **Route de Pré-Bois 20, 1215 Geneva, Switzerland** (“Lexmark”) and Customer as defined in the Agreement, under which Lexmark receives Personal Data in connection with Services it provides to Customer. This DPA shall be considered executed on the date (“Effective Date”) Customer accepts the Lexmark Cloud Services Customer Agreement.

### 1. **DEFINITIONS**

Unless expressly stated to the contrary or where the context requires otherwise, the capitalised terms shall have the meaning given to them herein for the purposes of this DPA. Terms not defined herein shall have the meaning set forth in the Agreement.

**1.1 “Applicable Data Protection Laws”** means any data protection laws or regulations to the extent applicable to the processing of Personal Data under the Agreement, including any binding laws or regulations ratifying, implementing, adopting, supplementing or replacing the foregoing; in each case, to the extent in force, and as such are updated, amended or replaced from time to time.

**1.2 “Authorised Personnel”** means an employee or agent of Lexmark who is authorised to process Personal Data under the authority of Lexmark.

**1.3 “Data Subject Request”** means a request from a Data Subject to exercise their individual rights with respect to their Personal Data, as granted by Applicable Data Protection Laws.

**1.4 “Instructions”** means Customer’s written instructions to Lexmark directing Lexmark to process the Personal Data as provided by Customer under the Agreement, this DPA, or through Customer’s use of the features and functionality of the Services or as otherwise mutually agreed by both parties in writing.

**1.5 “Personal Data”** means any data which is (i) defined as “Personal Data” “Personal Information” “Personally Identifiable Information” or any substantially similar term under Applicable Data Protection Laws and (ii) processed on behalf of Customer by Lexmark (including Authorised Personnel, Sub-processors, or affiliates) in connection with the Agreement.

**1.6 “Personal Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data in Lexmark’s possession or under its control (including when transmitted or stored by Lexmark).

**1.7 “Services”** means the services and/or products as described in the Agreement.

**1.8 “European Standard Contractual Clauses”** or (“EU SCCs”) means the standard contractual clauses approved by the European Commission for the transfer of personal data from the European Economic Area (“EEA”) to processors established in third countries which do not ensure an adequate level of data protection, annexed to the European Commission’s Decision

(EU) 2021/914 of 5 June 2021 currently found at [https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers\\_en](https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en) as may be amended, superseded or replaced.

**1.9 “Sub-processor”** means any person or entity appointed by Lexmark in relation to the processing of Personal Data in connection with the Agreement.

**1.10 “UK International Data Transfer Addendum”** or (“UK Addendum”) to the European Standard Contractual Clauses means the data transfer clauses approved by the UK Secretary of State for Digital, Culture, Media and Sport for the transfer of personal data from the United Kingdom (“UK”) to processors established in third countries which do not ensure an adequate level of data protection, currently found at <https://ico.org.uk/media/for-organizations/documents/4019539/international-data-transfer-addendum.pdf> as may be amended, superseded or replaced.

**1.11 “EU-US Data Privacy Framework”** or (“EU-US DPF”) means the European Commission’s adequacy decision of 10 July 2023, currently found at [https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf\\_en](https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en) as may be amended, superseded or replaced.

In this DPA, the following terms (and any substantially similar terms as defined under Applicable Data Protection Laws) shall have the meanings and otherwise be interpreted in accordance with Applicable Data Protection Law: **Business, Data Controller, Data Processor, Data Subject, Service Provider, Supervisory Authority, process(ing) and transfer.**

### 2. **PROCESSING OF DATA**

**2.1** The parties acknowledge and agree that with respect to processing of Personal Data, Lexmark is a Data Processor and a Service Provider and Customer is a Data Controller and Business, except that where Customer is a Data Processor in which case Lexmark is a Sub-processor of Customer. If Customer is a Data Processor of Personal Data, Customer represents and warrants that Customer’s instructions and processing of Personal Data, including its appointment of Lexmark as a Sub-processor, have been authorised by the respective Data Controller. For the avoidance of doubt, this DPA does not apply to Personal Data for which Lexmark is an independent controller in connection with Lexmark’s legitimate business operations solely when the processing is strictly necessary and proportionate for billing, accountability, customer relationship management (marketing, communication with procurement or sales personnel), related customer communications, complying with and resolving legal obligations, tax requirements, agreements and disputes.

**2.2** This DPA applies where and solely to the extent that Lexmark processes Personal Data on behalf of Customer for the purpose of providing the Services to the Customer pursuant to the Agreement and in accordance with Exhibit A of this DPA and the Instructions (the “Business Purposes”). Where Customer affiliates shall also benefit from the Services under the Agreement and are data controllers or data processors of data which Lexmark processes, Customer acknowledges that it has authority to accept

the terms and conditions of this DPA on their behalf. The subject matter, nature, purpose, and duration of processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit A.

**2.3** Lexmark shall process Personal Data only for the Business Purposes. Lexmark shall promptly notify Customer if an Instruction, in Lexmark's opinion, infringes Applicable Data Protection Laws. Lexmark shall not retain, use or disclose the Personal Data for any purpose other than the Business Purpose or as otherwise expressly permitted by Customer or Applicable Data Protection Laws. To the extent required by Applicable Data Protection Laws, Lexmark certifies that it understands the foregoing restrictions and will comply with them.

**2.4** Customer shall, in its use of the Services, at all times process Personal Data, and provide the Instructions for the processing of Personal Data, in compliance with Applicable Data Protection Laws. Customer represents and warrants that Customer has obtained or will obtain, all necessary consents, licenses and approvals for the processing of Personal Data under this DPA and, where applicable, has a valid legal basis under Applicable Data Protection Laws for the processing of Personal Data under this DPA. Customer further represents and warrants that Customer (i) will comply with all Applicable Data Protection Laws in its performance arising out of this DPA; and (ii) has reviewed Lexmark's security practices and acknowledges that such practices are appropriately designed to ensure a level of security appropriate to the risk of processing hereunder.

**2.5** Following expiration of the Agreement, Lexmark shall return or delete the Personal Data as set forth under the Agreement or applicable service documentation, or provide Customer the ability to delete such Personal Data directly through the tools or functionality made available by the Service. The foregoing obligations shall not apply (a) where deletion is not permitted under applicable law (including Applicable Data Protection Laws) or the order of a governmental or regulatory body; (b) where Lexmark retains such Personal Data for internal record keeping and compliance with any legal obligations; or (c) where Lexmark's then-current data retention or similar back-up system stores Personal Data, provided such data will remain protected in accordance with the measures described in the Agreement and this DPA.

### **3. AUTHORISED PERSONNEL**

**3.1** Lexmark shall ensure that all Authorised Personnel are made aware of the confidential nature of Personal Data and have executed confidentiality agreements or are otherwise subject to binding duties of confidentiality that prohibit them from disclosing or otherwise processing, any Personal Data except in accordance with the Instructions and their obligations in connection with the Services.

**3.2** Lexmark shall take commercially reasonable steps to ensure the reliability and appropriate training of any Authorised Personnel.

### **4. LEXMARK SUB-PROCESSORS**

**4.1** Customer hereby provides Lexmark with general written authorisation to engage Sub-processors to access and

process Personal Data in connection with the Services in accordance with this Section 4.

**4.2** Lexmark Cloud Services Agreed List of Sub-processors (the "Sub-processor List"), which may be updated by Lexmark from time to time, contains Sub-processors that are deemed authorised by Customer to process Personal Data in connection with this DPA for the service locations within the Territory specified in the Agreement. At least thirty (30) days before enabling any new Sub-processor to access or participate in the processing of Personal Data, Lexmark will add such Sub-processor to the Sub-processor List and notify Customer of that update. Customer may object to such an engagement on reasonable data protection grounds by providing notice to Lexmark within twenty (20) days of receipt of the aforementioned notice from Lexmark, otherwise that third party will be deemed an authorised Sub-processor for the purposes of this DPA.

**4.2.1** If Customer objects to an engagement in accordance with Section 4.2, Lexmark shall provide Customer with a written description of commercially reasonable alternative(s), if any, to such engagement. If Lexmark, in its sole discretion, cannot reasonably provide any such alternative(s), or if Customer does not agree to any such alternative(s) if provided, Customer may terminate the impacted Services. If Lexmark undertakes any such alternative, additional costs, if any, shall be borne by Customer. Alternatively, Customer's continued use of the Service following Customer's refusal of the proffered alternative will constitute Customer's consent for such a change to the Sub-processor List. Termination shall not relieve Customer of any fees owed to Lexmark under the Agreement provided that Lexmark has taken commercially reasonable steps to address Customer's objections.

**4.3** Lexmark shall ensure that each Sub-processor is subject to obligations regarding the processing of Personal Data that are substantially similar to those which Lexmark is subject under this DPA.

**4.4** Lexmark shall be liable to Customer for any breach of this DPA caused by the acts or omissions of its Sub-processors.

**4.5** If Customer and Lexmark have entered into the EU SCCs as described in Section 6 (Transfers of Personal Data), the above authorisations will constitute Customer's prior written consent to the subcontracting by Lexmark of the processing of Personal Data if such consent is required under the EU SCCs.

## **5. SECURITY OF PERSONAL DATA**

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Lexmark has implemented and shall maintain appropriate Lexmark Cloud Services Technical and Organisational Measures designed to ensure a level of security appropriate to the risk presented by the processing of the Personal Data.

## **6. TRANSFERS OF PERSONAL DATA**

**6.1** Customer acknowledges and agrees that Lexmark and its Sub-processors may provide the Services from any state,

province, country or other jurisdiction. As such, Customer instructs Lexmark and its Sub-processors to transfer and process Personal Data anywhere in the world where Lexmark or its Sub-processors offer data processing operations. Lexmark will at all times provide an adequate level of protection for the Personal Data processed, in accordance with the requirements of Applicable Data Protection Laws.

**6.2** With regard to countries, regions or territories with Applicable Data Protection Laws requiring a mechanism for valid export of Personal Data (defined as “Limited Transfer Region(s)” and such data “Limited Transfer Data”), neither Lexmark nor its Sub-processors may receive and process such Limited Transfer Data outside of such Limited Transfer Regions unless it or its Sub-processors take measures to adequately protect such data consistent with Applicable Data Protection Laws.

Such measures may include to the extent available and applicable under such laws:

- a) Processing in a country, a territory, or one or more specified sectors that are considered under Applicable Data Protection Laws as providing an adequate level of data protection;
- b) The parties’ agreement to enter into and comply with the EU SCCs and UK SCCs and any successors or amendments to such clauses or such other applicable contractual terms adopted and approved under Applicable Data Protection Laws;
- c) Implementing any other data transfer mechanisms or certifications approved under Applicable Data Protection Laws, including the EU–US DPF.

**6.3** The parties acknowledge and agree that they have, taking into account, without limitation, the Personal Data and third countries in scope, the relevant security measures under this DPA and the relevant parties participating in the processing of such Personal Data, conducted an assessment of the appropriateness of the relevant transfer mechanism adopted hereunder and have determined that such transfer mechanism is appropriately designed to ensure Personal Data transferred in accordance with this DPA a level of protection in the destination country that is essentially equivalent to that guaranteed under the Applicable Data Protection Laws

**6.4** To the extent that any substitute or additional appropriate safeguards or mechanisms under any Applicable Data Protection Laws of Limited Transfer Regions are required to transfer data from a Limited Transfer Region, as applicable, to any third country, the parties agree to implement the same as soon as practicable and document such requirements for implementation in an attachment to this DPA governing the parties’ processing of Limited Transfer Data.

**6.5** In the event the Services are covered by more than one transfer solution, the transfer of Personal Data will be subject to a single transfer solution in accordance with the following order of precedence: (a) the EU SCCs or (b) UK SCCs; and, if neither (a) nor (b) is applicable, then (c) other data transfer solutions permitted under Applicable Data Protection Laws.

**6.6** In connection with European Personal Data the parties agree that the EU SCCs will be incorporated by reference and form part of the Agreement as follows:

a) EEA Transfers. In relation to Personal Data that is subject to the GDPR (i) Customer is the “data exporter” and Lexmark is the “data importer”; (ii) the EU SCC Module Two terms apply to the extent the Customer is a Controller of Personal Data and the EU SCC Module Three terms apply to the extent the Customer is a Processor of Personal Data; (iii) in Clause 7, the optional docking clause applies; (iv) in Clause 9, Option 2 applies and changes to Sub-Processors will be notified in accordance with the ‘Sub-Processors’ section of this DPA; (v) in Clause 11, the optional language is deleted; (vi) in Clauses 17 and 18, the parties agree that the governing law and forum for disputes for the EU SCCs will be determined in accordance with the ‘Contracting Entity; Applicable Law; Notice’ section of the Agreement or, if such section does not specify an EU Member State, the Republic of Ireland (without reference to conflicts of law principles); (vii) the Annexes of the EU SCCs will be deemed completed with the information set out in Exhibit A of this DPA, the Technical and Organisational Measures, and the Sub-processor List; and (viii) if and to the extent the EU SCCs conflict with any provision of this DPA the EU SCCs will prevail to the extent of such conflict.

b) UK Transfers. In relation to European Data that is subject to the UK GDPR, the EU SCCs will apply in accordance with sub-section (a) and the following modifications: (i) the EU SCCs will be modified and interpreted in accordance with the UK Addendum; (ii) Tables 1, 2 and 3 of the UK Addendum will be deemed completed with the information set out in the Annexes of this DPA and Table 4 will be deemed completed by selecting “neither party”; and (iii) any conflict between the terms of the EU SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

c) Swiss Transfers. In relation to European Personal Data that is subject to the Swiss DPA, the EU SCCs will apply in accordance with sub-section (a) and the following modifications (i) references to “Regulation (EU) 2016/679” will be interpreted as references to the DPA; (ii) references to “EU”, “Union” and “Member State law” will be interpreted as references to Swiss law; and (iii) references to the “competent supervisory authority” and “competent courts” will be replaced with the “the Swiss Federal Data Protection and Information Commissioner ” and the “relevant courts in Switzerland”.

**6.7** Where the Lexmark contracting entity under the Agreement is not Lexmark International, Inc., such contracting entity will remain fully and solely responsible and liable to Customer for the performance of the EU SCCs by Lexmark International, Inc., and Customer will direct any instructions, claims or enquiries in relation to the EU SCCs to such contracting entity. If Lexmark cannot comply with its obligations under the EU SCCs or is breach of any warranties under the EU SCCs or UK Addendum (as applicable) for any reason, and Customer intends to suspend the transfer of European Personal Data to Lexmark or terminate the Agreement, Customer agrees to provide

Lexmark with reasonable notice to enable Lexmark to cure such non-compliance and reasonably cooperate with Lexmark to identify what additional safeguards, if any, may be implemented to remedy such non-compliance. If Lexmark has not or cannot cure the non-compliance, Customer may suspend or terminate the affected part of the Service in accordance with the Agreement without liability to either party (but without prejudice to any fees Customer has incurred prior to such suspension or termination).

## **7. DEMONSTRATION OF COMPLIANCE**

Lexmark will make all information reasonably necessary to demonstrate compliance with this DPA available to Customer and allow for and contribute to audits, including inspections conducted by or Customer's auditor to assess compliance with this DPA. Customer acknowledges and agrees that it will exercise its audit rights under this DPA and Clause 8.9 of the Standard Contractual Clauses by instructing Lexmark to comply with the audit measures described in this 'Demonstration of Compliance' section. Customer acknowledges that the Service is hosted by Lexmark's hosting Sub-Processors who maintain independently validated security programs (including SOC 2 and ISO 27001) and that Lexmark's systems are audited annually as part of SOC 2 compliance and regularly tested by independent third-party penetration testing firms. Upon request, Lexmark will supply (on a confidential basis) its SOC 2 report and summary copies of Lexmark's penetration testing report(s) to Customer so that Customer can verify Lexmark's compliance with this DPA. Further, at Customer's written request, Lexmark will provide written responses (on a confidential basis) to all reasonable requests for information made by Customer necessary to confirm Lexmark's compliance with this DPA, provided that Customer will not exercise this right more than once per calendar year unless Customer has reasonable grounds to suspect non-compliance with the DPA. To the extent certifications or reports contain Lexmark confidential information, Lexmark reserves the right to provide Customer with a summary or redacted version of such documentation.

## **8. COOPERATION AND RECORDS REQUESTS**

**8.1** Lexmark shall, to the extent permitted by law, promptly notify Customer following the receipt and verification of a Data Subject Request or shall otherwise advise the Data Subject to submit their Data Subject Request to Customer directly. In either case, Customer will be responsible for responding to such request.

**8.2** At the request of Customer and taking into account the nature of the processing applicable to any Data Subject Request, Lexmark shall apply appropriate technical and organisational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request (i) Customer is itself unable to respond or fulfil the request without Lexmark's assistance and (ii) Lexmark is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Lexmark.

**8.3** Lexmark shall, taking into account the nature of the processing and the information available to Lexmark provide Customer with reasonable cooperation and assistance for Customer to comply with its obligations under Applicable Data Protection Law (and to demonstrate the same), conduct a data protection impact assessment and, respond to any inquiry or

consultation with any Supervisory Authority. The obligations hereunder shall only apply where required of Lexmark by Applicable Data Protection Law and provided that Customer does not otherwise have access to the relevant information or functionality being requested. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Lexmark.

## **9. PERSONAL DATA BREACH**

**9.1** After becoming aware of a Personal Data Breach, Lexmark shall, without undue delay, inform Customer of the Personal Data Breach and take such steps as Lexmark, in its sole discretion, deems necessary and reasonable to remediate such Personal Data Breach (to the extent that remediation is within Lexmark's reasonable control).

**9.2** Lexmark shall, taking into account the nature of the processing and the information reasonably available to Lexmark: (a) provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under Applicable Data Protection Laws with respect to notifying relevant regulators and/or Data Subjects affected by such Personal Data Breach; and (b) provide Customer with information in Lexmark's reasonable control concerning the details of the Personal Data Breach including, as applicable, the nature of the Personal Data Breach, the categories and approximate numbers of Data Subjects and Personal Data records concerned, and the likely consequences of the Personal Data Breach.

**9.3** The obligations described in this Section 9 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer. In no event will Lexmark's cooperation or obligation to report or respond to a Personal Data Breach under this Section be construed as an acknowledgement by Lexmark of any fault or liability with respect to the Personal Data Breach.

**9.4** Notification of a Personal Data Breach, if any, will be delivered to one or more of Customer's business, technical or administrative contracts by any means Lexmark selects, including email. It is Customer's sole responsibility to ensure it provides and maintains accurate contact information at all times.

## **10. GOVERNMENT REQUESTS**

Lexmark undertakes to adopt appropriate technical and organisational measures to protect Personal Data against any interference by a government authority that goes beyond what is necessary in a democratic society to safeguard national security, defence, and public security. In the event that a government authority submits a request for Personal Data, where legally permitted, Lexmark will notify Customer in writing without undue delay and redirect the government entity to request that information directly from Customer. Lexmark certifies that it has not purposefully created, nor knowingly allowed to be created, back doors or similar programming that could be used by third parties to access Personal Data processed under this DPA on its systems by a government authority or created or changed its business processes in a manner that facilitates access to Personal Data processed under this DPA on its systems by government authorities. As part of this effort, Lexmark may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law



enforcement agency, then Lexmark will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Lexmark is legally prohibited from doing so.

## **11. MISCELLANEOUS**

**11.1** Lexmark collects and processes usage data derived from the use of the Services: (a) to provide services to Customer; (b) to address technical issues with the Services; (c) to improve Lexmark's Services and personalised experience; (d) as otherwise described in Lexmark's privacy policy and set out in the Agreement. Usage data is Lexmark's exclusive property.

**11.2** The liability of Lexmark and its respective employees, directors, officers, affiliates, successors, and assigns (the "Lexmark Parties"), arising out of or related to this DPA, whether in contract, tort, or other theory of liability, shall be subject to the "Limitation of Liability" and "Exclusions of Liability" sections

(or their equivalent sections) of the Agreement, and any reference in such section to the liability of Lexmark or the Lexmark Parties means the aggregate liability of the Lexmark Parties under the Agreement and this DPA together.

**11.3** This DPA is without prejudice to the rights and obligations of the parties under the Agreement which will continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Agreement, the terms of this DPA will prevail insofar as the subject matter concerns the processing of Personal Data. In the event of any conflict between the terms of this DPA and the EU SCCs then, only insofar as the EU SCCs apply, the EU SCCs will prevail.

**11.4** Customer and Lexmark each agree that the dispute resolution provisions of the Agreement (including governing law and venue) apply to this DPA, unless otherwise required by Applicable Data Protection Law.

## EXHIBIT A

### DESCRIPTION OF PROCESSING / TRANSFER

#### A. LIST OF PARTIES

DATA EXPORTER	DATA IMPORTER
<u>Name:</u> Customer, as defined in the Agreement	<u>Name:</u> Lexmark International Technology S.à.r.l.
<u>Address:</u> Customer's address, as set out in the Agreement	<u>Address:</u> Route de Pré-Bois 20, 1215 Geneva, Switzerland
<u>Name:</u> See Agreement	<u>Name:</u> Chad Talbott
<u>Position:</u> See Agreement	<u>Position:</u> Chief Privacy Officer
<u>Contact details:</u> See Agreement	<u>Contact details:</u> privacy@lexmark.com
<u>Activities relevant to the transfer:</u> See Section (B) below	<u>Activities relevant to the transfer:</u> See Section (B) below
<u>Signature and date:</u> Per execution on DPA above.	<u>Signature and date:</u> Per execution on DPA above.
<u>Role:</u> Controller	<u>Role:</u> Processor

#### B. DESCRIPTION OF THE PROCESSING/TRANSFER

##### Categories of Data Subjects whose Personal Data is processed/transferred

###### For the Provision of Lexmark Services

- Employees, freelancers, contacts, third-party providers and contractors of customer.
- Permitted/end users and other participants from time-to-time to whom the customer has granted the right to access the Services in accordance with the customer agreement with Lexmark.
- Customers of and individuals with whom those customers communicate with by email and/or instant messaging.
- Other individuals to the extent identifiable in the content of emails or their attachments or in archived content.

##### Categories of personal data processed/transferred

- Basic personal data (for example first name, last name, job title, email address)
- Authentication data (for example username and password)
- Contact information (for example work email and phone number)
- Unique identification numbers and signatures (for example IP addresses)
- Location data (for example, geo-location network data)
- Device identification (for example IMEI-number and MAC address)
- Meta data including sent, to, from, date, time, subject, which may include Personal Data

**Sensitive data processed (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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.**

No sensitive data or special categories of data are intended to be transferred but, in the case of data stored and processed in the provision of the Lexmark services, sensitive data or special categories of data may be contained in the content of or attachments to email and/or instant messaging - content which is not controlled by Lexmark.

##### Frequency of the processing/transfer

Personal data may be transferred on a continuous basis in order to provide the Services under the existing Agreement.

##### Nature of the processing

Personal Data is only processed for the provision of Services as set out in the Agreement and includes the following:

- Technical support and ticket resolution: To communicate and coordinate resolution of support requests;
- Reporting on contract performance: To report on contracted services and resolution activities;
- Security and authentication: To identify and verify the identity of individuals prior to providing access to systems and data, coordinate responses to potential information security events; and
- Administration of systems: To ensure the availability and security of systems.

### **Purpose(s) for which the personal data is processed/transferred**

Personal Data stored and Processed in the provision of Lexmark Services will be processed only to the extent necessary to provide Services for the purposes set out in the Agreement.

### **Duration of the processing**

Personal data is processed for the duration of the Agreement.

### **For transfers to (sub-) processors**

In accordance with the DPA, Lexmark may engage Sub-processors to provide some or all of the Services on Lexmark's behalf or use any current or future subsidiaries, branches or affiliates of Lexmark for the duration of the Agreement. Any such Sub-processors will be permitted to obtain personal data only to provide some or all of the Services Lexmark has engaged them to provide, and they are prohibited from using personal data for any other purpose.

### **C. Competent Supervisory Authority**

<b>Data Exporter</b>	<b>Competent Supervisory Authority</b>
EU/EEA	<p>EU/EEA Supervisory authority applicable to the data export is the EEA country of its establishment.</p> <p>-or-</p> <p>Where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR.</p> <p>-or-</p> <p>Where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the Data Subjects relevant to the transfer are located.</p>
Switzerland	Swiss Federal Data Protection and Information Commissioner
United Kingdom	Information Commissioners Office ("ICO")
All other countries	Pursuant to the Agreement or, where the Agreement is silent, the competent supervisory authority of the country in which the Customer is located.