Client Relationship Agreement for G-Cloud 15

The order of precedence is specified in Framework Schedule 6 (Order Form Template) of the G-Cloud 15 Framework Agreement. The Client Relationship Agreement (CRA) and applicable Attachments and Transaction Documents (TDs) are incorporated into each Call-Off Contract for the G-Cloud 15 Framework Agreement. Where “IBM” is used, it shall mean “Supplier” and where “Client” is used, it shall mean “Buyer” and where “Supplier Terms” is used, it shall mean the Agreement as defined below.

This Client Relationship Agreement (CRA) and applicable Attachments and Transaction Documents are the complete agreement regarding each transaction under this CRA (together, the "Agreement") under which the Client may order Cloud and other Services, (collectively, IBM Products) and third-party services (Non-IBM Products).

Transaction Documents (TDs) provide the specifics of transactions, such as charges and a description of and information about the Product. Examples of TDs include statements of work, service descriptions, ordering documents, supplements, or invoices. There may be more than one TD applicable to a transaction.

Attachments provide supplemental terms that apply across certain types of IBM Products or Non-IBM Products.

In the event of conflict, an Attachment prevails over this CRA, and a TD prevails over both the CRA and any Attachment and only applies to the specific transaction.

1. Services – Cloud Services

a. A Cloud Service is an "as a service" IBM offering that IBM makes available via a network, such as software as a service, platform as a service, infrastructure as a service, or other network delivered services. IBM may also provide other labour-based Services to support use of Cloud Services. IBM Cloud Services shall include all applicable Lots as defined under Framework Schedule 1 (Specification) as acquired under G-Cloud 15 Call-Off Contracts.

b. Cloud Services are designed to be available 24/7, subject to maintenance. IBM will provide advance notice of scheduled maintenance. Technical support and service level commitments, if any, are specified in an Attachment or TD.

c. When IBM accepts Client's order, IBM provides Client the authorisations specified in the TD. IBM provides the facilities, personnel, equipment, software, and other resources necessary to provide Cloud Services. IBM provides generally available user guides and documentation to support Client's use of the IBM Cloud Service.

d. Enabling Software is software that Client downloads to Client systems that facilitates the use of a Cloud Service and will be identified in a TD. Enabling Software is not part of the Cloud Service and Client may use Enabling Software only in connection with use of the Cloud Service and in accordance with any licensing terms specified in a TD. The licensing terms will specify applicable warranties, if any. **Otherwise, Enabling Software is provided as-is, without warranties of any kind.**

e. Client will provide hardware, software, and connectivity to access and use Cloud Services, including any required Client-specific URL addresses and associated certificates.

f. Client's authorised users may access Cloud Services only to the extent of authorisations Client acquires. Client is responsible for use of Cloud Services by any user who accesses the Cloud Services with Client's account credentials.

g. The following acceptable use terms apply for Client's use of the Cloud Services. Cloud Services may not be used to undertake any activity or host Content that: i) is unlawful, fraudulent, harmful, malicious, obscene, or offensive; ii) threatens or violates the rights of others; iii) disrupts or gains (or intends to disrupt or gain) unauthorised access to data, services, networks, or computing environments within or external to IBM; iv) sends unsolicited, abusive or deceptive messages of any type; or v) distributes any form of malware. Client may not use Cloud Services for crypto-mining, unless otherwise agreed by IBM in writing. Client may not: i) reverse engineer any portion of a Cloud Service; ii) assign or resell direct access to a Cloud Service to a third party outside Client’s Enterprise; or iii) combine a Cloud Service with Client's value add to create a Client-branded solution that Client markets to its end user customers unless otherwise agreed by IBM in writing.

1.1 Changes and Withdrawal of IBM Cloud Services

a. At any time and at IBM's discretion, IBM may change Cloud Services, including corresponding published descriptions.

b. The intent of any change will be to: i) make available additional features and functionality; ii) improve and clarify existing commitments; or iii) maintain alignment to current adopted operational and security standards or applicable laws. Changes will not degrade the security or functionality of the Cloud Services.

c. Changes will be effective when published or on the specified effective date. Any Changes that do not meet the conditions specified above will only take effect, and Client accepts, upon: i) a new order; ii) the term renewal date for the Cloud Services that automatically renew; or iii) notification from IBM of the change effective date for ongoing services that do not have a specified term.

d. IBM may withdraw a Cloud Service on 12 months' notice unless stated otherwise in a TD. IBM will continue to provide withdrawn Cloud Services for the remainder of Client's unexpired term or work with Client to migrate to another generally available IBM offering available under the G-Cloud 15 Framework Agreement.

1.2 Term and Termination of Cloud Services

a. The term begins on the date IBM notifies Client that Client can access the Cloud Services. The ordering TD will specify whether the Cloud Services renew automatically, proceed on a continuous use basis, or terminate at the end of the term. For automatic renewal, unless Client provides written notice to not to renew at least 30 days prior to the term expiration date, the Cloud Services will automatically renew for the specified term. For continuous use, the Cloud Services will continue to be available on a month-to-month basis until Client provides 30 days written termination notice to IBM. The Cloud Services will remain available until the end of the calendar month after such 30-day period.

b. IBM may suspend or limit, to the extent necessary, Client's use of a Cloud Service if IBM reasonably determines there is a material breach of Client's obligations, security breach, violation of law, or breach of the acceptable use terms set forth in section 1 above. IBM will provide notice prior to a suspension, as commercially reasonable. If the cause of a suspension can reasonably be remedied, IBM will provide notice of the actions Client must take to reinstate the Cloud Services. If Client fails to take such actions within a reasonable time, IBM may terminate the Cloud Services.

c. Client may terminate a Cloud Service on 30 days' notice: i) at the written recommendation of a government or regulatory agency following a change in either applicable law or the Cloud Services; ii) if a change to the Cloud Services causes Client to be noncompliant with applicable laws; or iii) if IBM notifies Client of a change to the Cloud Services that has a material adverse effect on Client's use of the Cloud Services, provided that IBM will have 90 days to work with Client to minimise such effect. In the event of any such Client termination above or a similar termination of a Non-IBM Product as permitted in the third-party agreement terms, IBM shall refund a portion of any prepaid amounts for the applicable Cloud Service for the period after the date of termination. Client may terminate a Cloud Services for material breach of IBM's obligations by IBM giving notice and reasonable time to comply. If the Cloud Services or Non-IBM Products are terminated for any other reason, Client will pay to IBM, on the date of termination, the total amounts due per the Agreement. Upon termination, IBM may assist Client in transitioning Content to an alternative technology for an additional charge and under separately agreed terms.

2. Services – Other Services

a. Services are project or other labour-based Services, such as consulting, installation, customisation and configuration, maintenance, and remote services IBM provides to Client. When IBM accepts Client's order, IBM will provide or make the Services as described in an Attachment or TD.

2.1 Service Deliverables Ownership and Licensing

a. When IBM provides deliverables, Client will own the copyright in works of authorship that IBM develops for Client as described in a TD (Project Materials). Project Materials exclude Existing Works. Existing Works are works of authorship delivered to Client, but not created, under the TD, and includes any modifications or enhancements of such works made during the performance of the Services. Some Existing Works may be subject to a separate license agreement (Existing Licensed Works).

b. IBM grants Client an irrevocable (subject to Client's payment obligations), nonexclusive, worldwide license to use, execute, reproduce, display, perform and prepare derivatives of Existing Works that are not Existing Licensed Works. IBM retains an irrevocable, nonexclusive, worldwide, paid-up license to use, execute, reproduce, display, perform, sublicense, distribute, and prepare derivative works of Project Materials.

2.2 Services Termination

a. Either party may terminate a Service if a material breach concerning the Service is not remedied within a reasonable time.

b. IBM will provide at least 90 days' notice prior to withdrawal of standard Services offerings.

c. Client agrees to pay charges for Services provided through the effective date of termination.

d. If Client terminates without cause or IBM terminates for breach, Client will:

   (1) meet all minimum commitments;

   (2) pay termination or adjustment charges specified in a TD; and

   (3) pay any additional costs IBM reasonably incurs because of early termination, such as costs relating to subcontracts or resource relocation.

   IBM will take reasonable steps to mitigate any such additional costs.

e. Specific termination rights for a Service may be specified in a TD.

3. Content and Data Protection

a. Content consists of all data, software, and information that Client or its authorised users provides, authorises, makes available or grants access to, or inputs to the Cloud Service or information or data Client may provide, authorise, make available or grant access to, in connection with IBM providing other Services. Client grants the rights and permissions to IBM, its affiliates, and Subcontractors of either, to use, provide, store, and otherwise process Content solely for the purpose of providing the Cloud Services or other Services. Use of the Cloud Services or other Services will not affect Client's ownership or license rights in Content.

b. IBM, its affiliates, and Subcontractors of either may access and use the Content solely for the purpose of providing and managing the applicable Cloud Services or other Services. IBM will treat all Content as confidential by only disclosing to IBM employees and Subcontractors to the extent necessary to provide the Cloud Services or perform other Services.

c. Client is responsible for obtaining all necessary rights and permissions to permit processing of Content in the Cloud Services or to provide other Services. Client will make disclosures and obtain consent required by law before Client provides, authorises or makes available access to or inputs individuals' information, including personal or other regulated data, for processing in the Cloud Services or use in providing the other Services, by IBM, its affiliates or Subcontractors.

d. If any Content could be subject to governmental regulation or may require security measures beyond those specified by IBM for the Cloud Services or to provide other Services, Client will not provide, authorise, allow access to, or input the Content for processing in the Cloud Services or provide or allow access of Content to IBM to provide other Services unless specifically permitted in the applicable TD or unless IBM has first agreed in writing to implement additional security and other measures. Client is responsible for adequate back-up of Content on Client managed systems prior to providing or allowing access of Content to IBM to provide Services.

e. IBM Data Security and Privacy Principles (DSP), at Appendix A, apply for generally available standard IBM Cloud Services and other Services as identified in a TD. At IBM's discretion, IBM may change the DSP from time to time and the change will be effective when published or on the specified effective date. The intent of any change will be to improve and clarify existing commitments and maintain alignment to current adopted operational and security standards or applicable laws. The intent is not to degrade the security or functionality. The most up to date version of the DSP can be found at http://ibm.com/terms/?id=z126-7745.

f. The specific security features and functions of a Cloud Service or other Services will be described in the applicable Attachment and TD. Client is responsible for selecting, ordering, enabling, or using available data protection features appropriate to support Client's use of Cloud Services. Client is responsible for assessing the suitability of the Cloud Services for the Content and Client's intended use or the use of Content with the Services IBM will provide. Client acknowledges that the use of Cloud Services and other Services meet Client's requirements and processing instructions required to comply with applicable laws.

g. IBM's Data Processing Addendum (DPA) is detailed in Appendix B. The DPA and applicable DPA Exhibit(s) apply to IBM’s processing of personal data on behalf of the Client. Each IBM Product has a DPA Exhibit that specifies how IBM will process the Client's data. The applicable DPA Exhibit is included by reference in the TD. The most up to date version of the DPA can be found at http://ibm.com/dpa.

h. For Cloud Services with self-managed features, Client can remove Content at any time. Otherwise, IBM will return or remove Content from IBM computing resources upon the expiration or cancellation of the Cloud Service or other Services, or earlier upon Client's request. IBM may charge for certain activities performed at Client's request (such as delivering Content in a specific format). IBM does not archive Content; however, some Content may remain in backup files until expiration of such files as governed by IBM's backup retention practices.

4. Warranties

a. IBM warrants that it provides Cloud Services and Services using commercially reasonable care and skill and as described in an applicable Attachment or TD, including any completion criteria. Project Materials will comply with the Attachment or TD at the time of delivery. **The warranty for Cloud Services or Services ends when the Cloud Services or Services end.**

b. **These warranties are the exclusive warranties from IBM and replace all other warranties, including the implied warranties or conditions of satisfactory quality, merchantability, non-infringement, and fitness for a particular purpose. IBM does not warrant uninterrupted or error-free operation of an IBM Product or that IBM will correct all defects or prevent third-party disruptions or unauthorised third-party access to an IBM Product. IBM warranties will not apply if there has been misuse, modification, damage not caused by IBM, or failure to comply with written instructions provided by IBM. Non-IBM Products and preview products, or identified non-warranted IBM Products, are sold under the Agreement as-is, without warranties of any kind. Third parties may provide their own warranties to Client for Non-IBM Products.**

5. Charges, Taxes, Payment and Verification

a. Client's right to use IBM Cloud Services or Non-IBM Cloud Services is contingent on Client paying applicable charges as specified in a TD or applicable agreement under which Client acquired the entitlements. Client is responsible to acquire additional entitlements in advance of any increase of its use.

b. Client agrees to pay all applicable charges specified in a TD for an IBM Product or Non-IBM Product and charges for use in excess of authorisations. Charges are exclusive of any customs or other duty, tax, and similar levies imposed by any authority resulting from Client's acquisitions under the Agreement and will be invoiced in addition to such charges. Amounts are due upon receipt of the invoice from IBM and payable within 30 days of the invoice date to an account specified by IBM and late payment fees may apply. Prepaid IBM Products or Non-IBM Products must be used within the applicable period. IBM does not give credits or refunds for any prepaid, one-time charges, or other charges already due or paid, except as may be specified in an Agreement.

c. In the event Client is required to pay any withholding or deduction of tax required under an applicable governmental entity regulation based on IBM’s charge for a cross border transaction, Client will increase the sum payable by the

amount necessary to ensure IBM receives an amount equal to the sum it would have received had no withholdings or deductions been made. Client is responsible to pay any withholding tax directly to the appropriate government entity where required by law.

d. If Client imports, exports, transfers, accesses, or uses an IBM Product or Non-IBM Product across a border, Client agrees to be responsible for and pay authorities any custom, duty, tax, or similar levy assessed by the authorities. This excludes those taxes based on IBM's net income.

e. IBM will invoice: i) recurring charges at the beginning of the selected billing frequency term; ii) overage and usage charges in arrears; and iii) one-time charges upon IBM's acceptance of an order.

f. IBM may change recurring charges, labour rates and minimum commitments on 90 days' notice, except for Cloud Services. For Cloud Services, if IBM commits to pricing as specified in a TD, IBM will not change such pricing during the specified term. If there is not a specified commitment, then IBM may change pricing on thirty days' notice. A change applies on the invoice date or the first day of the charging period or new term on or after the effective date IBM specifies in the notice. IBM may change one-time charges without notice. However, a change to a one-time charge does not apply to an order if: i) IBM receives the order before the announcement date of the increase; and ii) within 90 days after IBM's receipt of the order, the Product is made available to Client.

6. Liability and Intellectual Property Protection

a. IBM's entire liability for all claims related to the Agreement will not exceed the amount of any actual direct damages incurred by Client up to 125% of the amounts paid (if recurring charges, up to 12 months' charges apply) for the Product that is the subject of the claim, regardless of the basis of the claim. **IBM will not be liable for special, incidental, exemplary, indirect, or consequential damages, or lost profits, business, value, revenue, goodwill, or anticipated savings.** These limitations apply collectively to IBM, its affiliates, Subcontractors, and suppliers.

b. The following amounts are not subject to the above cap: i) third-party payments related to infringement claims described in the paragraph c below; and ii) damages that cannot be limited under applicable law.

c. If a third party asserts a claim against Client that an IBM Product acquired under the Agreement infringes a patent or copyright, IBM will defend Client against that claim and pay amounts finally awarded by a court against Client or included in a settlement approved by IBM. To obtain IBM's defense against and payment of infringement claims, Client must promptly: i) notify IBM in writing of the claim; ii) supply information requested by IBM; and iii) allow IBM to control, and reasonably cooperate in, the defense and settlement, including mitigation efforts. IBM's defense and payment obligations for infringement claims extend to claims of infringement based on open-source code that IBM selects and embeds in an IBM Product.

d. IBM has no responsibility for claims based on: i) Non-IBM Products; ii) items not provided by IBM; iii) IBM’s proper use of any Client required third-party product or service related to the administration of the transaction; iv) any violation of law or third-party rights caused by Content or any Client materials, designs, specifications; or v) Client’s use of a non-current version or release of an IBM Product when an infringement claim could have been avoided by using a current version or release.

7. Termination

a. Either party may terminate: i) this CRA without cause on at least 30 days' notice to the other after expiration or termination of its obligations under each Agreement; or ii) immediately for cause if the other is in material breach of an Agreement, provided the non-complying party is given notice and reasonable time to comply. Termination of this CRA does not terminate transactions in effect and not affected by the cause of a material breach and provisions of the Agreement, as they relate to such transactions, remain in effect until fulfilled or otherwise terminated in accordance with the Agreement term.

b. Any terms that by their nature extend beyond the Agreement termination remain in effect until fulfilled and apply to successors and assignees.

c. Each party will allow the other reasonable opportunity to comply before it claims the other has not met its obligations. Client's failure to pay, or Client providing inaccurate or fraudulent account or payment information to acquire IBM Products or Non-IBM Products, is a material breach.

8. Governing Laws and Geographic Scope

a. Both parties agree to the application of the laws of England, without regard to conflict of law principles. Any disputes will be brought before a court of competent jurisdiction within such country.

b. The rights and obligations of each party are valid only in the country where the transaction is performed (or for IBM or Non-IBM Cloud Services or remotely delivered IBM or Non-IBM Services, the country of Client's business address) or, if IBM agrees, the country where the IBM Product or Non-IBM Product is placed in productive use, except all licenses are valid as specifically granted.

c. Each party is also responsible for complying with: i) laws and regulations applicable to its business and Content; and ii) import, export and economic sanction laws and regulations, including the defense trade control regime of the United States of America and any applicable jurisdiction, that prohibit or restrict the import, export, re-export, or transfer of products, technology, services or data, directly or indirectly, to or for certain countries, end uses or end users. IBM will

not serve as Client's exporter or importer, except as required by data protection laws, for: i) any Content; or ii) use of any portion of a Cloud Service from a country outside Client's business address.

d. If any provision of the Agreement is invalid or unenforceable, the remaining provisions remain in full force and effect. Nothing in the Agreement affects statutory rights of consumers that cannot be waived or limited by contract. The United Nations Convention on Contracts for the International Sale of Goods does not apply to transactions under the Agreement.

9. General

a. IBM is an independent contractor, not Client's agent, joint venturer, partner, or fiduciary, and does not undertake to perform any of Client's regulatory obligations or assume any responsibility for Client's business or operations. Client is responsible for its use of IBM Products and Non-IBM Products. IBM is acting as an information technology provider only. IBM's direction, suggested usage, guidance, or Client's use of an IBM Product does not constitute medical, clinical, legal, accounting, or other licensed professional advice. Client should obtain its own expert advice. Each party is responsible for determining the assignment of its and its affiliates personnel and their respective Subcontractors, and for their direction, control, and compensation.

b. Client may not use IBM Products or Non-IBM Products if failure or interruption of the IBM Products or Non-IBM Products could lead to death, serious bodily injury, or property or environmental damage.

c. Parties will not disclose confidential information to employees or Subcontractors of the other party without a separate, signed confidentiality agreement. If confidential information is exchanged in connection with the Agreement, the applicable confidentiality agreement is incorporated into, and subject to, this CRA. This paragraph does not apply to Content provided in the use of an IBM Cloud Service or Non-IBM Cloud Service.

d. Client accepts an Attachment or TD by ordering, enrolling, using, or making a payment for, the IBM Product or Non-IBM Product. Since this CRA may apply to many future orders, IBM may change this CRA by providing Client at least 90 days' written notice. Changes are not retroactive. They will only apply as of the effective date to: i) new orders; ii) ongoing or continuous IBM Product or Non-IBM Product offerings that do not expire; and iii) renewals. For transactions with a defined renewable contract period stated in a TD, Client may request that IBM defer the change effective date until the end of the current contract period. Client accepts changes by placing new orders or continuing use after the change effective date or allowing transactions to renew after receipt of the change notice. Except as specifically provided in this CRA or as specified in an Attachment or TD, all changes to an Agreement must be in writing signed by both parties.

e. IBM maintains a robust set of business conduct and related guidelines covering conflicts of interest, market abuse, anti-bribery and corruption, and fraud. IBM and its personnel comply with such policies and require Subcontractors to have similar policies.

f. IBM, its affiliates, and Subcontractors of either require use of business contact information and certain account usage information. This information is not Content. Business contact information is used to communicate and manage business dealings with the Client. Examples of business contact information include name, business telephone, address, email, user ID, and tax registration information. Account usage information is required to enable, provide, manage, support, administer, and improve IBM Products. Examples of account usage information include reported errors and digital information gathered using tracking technologies, such as cookies and web beacons, during use of IBM Products. The IBM Privacy Statement at https://www.ibm.com/privacy/ provides additional details with respect to IBM's collection, use, and handling of business contact and account usage information. When Client provides information to IBM and notice to, or consent by, the individuals is required for such processing, Client will notify individuals and obtain consent.

g. IBM may offer Non-IBM Products, or an IBM Product may enable access to Non-IBM Product, that may require acceptance of third-party terms presented to the Client. Linking to or use of Non-IBM Products constitutes Client's agreement with such terms. Third-party terms and privacy practices govern use of a Non-IBM Cloud Service or other Service, including Content Client may provide, grant access to or input to. IBM will invoice Client for charges due and submit Client's order details to the third-party provider for the enablement and delivery of the Non-IBM Product. IBM is not a party to any third-party agreement and is not responsible for Non-IBM Products. Access to ongoing Non-IBM Products may be discontinued at any time if the third party discontinues or IBM no longer makes available such Non-IBM Products.

h. An IBM Product or Non-IBM Product or feature of an IBM Product or Non-IBM Product is considered "preview product" when IBM makes such product or features available at no charge, with limited or pre-release functionality, or for a limited time, to try available functionality (such as beta, trial, evaluation, no-charge, or designated preview products). Service level agreements, if any, do not apply to preview products. A preview product may not be covered by support and IBM may change or discontinue a preview product at any time and without notice. For any preview product that is provided as pre-release, IBM is not obligated to release a generally available product. Client is responsible to return a preview product or place an order under generally available terms for acquiring IBM Product or Non-IBM Product beyond the preview period. IBM may provide Client opportunities to voluntarily provide feedback in connection with the use of IBM Products, which IBM may use for any purpose.

i. Neither party may assign the Agreement, in whole or in part, without the prior written consent of the other. IBM may assign rights to receive payments. IBM will remain responsible to perform its obligations. Assignment by IBM in

conjunction with the sale of the portion of IBM's business that includes an IBM Product or Non-IBM Product is not restricted. IBM may share an Agreement and related documents in conjunction with any assignment.

j. All notices under the Agreement must be in writing and sent to the business address specified for the Agreement unless a party designates in writing a different address. The parties consent to the use of electronic means and facsimile transmissions for communications as a signed writing. Any reproduction of the Agreement made by reliable means is considered an original. The Agreement supersedes any course of dealing, discussions, or representations between the parties. Where approval, acceptance, consent, access, cooperation, or similar action by either party is required, such action will not be unreasonably delayed or withheld.

k. No right or cause of action for any third party is created by the Agreement or any transaction under it. Neither party will bring a legal action arising out of or related to the Agreement more than two years after the cause of action arose. Neither party is responsible for failure to fulfil its non-monetary obligations due to causes beyond its control.

l. IBM may use personnel and resources in locations worldwide, including Subcontractors to support the delivery of IBM Products and Non-IBM Products. Client's use of IBM Products or Non-IBM Products may result in the transfer of Content, including personally identifiable information, across country borders. A list of countries where Content may be transferred and processed is described in the applicable TD or support documentation. IBM is responsible for the obligations under the Agreement even if IBM uses a Subcontractor and will have appropriate agreements in place to enable IBM to meet its obligations.

m. If IBM and Client agree to use a Client requested third-party service to support the procurement or payment activities associated with an Agreement, IBM agrees to submit or receive applicable documents (such as invoices or similar contracting documents) using the third-party service. In the event: i) the third-party service becomes unavailable for any reason; or ii) the third-party provider modifies the service or terms of use in a manner IBM deems commercially unacceptable, the Client agrees to directly accept documents. Client remains responsible to IBM for timely payments of invoices and for any claims or proceedings related to the third-party service provider's failure to comply with applicable laws or for such provider's use, misuse, or disclosure of data or confidential information. IBM agrees to promptly notify Client in writing of any such claim or proceeding.

Agreed to:	Agreed to:
Client Company Name (Client):	IBM Company (IBM): IBM United Kingdom Limited
By_____ Authorised signature	By_____ Authorised signature
Title:	Title:
Name (type or print):	Name (type or print):
Date:	Date:
Client number:	Agreement number:
Enterprise number:	
Client address:	IBM address: Registered in England and Wales with number 741598 Registered Office: Building C, IBM Hursley Office, Hursley Park Road, Winchester, Hampshire, United Kingdom, SO21 2JN

Appendix A - IBM Data Security and Privacy Principles

1. Definitions

Capitalized terms used herein have the meanings given below or if not defined below, the meanings given in the applicable written contract between IBM and Client for the IBM Services.

Client – is the entity to which IBM is providing the IBM Services under an IBM Services Document.

Components – are the application, platform, or infrastructure elements of an IBM Service that IBM operates and manages.

Content – consists of all data, software, and information that Client or its authorized users provide, authorize access to, or input to IBM Services.

DSP – is this IBM Data Security and Privacy Principles document.

IBM Cloud Services – are "as a service" IBM offerings that IBM makes available via a network, such as software as a service, platform as a service, or infrastructure as a service.

IBM Services Document – is a Transaction Document and any other document that is incorporated into a written contract between IBM and a Client and that addresses details of a specific IBM Service.

IBM Services – are (a) IBM Cloud Services, (b) other IBM service offerings, including infrastructure or application service offerings that IBM delivers and dedicates to or customizes for a Client, and (c) any other services, including consulting, maintenance, or support, that IBM provides to a Client.

Security Incident – is an unauthorized access and unauthorized use of Content.

Transaction Document – is a document that details the specifics of transactions, such as charges and a description of and information about an IBM Cloud Service. Examples of Transaction Documents include statements of work, service descriptions, ordering documents and invoices for an IBM Cloud Service. There may be more than one Transaction Document applicable to a transaction.

2. Overview

The technical and organizational measures provided in this DSP apply to IBM Services (including any Components) only where IBM has expressly agreed to comply with the DSP in a written contract between IBM and Client. For clarity, those measures do not apply where Client is responsible for security and privacy or as specified below or in an IBM Services Document.

a. Client is responsible for determining whether an IBM Service is suitable for Client's use and implementing and managing security and privacy measures for components that IBM does not provide or manage within the IBM Services. Examples of Client responsibilities for IBM Services include: (1) the security of systems and applications built or deployed by the Client upon an infrastructure as a service or platform as a service offering or upon infrastructure, Components or software that IBM manages for a Client, and (2) Client end-user access control and application level security configuration for a software as a service offering that IBM manages for a Client or an application service offering that IBM delivers to a Client.

b. Client acknowledges that IBM may modify this DSP from time to time at IBM's sole discretion and such modifications will replace prior versions as of the date that IBM publishes the modified version. Notwithstanding anything to the contrary in any written contract between IBM and Client, the intent of any modification will be to: (1) improve or clarify existing commitments, (2) enable IBM to appropriately prioritize its security focus to address evolving data and cybersecurity threats and issues, (3) maintain alignment to current adopted standards and applicable laws, or (4) provide additional features and functionality. Modifications will not degrade the security or data protection features or functionality of IBM Services.

c. In the event of any conflict between this DSP and an IBM Services Document, the IBM Services Document will prevail and if the conflicting terms are in a Transaction Document, they will be identified as overriding the terms of this DSP and will only apply to the specific transaction.

3. Data Protection

a. IBM will treat all Content as confidential by not disclosing Content except to IBM employees, contractors, and suppliers (including subprocessors), and only to the extent necessary to deliver the IBM Services.

b. Security and privacy measures for each IBM Service are implemented in accordance with IBM's security and privacy by design practices to protect Content processed by an IBM Service, and to maintain the availability of such Content pursuant to the applicable written contract between IBM and Client, including applicable IBM Services Documents.

c. Additional security and privacy information specific to an IBM Service may be available in the relevant IBM Services Document or other standard documentation to aid in Client's initial and ongoing assessment of an IBM Service's suitability for Client's use. Such information may include evidence of stated certifications and accreditations, information related to such certifications and accreditations, data sheets, FAQs, and other generally available documentation. IBM will direct Client to available standard documentation if asked to complete Client-preferred security or privacy questionnaires.

4. Security Policies

a. IBM will maintain and follow written IT security policies and practices that are integral to IBM's business and mandatory for all IBM employees. The IBM Chief Information Security Officer will maintain responsibility and executive oversight for such policies, including formal governance and revision management, employee education, and compliance enforcement.

b. IBM will review its IT security policies at least annually and amend such policies as IBM deems reasonable to maintain protection of IBM Services and Content.

c. IBM will maintain and follow its standard mandatory employment verification requirements for all new hires and will extend such requirements to wholly-owned IBM subsidiaries. In accordance with IBM internal processes and procedures, these requirements will be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks as deemed necessary by IBM. Each IBM company is responsible for implementing these requirements in its hiring process as applicable and permitted under local law.

d. IBM employees will complete IBM's security and privacy education annually and certify each year that they will comply with IBM's ethical business conduct, confidentiality, and security policies, as set out in IBM's Business Conduct Guidelines. Additional training will be provided to any persons granted privileged access to Components that is specific to their role within IBM's operation and support of the IBM Services, and as required to maintain compliance and accreditations stated in any relevant IBM Services Document.

5. Compliance

a. For standard (non-custom) IBM Cloud Services, the measures implemented and maintained by IBM within each IBM Cloud Service will be subject to annual certification of compliance with ISO 27001 or SSAE SOC 2, or both, unless stated otherwise in an IBM Services Document.

b. Additionally, IBM will maintain compliance and accreditation for the IBM Services as defined in an IBM Services Document.

c. Upon request, IBM will provide evidence of the compliance and accreditation required by 5a. and 5b., such as certificates, attestations, or reports resulting from accredited independent third-party audits (accredited independent third-party audits will occur at the frequency required by the relevant standard).

d. IBM is responsible for these data security and privacy measures even if IBM uses a contractor or supplier (including subprocessors) in the delivery or support of an IBM Service.

6. Security Incidents

a. IBM will maintain and follow documented incident response policies consistent with National Institute of Standards and Technology, United States Department of Commerce (NIST) guidelines or equivalent industry standards for computer security incident handling and will comply with the data breach notification terms of the applicable written contract between IBM and Client.

b. IBM will investigate Security Incidents of which IBM becomes aware, and, within the scope of the IBM Services, IBM will define and execute an appropriate response plan. Client may notify IBM of a suspected vulnerability or incident by submitting a request through the incident reporting process specific to the IBM Service (as referenced in an IBM Services Document) or, in the absence of such process, by submitting a technical support request.

c. IBM will notify Client without undue delay upon confirmation of a Security Incident that is known or reasonably suspected by IBM to affect Client. IBM will provide Client with reasonably requested information about such Security Incident and the status of any IBM remediation and restoration activities.

7. Physical Security and Entry Control

a. IBM will maintain appropriate physical entry controls, such as barriers, card-controlled entry points, surveillance cameras, and manned reception desks, to protect against unauthorized entry into IBM managed facilities (data centers) used to host the IBM Services. Auxiliary entry points into such data centers, such as delivery areas and loading docks, will be controlled and isolated from computing resources.

b. Access to IBM-managed data centers and controlled areas within those data centers will be limited by job role and subject to authorized approval. Such access will be logged, and such logs will be retained for not less than one year. IBM will revoke access to IBM-managed data centers upon separation of an authorized employee. IBM will follow formal documented separation procedures that include prompt removal from access control lists and surrender of physical access badges.

c. Any person granted temporary permission to enter an IBM-managed data center facility or a controlled area within such a data center will be registered upon entering the premises, must provide proof of identity upon registration, and will be escorted by authorized personnel. Any temporary authorization to enter, including deliveries, will be scheduled in advance and require approval by authorized personnel.

d. IBM will take precautions to protect the physical infrastructure of IBM managed data center facilities against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

8. Access, Intervention, Transfer and Separation Control

a. IBM will maintain a documented security architecture for Components. IBM will separately review such security architecture, including measures designed to prevent unauthorized network connections to systems, applications and network devices, for compliance with its secure segmentation, isolation, and defense-in-depth standards prior to implementation.

b. IBM may use wireless networking technology in its maintenance and support of the IBM Services and associated Components. Such wireless networks, if any, will be encrypted and require secure authentication and will not provide direct access to IBM Cloud Services networks. IBM Cloud Services networks do not use wireless networking technology.

c. IBM will maintain measures for an IBM Service that are designed to logically separate and prevent Content from being exposed to or accessed by unauthorized persons. IBM will maintain appropriate isolation of its production and non-production environments, and, if Content is transferred to a non-production environment, for example to reproduce an error at Client's request, security and privacy protections in the non-production environment will be equivalent to those in production.

d. IBM will encrypt Content not intended for public or unauthenticated viewing when transferring Content over public networks and enable use of a cryptographic protocol, such as HTTPS, SFTP, or FTPS, for Client's secure transfer of Content to and from the IBM Services over public networks.

e. IBM will encrypt Content at rest if and as specified in an IBM Services Document. If an IBM Service includes management of cryptographic keys, IBM will maintain documented procedures for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use.

f. If IBM requires access to Content to provide the IBM Services, and if such access is managed by IBM, IBM will restrict access to the minimum level required. Such access, including administrative access to any underlying Components (privileged access), will be individual, role-based, and subject to approval and regular validation by authorized IBM personnel following the principles of segregation of duties. IBM will maintain measures to identify and remove redundant and dormant accounts with privileged access and will promptly revoke such access upon the account owner's separation or upon the request of authorized IBM personnel, such as the account owner's manager.

g. Consistent with industry standard practices, and to the extent natively supported by each Component, IBM will maintain technical measures enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, password change frequency, and secure transfer and storage of such passwords and passphrases.

h. IBM will monitor use of privileged access and maintain security information and event management measures designed to: (1) identify unauthorized access and activity, (2) facilitate a timely and appropriate response, and (3) enable internal and independent third-party audits of compliance with documented IBM policy.

i. Logs in which privileged access and activity are recorded will be retained in compliance with IBM's worldwide records management plan. IBM will maintain measures designed to protect against unauthorized access, modification, and accidental or deliberate destruction of such logs.

j. To the extent supported by native device or operating system functionality, IBM will maintain computing protections for its end-user systems that include, but may not be limited to, endpoint firewalls, full disk encryption, signature-based malware detection and removal, time-based screen locks, and endpoint management solutions that enforce security configuration and patching requirements.

k. IBM will securely sanitize physical media intended for reuse prior to such reuse, and will destroy physical media not intended for reuse, consistent with NIST guidelines for media sanitization.

9. Service Integrity and Availability Control

a. IBM will: (1) perform security and privacy risk assessments of the IBM Services at least annually, (2) perform security testing and vulnerability assessments of the IBM Services before production release and at least annually thereafter, (3) enlist a qualified independent third party, IBM X-Force™ or, if specified in an IBM Services Document, another qualified testing service to perform penetration testing of the IBM Cloud Services, at least annually, (4) perform automated vulnerability scanning of underlying Components of the IBM Services against industry security configuration best practices, (5) remediate identified vulnerabilities from security testing and scanning, based on associated risk, exploitability, and impact, and (6) take reasonable steps to avoid disruption to the IBM Services when performing its tests, assessments, scans, and execution of remediation activities.

b. IBM will maintain measures designed to assess, test, and apply security advisory patches to the IBM Services and associated systems, networks, applications, and underlying Components within the scope of the IBM Services. Upon determining that a security advisory patch is applicable and appropriate, IBM will implement the patch pursuant to documented severity and risk assessment guidelines, based on Common Vulnerability Scoring System ratings of

patches, when available. Implementation of security advisory patches will be subject to IBM change management policy.

c. IBM will maintain policies and procedures designed to manage risks associated with the application of changes to IBM Services. Prior to implementation, changes to an IBM Service, including its systems, networks, and underlying Components, will be documented in a registered change request that includes a description of and reason for the change, implementation details and schedule, a risk statement addressing impact to the IBM Service and its clients, expected outcome, rollback plan, and documented approval by authorized personnel.

d. IBM will maintain an inventory of all information technology assets used in its operation of IBM Services. IBM will continuously monitor and manage the health, including capacity, and availability of IBM Services and underlying Components.

e. Each IBM Service will be separately assessed for business continuity and disaster recovery requirements through appropriate business impact analysis and risk assessments intended to identify and prioritize critical business functions. Each IBM Service will have, to the extent warranted by such risk assessments, separately defined, documented, maintained, and annually validated business continuity and disaster recovery plans consistent with industry standard practices. Recovery point and time objectives for an IBM Service, if provided for in the relevant IBM Services Document, will be established with consideration given to the IBM Service's architecture and intended use. Physical media intended for off-site storage, if any, such as media containing backup files, will be encrypted prior to transport.

Appendix B - Data Processing Addendum

This Data Processing Addendum (DPA) and its applicable DPA Exhibits apply to the Processing of Personal Data by IBM on behalf of Client (Client Personal Data) in order to provide services (Services) pursuant to the Agreement between Client and IBM. This DPA is incorporated into the Agreement and the DPA Exhibits for each Service will be provided in the applicable Transaction Document (TD). In the event of conflict, the DPA Exhibit prevails over the DPA which prevails over the rest of the Agreement.

Capitalized terms used have the meanings given below.

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing Personal Data.

Data Subject means a natural person who can be identified, directly or indirectly.

Data Protection Laws means all legislation and regulations applicable to the Processing of Personal Data under the Agreement.

Non-Adequate Countries means countries not providing an adequate level of data protection pursuant to Data Protection Laws or a decision of a Supervisory Authority.

Personal Data means any information relating to a Data Subject.

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Client Personal Data.

Process or **Processing** means any operation or set of operations performed on Client Personal Data, including storage, use, access and reading.

Processor means a natural or legal person which Processes Client Personal Data on behalf of Client.

Subprocessor means any other Processor IBM engages to Process Client Personal Data.

Supervisory Authority means an independent public authority responsible for monitoring the application of the applicable Data Protection Laws.

1. Processing

1.1 Client is either (a) a Controller of Client Personal Data; or (b) a Processor acting on behalf of other Controllers and has been instructed by and obtained the authorization of the relevant Controller(s) for the Processing of Client Personal Data by IBM as Client's subprocessor. Client appoints IBM as Processor to Process Client Personal Data. If there are other Controllers, Client will identify and inform IBM if required by the applicable Data Protection Laws.

1.2 A list of categories of Data Subjects, types of Client Personal Data and Processing activities is set out in the applicable DPA Exhibit for each Service. The duration of the Processing corresponds to the duration of the Service. The purpose and subject matter of the Processing is the provision of the Service as described in the Agreement.

1.3 IBM will Process Client Personal Data to provide and secure the Service according to Client's documented instructions or as otherwise set out in the Agreement. The scope of Client's instructions for the Processing of Client Personal Data is defined by the Agreement, and, if applicable, by Client's use of the features of the Service.

When providing Services, IBM will not further combine, use, retain or disclose Client Personal Data outside of the direct business relationship between IBM and Client or for any purpose other than to perform the Services and business purposes specified in the Agreement. IBM will not sell or share Client Personal Data as required by the applicable Data Protection Laws.

1.4 Client may provide further instructions regarding the Processing of Client Personal Data (Additional Instructions) as described in Section 10.2 and IBM will use commercially reasonable efforts to follow them.

If IBM notifies Client that an Additional Instruction is not feasible or that IBM can no longer meet its obligations as Processor, the parties shall work together to find an alternative. If IBM notifies Client that no alternative is feasible, Client may terminate the affected Service, in accordance with the Agreement. If IBM believes an instruction violates the applicable Data Protection Laws, IBM will notify Client, and may suspend the performance of such instruction until Client has modified or confirmed its lawfulness in documented form.

1.5 Client shall serve as a single point of contact for IBM and exercise any rights of other Controllers on their behalf, obtaining necessary permissions. IBM is discharged from informing or notifying other Controllers when IBM has informed or notified Client. IBM will also serve as a single point of contact for Client for its obligations as a Processor under this DPA.

1.6 Each party will comply with its respective obligations under the applicable Data Protection Laws for the processing of Client Personal Data and is responsible for determining the requirements of laws or regulations applicable to its own business. Client will not use the Services in a manner that would violate applicable Data Protection Laws.

2. Technical and Organizational Measures

Client and IBM agree that IBM will implement and maintain the technical and organizational measures set forth in the applicable DPA Exhibit (TOMs) which ensure a level of security appropriate to the risk for IBM's scope of responsibility. TOMs are subject to technical progress and further development. Accordingly, IBM reserves the right to modify the TOMs provided that the functionality and security of the Services are not degraded.

3. Data Subject Rights and Requests

IBM will notify Client of Data Subjects requests addressed directly to IBM, where the Data Subject has provided information to identify Client. If not, IBM will direct the Data Subject to Client. Client shall be responsible to handle such requests with IBM providing reasonable assistance under Section 10.2.

4. Third Party Requests and Confidentiality

4.1 IBM will not disclose Client Personal Data to any third party, unless authorized by the Client or required by law. If a government or Supervisory Authority demands access to Client Personal Data:

a. IBM will notify Client of such request to enable Client to take all necessary actions to communicate directly with the relevant authority and respond to such request.

b. If IBM is prohibited by law to notify Client of such request, it will make best reasonable efforts to challenge such prohibition and it commits to providing the minimum amount of information permissible when responding, based on a reasonable interpretation of the order.

c. IBM will provide to Client general information relative to any such request received from a government or Supervisory Authority during the preceding 12-month period.

4.2 IBM requires all of its personnel authorized to Process Client Personal Data to commit themselves to the requirements of this section.

5. Audit

Subject to the appropriate confidentiality and Section 10.2, IBM shall allow for, and contribute to, audits conducted by Client or another auditor mandated by Client, who shall be not a direct competitor of IBM, including inspections to the extent required by the applicable Data Protection Laws, in accordance with the following procedures:

a. IBM will provide Client or its mandated auditor with the most recent certifications and/or summary audit report(s), which IBM has procured to regularly test, assess and evaluate the effectiveness of the TOMs.

b. IBM will reasonably cooperate with Client by providing available additional information concerning the TOMs, to help Client better understand such TOMs.

c. If further information is needed by Client to comply with its own or other Controllers audit obligations or a competent Supervisory Authority's request, Client will inform IBM in writing to enable IBM to provide such information or to grant access to it.

d. To the extent it is not possible to otherwise satisfy an audit right mandated by applicable law or expressly agreed by the Parties, only legally mandated entities (such as a governmental regulatory agency having oversight of Client's operations), Client or its mandated auditor may conduct an onsite visit of the IBM facilities used to provide the Service, during normal business hours and only in a manner that causes minimal disruption to IBM's business, subject to coordinating the timing of such visit in order to reduce any risk to IBM's other customers.

6. Return or Deletion of Client Personal Data

Upon termination or expiration of the Agreement IBM will either delete or return Client Personal Data in its possession as set out in the respective DPA Exhibit, unless otherwise required by applicable law.

7. Subprocessors

7.1 Client authorizes the engagement of the Subprocessors listed in the respective DPA Exhibit. IBM will notify Client in advance of any addition or replacement of the Subprocessors, as reported in the applicable DPA Exhibit or in the Agreement. Within 30 days after IBM's notification, Client may object in writing stating specific reasons and possible mitigations, if any. If Client does not object within such period, the Subprocessor may process Client Personal Data. IBM shall impose substantially similar but no less protective data protection obligations as set out in this DPA on any approved Subprocessor prior to the Subprocessor initiating any Processing of Client Personal Data.

7.2 If Client reasonably objects to a Subprocessor and IBM cannot reasonably accommodate the objection, IBM will notify Client. Client may terminate the affected Services, otherwise the parties shall cooperate to find a feasible solution in accordance with the dispute resolution process, as set out in the Agreement, if applicable.

8. Transborder Data Processing and Country Required Terms

8.1 In the case of a transfer of Client Personal Data to Non-Adequate Countries, the parties shall cooperate to ensure compliance with the applicable Data Protection Laws by relying on the Transborder Data Processing document available at https://www.ibm.com/support/customer/csol/terms/?id=Z126-8005 or this DPA, as applicable. If Client believes the measures are not sufficient to satisfy the legal requirements, Client shall notify IBM and the parties shall work together to find an alternative.

8.2 Depending on the applicable Data Protection Laws, the parties can be subject to additional country required terms available at https://www.ibm.com/support/customer/csol/terms/?id=Z126-8005 (Country Required Terms).

9. Personal Data Breach

IBM will notify Client without undue delay after becoming aware of a Personal Data Breach with respect to the Services. IBM will promptly investigate the Personal Data Breach if it occurred on IBM infrastructure or in another area IBM is responsible for and will assist Client as set out in Section 10.

10. Assistance

10.1 IBM will assist Client by technical and organizational measures for the fulfillment of Client's obligation to comply with Data Subjects rights, security of Processing, Personal Data Breach notification and data protection impact assessment, including prior consultation with the responsible Supervisory Authority, if required, taking into account the nature of the processing and the information available to IBM.

10.2 Client will make a written request for any assistance, or any Additional Instructions, under this DPA. The parties shall reasonably cooperate to find a feasible solution in accordance with the Agreement.

EU Data Act Terms

The provisions set forth in the EU Data Act Terms apply to:

1. the access to and use of Product Data and Related Services Data ("Data") (Section 1. Data Access and Use); and

2. the Switching process between Data Processing Services (Section 2. Switching Data Processing Services)

in accordance with REGULATION (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on the harmonized rules on fair access to and use of data ("Data Act").

The EU Data Act Terms are incorporated into the Agreement and in the event of a conflict, their provisions prevail over the rest of the Agreement.

Capitalized terms not defined in the EU Data Act Terms have the meanings given to them in the Data Act and the Agreement.

1. Data Access and Use

1.1. Information Relating to Data

IBM provides information about the Data required to be provided to Client under Article 3 of the Data Act on the applicable IBM Documentation page labeled "EU Data Act" (the "Data Information Page").

1.2. IBM Use

Client agrees that IBM may use the Data for the purposes of: performing the Agreement; monitoring, supporting and maintaining the IBM Machine or Services; improving the performance or function of any product or service offered by IBM; assisting Client with planning; developing new features, functions, or products or services offered by IBM; and aggregating Data with other data and creating derived data for any lawful purpose. Client agrees that IBM may use the Data to assess claims related to the above purposes. Client agrees that IBM may share the Data with third parties under contract with IBM only for the above purposes.

1.3. Data Access by Client

a. IBM will make the Data accessible to Client in accordance with the Data Act. The means by which Client can access the Data is set forth on the Data Information Page.
b. IBM may unilaterally change Data specifications or the way Data can be accessed. Changes may include, but are not limited to, technical modification of any delivery method, the IBM Machine or Related Service. Client may be required to agree to additional contract terms or other protective measures. IBM will provide Client with reasonable notice of such changes on the Data Information Page.

2. Switching Data Processing Services

2.1. Client may, subject to Client's payment obligations under the Agreement, terminate the Agreement by initiating the Switching in accordance with the terms described herein.

2.2. To initiate the Switching, Client shall submit a written notice at least two (2) months in advance. For submitting the notice Client will use the established communication channels, such as the Cloud Services portal or by opening a Service Support Case. Upon expiration of the notice period, the parties shall enter into a transitional period of thirty (30) calendar days to discuss the details of the Switching. Following the transitional period, a retrieval phase of thirty (30) calendar days shall commence.

2.3. Within fourteen (14) working days of Client initiating the Switching IBM may notify Client in writing that the transitional period is technically unfeasible and indicate an alternative transitional period, which shall not exceed seven (7) months.

2.4. Upon written notice from Client to be provided to IBM, Client may request IBM to extend the transitional period once during the Switching, as soon as practicable.

2.5. Within the notice period, Client shall notify IBM without undue delay of its intention to perform one or more of the following actions: (a) switch to a Data Processing Service provided by another provider with related information, or (b) port its Exportable Data and Digital Assets to an on-premises ICT infrastructure or (c) erase its Exportable Data and Digital Assets.

2.6. IBM shall inform Client of the categories of data and Digital Assets (if any) that will be ported during the Switching, including those data that are not portable due to the exemption under the Data Act.

2.7. IBM shall support Client's exit strategy by providing relevant information, also related to continuity risks, and reasonable assistance, including by maintaining business continuity and adherence to IBM Data Security and Privacy Principles (DSP) throughout the Switching.

2.8. The Agreement is intended terminated when: (a) the Switching is successfully complete or (b) when Client indicates during the notice period that Client does not wish to switch, but to erase its Exportable Data and Digital Assets. IBM will notify Client accordingly.

2.9. IBM will delete all Exportable Data and Digital Assets in accordance with the provisions set forth in the" Deletion and Return of Content" section of the relevant Data Sheet(s).