Data Processing Addendum (DPA) and Data Security and Privacy Principles (DSPP) Including DPA exhibits for Product Families

for the provision by Responsiv Solutions Limited of all products and services.

Part number **RL000CQ v2.1**

August 2023 Edition

This document consolidates and supersedes all versions and editions published prior to August 2023 of the Responsiv Data Processing Addendum (DPA), Data Security and Privacy Principles (DSPP), and provides standardised DPA exhibits for Responsiv Cloud, Responsiv Assist (Support), and Responsiv Consulting product Families.

responsiv

simple · effective · distinctive

TABLE OF CONTENTS

1 RESPONSIV DATA PROCESSING ADDENDUM

This Data Processing Addendum (DPA) and associated specific Data Processing clauses defined in the Entitlement and/or Product Description (DPA Exhibits) apply to the Processing of Personal Data by Responsiv on behalf of Customer (Customer Personal Data) subject to the General Data Protection Regulation 2016/679 (GDPR) or any other relevant data protection laws identified from time to time (together 'Data Protection Laws') in order to provide services (Services) pursuant to the Agreement between Customer and Responsiv.

1.1 PRECEDENCE

1.1.1 DPA Exhibits for each Service will be provided in the applicable Transaction Document (TD) or attached in this document.

1.1.2 This DPA is incorporated into the Agreement. Capitalised terms used and not defined herein have the meanings given them in the applicable Data Protection Laws.

1.1.3 In the event of conflict, the DPA Exhibit prevails over the DPA which prevails over the rest of the Agreement.

1.2 PROCESSING

1.2.1 Customer is: (a) Controller of Customer Personal Data; or (b) acting as Processor on behalf of other Controllers and has been instructed by and obtained the authorisation of the relevant Controller(s) to agree to the Processing of Customer Personal Data by **Responsiv as Customer's sub-processor** as set out in this DPA.

1.2.1.1 Customer appoints Responsiv as Processor to Process Customer Personal Data.

1.2.1.2 If there are other Controllers, Customer will identify and inform Responsiv of any such other Controllers prior to providing their Personal Data, in accordance with the DPA Exhibit.

1.2.2 A list of categories of Data Subjects, types of Customer Personal Data, Special Categories of Personal Data and the processing activities is set out in the applicable DPA Exhibit for a Service. The duration of the Processing corresponds to the duration of the Service, unless otherwise stated in the DPA Exhibit. The purpose and subject matter of the Processing is the provision of the Service as described in the Agreement.

1.2.3 Responsiv will Process Customer Personal Data according to Customer's documented instructions. The scope of Customer's instructions for the Processing of Customer Personal Data is defined by the Agreement, and, if applicable, Customer's and its authorised users' use and configuration of the features of the Service. Customer may provide further legally required instructions regarding the Processing of Customer Personal Data (Additional Instructions) as described in Section 1.11.2. If Responsiv notifies Customer that an Additional Instruction is not feasible, the parties shall work together to find an alternative. If Responsiv notifies the Customer that neither the Additional Instruction nor an alternative is feasible, Customer may terminate the affected Service, in accordance with any applicable terms of the Agreement. If Responsiv believes an instruction violates the Data Protection Laws, Responsiv will immediately inform Customer, and may suspend the performance of such instruction until Customer has modified or confirmed its lawfulness in documented form.

1.2.4 Customer shall serve as a single point of contact for Responsiv. As other Controllers may have certain direct rights against Responsiv, Customer undertakes to exercise all such rights on their behalf and to obtain all necessary permissions from the other Controllers. Responsiv shall be discharged of its obligation to inform or notify another Controller when Responsiv has provided such information or notice to Customer. Similarly, Responsiv will serve as a single point of contact for Customer with respect to its obligations as a Processor under this DPA.

1.2.5 Responsiv will comply with all Data Protection Laws in respect of the Services applicable to Responsiv as Processor. Responsiv is not responsible for determining the requirements of laws or regulations applicable to Customer's business, or that a Service meets the requirements of any such applicable laws or regulations. As between the parties, Customer is responsible for the lawfulness of the Processing of the Customer Personal Data. Customer will not use the Services in a manner that would violate applicable Data Protection Laws.

1.3 TECHNICAL AND ORGANISATIONAL MEASURES

1.3.1 Customer and Responsiv agree that Responsiv 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 Responsiv's scope of responsibility. TOMs are subject to technical progress and further development. Accordingly, Responsiv reserves the right to modify the TOMs provided that the functionality and security of the Services are not degraded.

1.4 DATA SUBJECT RIGHTS AND REQUESTS

1.4.1 Responsiv will inform Customer of requests from Data Subjects exercising their Data Subject rights (e.g., including but not limited to rectification, deletion and blocking of data) addressed directly to Responsiv regarding Customer Personal Data. Customer shall be responsible to handle such requests of Data Subjects. Responsiv will reasonably assist Customer in handling such Data Subject requests in accordance with Section 1.11.2.

1.4.2 If a Data Subject brings a claim directly against Responsiv for a violation of their Data Subject rights, Customer will reimburse Responsiv for any cost, charge, damages, expenses, or loss arising from such a claim to the extent that Responsiv has notified Customer about the claim and given Customer the opportunity to cooperate with Responsiv in the defense and settlement of the claim. Subject to the terms of the Agreement, Customer may claim from Responsiv damages resulting from Data Subject claims for a violation of their Data Subject rights caused by Responsiv's breach of its obligations under this DPA and the respective DPA Exhibit.

1.5 THIRD PARTY REQUESTS AND CONFIDENTIALITY

1.5.1 Responsiv will not disclose Customer Personal Data to any third party, unless authorised by the Customer or required by law. If a government or Supervisory Authority demands access to Customer Personal Data, Responsiv will notify Customer prior to disclosure, unless such notification is prohibited by law.

1.5.2 Responsiv requires all its personnel authorised to Process Customer Personal Data to commit themselves to confidentiality and not Process such Customer Personal Data for any other purposes, except on instructions from Customer or unless required by applicable law.

1.6 AUDIT

1.6.1 Responsiv shall allow for, and contribute to, audits, including inspections, conducted by the Customer or another auditor mandated by the Customer in accordance with the following procedures:

1.6.1.1 Upon Customer's written request, Responsiv will provide Customer or its mandated auditor with the most recent certifications and/or summary audit report(s), which Responsiv has procured to regularly test, assess, and evaluate the effectiveness of the TOMs, to the extent set out in the DPA Exhibit.

1.6.1.2 Responsiv will reasonably cooperate with Customer by providing available additional information concerning the TOMs, to help Customer better understand such TOMs.

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

1.6.2 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 Customer's operations), the Customer or its mandated auditor may conduct an onsite visit of the Responsiv facilities used to provide the Service, during normal business hours and only in a manner that causes minimal disruption to Responsiv's business, subject to coordinating the timing of such visit and in accordance with any audit procedures described in the DPA Exhibit in order to reduce any risk to Responsiv's other customers.

1.6.3 Any other auditor mandated by the Customer shall not be a direct competitor of Responsiv regarding the Services and shall be bound to an obligation of confidentiality.

1.6.4 Each party will bear its own costs in respect of paragraphs 1.6.1.1 and 1.6.1.2 of Section 1.6.1, otherwise Section 1.11.2 applies accordingly.

1.7 RETURN OR DELETION OF CUSTOMER PERSONAL DATA

1.7.1 It is the Customer's responsibility to arrange for recovery of their Customer Personal Data prior to termination or expiration of the Agreement. Responsiv will make reasonable efforts support extraction of Customer Personal Data.

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

1.8 SUB-PROCESSORS

1.8.1 Customer authorises the engagement of other Processors to Process Customer Personal Data (Sub-processors). A list of the current Sub-processors is set out in the respective DPA Exhibit. Responsiv will notify Customer in advance of any addition or replacement of the Sub-processors as set out in the respective DPA Exhibit. Within 30 days after Responsiv's notification of the intended change, Customer can object to the addition of a Sub-processor on the basis that such addition would cause Customer to violate applicable legal requirements. Customer's objection shall be in writing and include Customer's specific reasons for its objection and options to mitigate, if any. If Customer does not object within such period, the respective Sub-processor may be commissioned to Process Customer Personal Data. Responsiv shall impose substantially similar but no fewer protective data protection obligations as set out in this DPA on any approved Sub-processor prior to the Sub-processor initiating any Processing of Customer Personal Data.

1.8.2 If Customer legitimately objects to the addition of a Sub-processor and Responsiv cannot reasonably accommodate Customer's objection, Responsiv will notify Customer. Customer may terminate the affected Services as set out in the Agreement, otherwise the parties shall cooperate to find a feasible solution in accordance with the dispute resolution process.

1.9 TRANSBORDER DATA PROCESSING

1.9.1 In the case of a transfer of Customer Personal Data to a country not providing an adequate level of protection pursuant to the Data Protection Laws (Non-Adequate Country), the parties shall cooperate to ensure compliance with the applicable Data Protection Laws as set out in the following Sections. If Customer believes the measures set out below are not sufficient to satisfy the legal requirements, Customer shall notify Responsiv, and the parties shall work together to find an alternative.

1.9.2 By entering into the Agreement, Customer is entering into EU Standard Contractual Clauses as set out in the applicable DPA Exhibit (EU SCC) with (i) each Sub-processor listed in the respective DPA Exhibit that is located in a Non-Adequate Country (Responsiv Data Importers) and (ii) Responsiv, if located in a Non- Adequate Country, as follows:

1.9.2.1 if Customer is a Controller of all or part of the Customer Personal Data, Customer is entering into the EU SCC in respect to such Customer Personal Data; and

1.9.2.2 if Customer is acting as Processor on behalf of other Controllers of all or part of the Customer Personal Data, then Customer is entering into the EU SCC:

1.9.2.2.1 as back-to-back EU SCC in accordance with Clause 11 of the EU Standard Contractual Clauses (Back-to-Back SCC), if Customer has entered separate EU Standard Contractual Clauses with the Controllers; or on behalf of the other Controller(s).

1.9.2.2.2 Customer agrees in advance that any new Responsiv Data Importer engaged by Responsiv in accordance with Section 1.8 shall become an additional data importer under the EU SCC and/or Back-to-Back SCC.

1.9.2.3 If a Sub-processor located in a Non-Adequate Country is not an Responsiv Data Importer (Third Party Data Importer) and EU SCC are entered into in accordance with Section 1.9.2, then, Responsiv or a Responsiv Data Importer shall enter into Back-to-Back SCC with such a Third Party Data Importer. Otherwise, Customer on its own behalf and/or, if required, on behalf of other Controllers shall enter separate EU Standard Contractual Clauses or Back-to-Back SCC as provided by Responsiv.

1.9.2.4 If Customer is unable to agree to the EU SCC or Back-to-Back SCC on behalf of another Controller, as set out in section 1.9.2 and 1.9.2.3, Customer will procure the agreement of such other Controller to enter into those agreements directly. Additionally, Customer agrees and, if applicable, procures the agreement of other Controllers that the EU SCC or the Back-to-Back SCC, including any claims arising from them, are subject to the terms set forth in the Agreement, including the exclusions and limitations of liability. In case of conflict, the EU SCC and Back-to-Back SCC shall prevail.

1.10 Personal Data Breach

1.10.1 Responsiv will notify Customer without undue delay after becoming aware of a Personal Data Breach with respect to the Services. Responsiv will promptly investigate the Personal Data Breach if it occurred on Responsiv infrastructure or in another area Responsiv is responsible for and will assist Customer as set out in Section 1.11.

1.11 Assistance

1.11.1 Responsiv will assist Customer by technical and organizational measures for the fulfilment of Customer's obligation to comply with the rights of Data Subjects and in ensuring compliance with Customers obligations relating to the security of Processing, the notification and communication of a Personal Data Breach and the 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 Responsiv.

1.11.2 Customer will make a written request for any assistance referred to in this DPA. Responsiv may charge Customer no more than a reasonable charge to perform such assistance or an Additional Instruction, such charges to be set forth in a quote and agreed in writing by the parties, or as set forth in an applicable change control provision of the Agreement. If Customer does not agree to the quote, the parties agree to reasonably cooperate to find a feasible solution in accordance with the dispute resolution process.

1.12 Sub processors

Responsiv may use the following Sub processors in the Processing of Client Personal Data:

IBM, Microsoft, Amazon Web Services, Google, Redcentric, TD-SYNNEX, and Responsiv Partners and suppliers as needed.

This agreed list of Sub processors may be amended or altered from time to time, in writing, by the Parties, in accordance with the established PCR process as outlined in the SOW. Responsiv will notify Client of any intended changes to Sub processors by publishing changes the website listed within this section.

1.13 Technical and Organizational Measures

1.13.1 The technical and organizational measures (TOMs) applicable to Responsiv Products and Services are described in Responsiv Data Security and Privacy Principles (DSPP) later in this document. Specific provisions are indicated as part of the product family or specific entitlement Data Processing Addendum (DPA).

1.13.2 Client confirms its obligation to implement appropriate TOMs within its own area of responsibility as required by applicable Data Protection Laws.

1.14 Data Privacy Officer and Other Controllers

1.14.1 Client is responsible for providing complete, accurate and up-to-date information about its data privacy officer and each other Controllers (including their data privacy officer) by notifying Responsiv via the established project change request (PCR) process for the engagement. The Responsiv privacy contact can be contacted at Infosec@responsiv.co.uk

2 Responsiv Data Security and Privacy Principles (DSPP)

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

2.1 Acceptance

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

security configuration for a software as a service offering that Responsiv manages for a Customer or an application service offering that Responsiv delivers to a Customer.

2.1.2 Customer acknowledges that Responsiv may modify this DSPP from time to time at Responsiv's sole discretion and such modifications will replace prior versions as of the date that Responsiv publishes the modified version. Notwithstanding anything to the contrary in any written contract between Responsiv and Customer, the intent of any modification will be to: (1) improve or clarify existing commitments, (2) enable Responsiv to appropriately prioritise 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 Responsiv Services.

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

2.2 DEFINITIONS

2.2.1 Capitalised terms used herein have the meanings given below or if not defined below, the meanings given in the applicable written contract between Responsiv and Customer for the Responsiv Services.

2.2.2 **Customer** – is the entity to which Responsiv is providing the Responsiv Services under a Responsiv Services Document.

2.2.3 **Components** – are the application, platform, or infrastructure elements of a Responsiv Service that Responsiv operates and manages.

2.2.4 **Content** – consists of all data, software, and information that Customer or its authorised users provide, authorise access to, or input to Responsiv Services.

2.2.5 **DSPP** – is this Responsiv Data Security and Privacy Principles document.

2.2.6 **Responsiv Cloud Services** – are "as a service" or “as a platform” Responsiv offerings that Responsiv makes available via a network, such as software as a service, platform as a service, or infrastructure as a service.

2.2.7 **Responsiv Services Document** – is a Transaction Document and any other document that is incorporated into a written contract between Responsiv and a Customer and that addresses details of a specific Responsiv Service.

2.2.8 **Responsiv Services** – are (a) Responsiv Cloud Services, (b) other Responsiv service offerings, including infrastructure or application service offerings that Responsiv delivers and dedicates to or customises for a Customer, and (c) any other services, including consulting, maintenance, or support, that Responsiv provides to a Customer.

2.2.9 **Security Incident** – is an unauthorised access and unauthorised use of Content.

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

2.3 DATA PROTECTION

2.3.1 Responsiv will treat all Content as confidential by not disclosing Content except to Responsiv employees, contractors, and suppliers (including sub-processors), and only to the extent necessary to deliver the Responsiv Services.

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

2.3.3 Additional security and privacy information specific to a Responsiv Service may be available in the relevant Responsiv Services Document or other standard documentation to aid in Customer's initial and ongoing assessment of a Responsiv Service's suitability for Customer's use. Responsiv will direct Customer to available standard documentation if asked to complete Customer-preferred security or privacy questionnaires.

2.4 BUSINESS CONTINUITY

2.4.1 Customer is responsible for their own data backup, and associated recovery of Customer Content, in the event of disaster situation.

2.5 SECURITY POLICIES

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

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

2.5.3 Responsiv will maintain and follow its standard mandatory employment verification requirements for all new hires. In accordance with Responsiv 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 Responsiv.

2.5.4 Responsiv employees will complete Responsiv's security and privacy education annually. Additional training will be provided to any persons granted privileged access to Components that is specific to their role within Responsiv's operation and support of the Responsiv Services, and as required to maintain compliance and accreditations stated in any relevant Responsiv Services Document

2.6 COMPLIANCE

2.6.1 For standard (non-custom) Responsiv Cloud Services, the measures implemented and maintained by Responsiv within each Responsiv Cloud Service will be subject to annual review and where applicable, penetration tests.

2.6.2 Additionally, Responsiv will maintain compliance and accreditation for the Responsiv Services as defined in a Responsiv Services Document.

2.6.3 Upon request, Responsiv will provide evidence of the compliance and accreditation required by 2.6.1. and 2.6.2, 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).

2.6.4 Responsiv is responsible for these data security and privacy measures even if Responsiv uses a contractor or supplier (including sub-processors) in the delivery or support of a Responsiv Service.

2.7 SECURITY INCIDENTS

2.7.1 Responsiv will maintain and follow documented incident response policies consistent with industry standard practices or equivalent industry standards for computer security incident handling and will comply with the data breach notification terms of the applicable written contract between Responsiv and Customer.

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

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

2.8 PHYSICAL SECURITY AND ENTRY CONTROL

2.8.1 Responsiv Services are hosted on industry recognised cloud platforms including, but not limited to, IBM Cloud, Microsoft Azure, Amazon AWS, Google Cloud. All physical security and entry controls will be managed by our cloud platform providers in line with their published policies. Responsiv will assist Customers identify information relating to the policies published by our cloud platform providers in this area so that the Customer can assure themselves of the suitability of the platform to meet their specific requirements.

2.9 ACCESS, INTERVENTION, TRANSFER AND SEPARATION CONTROL

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

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

2.9.3 Responsiv will maintain measures for a Responsiv Service that are designed to logically separate and prevent Content from being exposed to or accessed by unauthorised persons. Responsiv 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 Customer's request, security and privacy protections in the non-production environment will be equivalent to those in production.

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

2.9.5 If requested by the Customer and to the extent supported by the products, Responsiv will encrypt Content at rest and restrict access using ACL if and as specified in a Responsiv Services Document. If a Responsiv Service includes management of cryptographic keys, Responsiv will maintain documented procedures for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use.

2.9.6 If Responsiv requires access to Content to provide the Responsiv Services, and if such access is managed by Responsiv, Responsiv 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 authorised Responsiv personnel following the principles of segregation of duties. Responsiv 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 authorised Responsiv personnel, such as the account owner's manager.

2.9.7 Consistent with industry standard practices, and to the extent natively supported by each Component, Responsiv 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.

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

2.9.9 To the extent supported by native device or operating system functionality, Responsiv 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.

2.10 SERVICE INTEGRITY AND AVAILABILITY CONTROL

2.10.1 Responsiv will: (1) perform security and privacy risk assessments of the Responsiv Services at least annually, (2) perform security testing and vulnerability assessments of the Responsiv Services before production release and at least annually thereafter, (3) enlist a qualified independent third party, or, if specified in a Responsiv Services Document, another qualified testing service to perform penetration testing of the Responsiv Cloud Services, at least annually, (4) perform automated vulnerability scanning of underlying Components of the Responsiv 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 Responsiv Services when performing its tests, assessments, scans, and execution of remediation activities.

2.10.2 Responsiv will maintain measures designed to assess, test, and apply security advisory patches to the Responsiv Services and associated systems, networks, applications, and underlying Components within the scope of the Responsiv Services. Upon determining that a security advisory patch is applicable and appropriate, Responsiv will implement the patch pursuant to 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 Responsiv change management policy.

2.10.3 Responsiv will maintain policies and procedures designed to manage risks associated with the application of changes to Responsiv Services. Prior to implementation, changes to a Responsiv 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 Responsiv Service and its clients, expected outcome, rollback plan, and documented approval by authorised personnel.

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

2.10.5 Each Responsiv Service will be separately assessed for business continuity and disaster recovery requirements through appropriate business impact analysis and risk assessments intended to identify and prioritise critical business functions. Each Responsiv 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 a Responsiv Service, if provided for in the relevant Responsiv Services Document, will be established with consideration given to the Responsiv Service's architecture and intended use.

DPA exhibits for Product Families

3 DPA: CONSULTING SERVICES

3.1.1 This Data Processing Addendum Exhibit (DPA Exhibit) specifies the DPA for the identified service family.

3.2 PROCESSING

3.2.1 Responsiv will process Client Personal Data for the Services, as described in TD (SoW) and as provided by this DPA Exhibit. Duration of Processing is the duration of the Services being provided unless as otherwise set out in the related Statement of Work (SOW).

3.3 PROCESSING ACTIVITIES

3.3.1 The processing activities using Client Personal Data are specified in the TD and may include:

3.3.1.1 Receipt of Client Personal Data from Client and/or other third parties

3.3.1.2 Computer processing of Personal Data, including data transmission, data retrieval, data access, Transformation, Manipulation (parsing, formatting, or transformation) of data, Masking and pseudonymization to make it more difficult to identify individuals or anonymization such that individuals cannot be identified, and network access to allow data transfer if required.

3.3.1.3 Technical testing of computing environments when this testing results in access to Client Personal Data

3.3.1.4 Monitoring of computing environments for security threats when this monitoring results in access to Client Personal Data

3.3.1.5 Reading data, Presenting, accessing, using or copying data, sharing with third parties, Storage of data including backups, Deletion of data

3.3.1.6 Transformation and transition of Client Personal Data as necessary to deliver the Services.

3.4 CLIENT PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS

3.4.1 Data Subjects associated with Client Personal Data that are processed as part of the Service include Client employees, customers, business partners, and suppliers.

3.4.2 Given the nature of the Services, Client acknowledges that Responsiv is not able to verify or maintain the above list of Categories of Data Subjects. Therefore, Client will notify Responsiv about any required changes of the list above by updating the related Statement of Work (SOW) via the established Project Change Request (PCR). Responsiv will process Personal Data of all Data Subjects listed above in accordance with the Agreement. If changes to the list of Categories of Data Subjects require changes of the agreed Processing, Client shall provide Additional Instructions to Responsiv as set out in the DPA.

3.5 TYPES OF PERSONAL DATA

3.5.1 The following list sets out what Types of Client Personal Data may be processed within the Services. Any deviations to the following list to be processed will be explicitly stated within the related SOW.

3.5.1.1 Business Contact Information (name, address, phone number, email.).

3.5.1.2 Technically Identifiable Personal Data (device IDs, usage identifiers, IP addresses, all when linked to an individual).

3.5.1.3 Employment-Related Personal Data (HR data, including job history, performance review information.)

3.5.1.4 Location Information (geolocation data associated with an individual)

3.6 SPECIAL CATEGORIES OF PERSONAL DATA

No Special Categories of Personal Data will be provided to Responsiv by the Client unless specifically provided in writing (such Special Categories of Personal Data include, but are not limited to, Personal Data related to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, genetic data, or biometric data). In the case that Special Categories of Personal Data are included for processing, the Client will notify Responsiv of the data type(s) in question, in writing by amendment to the SOW. Responsiv will confirm the data types and assess any subsequent impact on the provision of the Services via the established Project Change Control (PCR) process and the specific data type(s) will be explicitly stated within the related SOW.

3.7 DELETION AND RETURN OF CLIENT PERSONAL DATA

3.7.1 Responsiv will delete Client Personal Data at the end of the Services subject to the following:

3.7.1.1 Content (including Customer Personal Data) that is stored or persisted within Cloud Services will become unavailable within 30 days after termination or expiration of the Cloud Service.

3.7.1.2 Content (including Customer Personal Data) that is stored or persisted within the Responsiv Service Desk will remain indefinitely for audit and review purposes.

3.7.1.3 Content (including Customer Personal Data) may remain in the Cloud Service and Service Desk backups until the expiration of such backups no more than 360 days after data is collected.

4 DPA: SOFTWARE AND CLOUD SUPPORT SERVICES

4.1.1 This Data Processing Addendum Exhibit (DPA Exhibit) specifies the DPA for the identified service family.

4.2 PROCESSING

4.2.1 Responsiv will process Client Personal Data for the Service, as described in the Agreement, including the DPA and this DPA Exhibit. The duration of the Processing will be for a period of one year after the close of each individual request for Service.

4.3 PROCESSING ACTIVITIES

4.3.1 The processing activities using Client Personal Data are specified in the TD and may include:

4.3.1.1 Receipt of Client Personal Data from Client and/or other third parties

4.3.1.2 Computer processing of Personal Data, including data transmission, data retrieval, data access, Transformation, Manipulation (parsing, formatting, or transformation) of data, Masking and pseudonymization to make it more difficult to identify individuals or anonymization such that individuals cannot be identified, and network access to allow data transfer if required.

4.3.1.3 Technical testing of computing environments when this testing results in access to Client Personal Data

4.3.1.4 Monitoring of computing environments for security threats when this monitoring results in access to Client Personal Data

4.3.1.5 Reading data, Presenting, accessing, using, or copying data, sharing with third parties, Storage of data including backups, Deletion of data.

4.4 CLIENT PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS

4.4.1 Data Subjects associated with Client Personal Data that are processed as part of the Service include Client employees (including temporary or casual workers, volunteers, assignees, trainees, retirees, candidates, applicants), customers, prospects, interested parties, business partners, and suppliers.

4.4.2 Given the nature of the Services, Client acknowledges that Responsiv is not able to verify or maintain the above list of Categories of Data Subjects. Therefore, Client will notify Responsiv about any required changes of the list above by updating the related Statement of Work (SOW) via the established Project Change Request (PCR). Responsiv will process Personal Data of all Data Subjects listed above in accordance with the Agreement. If changes to the list of Categories of Data Subjects require changes of the agreed Processing, Client shall provide Additional Instructions to Responsiv as set out in the DPA.

4.5 SPECIAL CATEGORIES OF PERSONAL DATA

4.5.1 No Special Categories of Personal Data will be provided to Responsiv by the Client unless specifically provided in writing (such Special Categories of Personal Data include, but are not limited to, Personal Data related to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, genetic data, or biometric data). In the case that Special Categories of Personal Data are included for processing, the Client will notify Responsiv of the data type(s) in question, in writing by amendment to the SOW. Responsiv will confirm the data types and assess any subsequent impact on the provision of the Services via the established Project Change Control (PCR) process and the specific data type(s) will be explicitly stated within the related SOW.

4.6 TYPES OF PERSONAL DATA AND SPECIAL CATEGORIES OF PERSONAL DATA

4.6.1 Given the nature of the Services, Client acknowledges that Responsiv is not able to review data provided by Client to determine if it contains any Client Personal Data including Special Categories of Personal Data outside the list set out in Section 2 above or as may be provided by the Client.

4.6.2 Therefore, Client is responsible to provide Responsiv with, and keep updated, lists of Personal Data and Special Categories of Personal Data that Responsiv can have access to during the Service.

4.6.3 In the absence of other instructions from Client, Responsiv will assume that during the Services Responsiv can have access, even incidentally, to all types of data provided by Client.

4.6.4 The technical and organization measures above will be used by Responsiv to safeguard all type of Client Personal Data. If changes to the above lists require changes of the agreed Processing, Client shall provide Additional Instructions to Responsiv as set out in the DPA.

4.7 DELETION AND RETURN OF CLIENT PERSONAL DATA

4.7.1 Responsiv will delete Client Personal Data at the end of the Services subject to the following:

4.7.1.1 Content (including Customer Personal Data) that is stored or persisted within Cloud Services will become unavailable within 30 days after termination or expiration of the Cloud Service.

4.7.1.2 Content (including Customer Personal Data) that is stored or persisted within the Responsiv Service Desk will remain indefinitely for audit and review purposes.

4.7.1.3 Content (including Customer Personal Data) may remain in the Cloud Service and Service Desk backups until the expiration of such backups no more than 360 days after data is collected.

5 END OF DOCUMENT