Data Processing Addendum for Quadient Impress Cloud Services (United Kingdom)

This Data Processing Addendum forms part of the main contract (made of the agreement entitled "End User License Agreement for Quadient Impress Cloud Services (United Kingdom)" dated as of 17.07.2021 and as amended or updated from time to time (the **"Main Contract")**

between

the Licensee as defined under the Main Contract

– hereinafter referred to as the Controller –

and

Quadient UK Limited, company number 02658324)

at 3rd Floor Press Centre, Here East, 14 East Bay Lane, London, E15 2GW

– hereinafter referred to as the Processor –

Preamble

This Data Processing Addendum details the obligations of the parties related to the protection of data resulting from the scope of the processing of personal data on behalf of Controller as defined in detail in the Main Contract. It shall apply to all activities within the scope of and related to the Main Contract, and in whose context the Processor's employees or a third party acting on behalf of the Processor may come into contact with personal data of the Controller.

1. Definitions

The terms, 'personal data' (or 'data'), 'processing', 'supervisory authority', 'data subject', 'member state' and 'transfer' shall have the same meaning as in the UK GDPR as defined in section 3(10) (and supplemented by section 205(4) of the Data Protection Act 2018 or "**the UK GDPR**"), and their cognate terms shall be construed accordingly.

2. Subject Matter, Duration, and Specification of the Data Processing

The subject matter and duration of this Data Processing Addendum shall be as defined in the Main Contract. Except where this Data Processing Addendum expressly stipulates any surviving obligation, the term of this Data Processing Addendum shall follow the term of the Main Contract.

Data processing shall include the following data:

Type of personal data	Type and purpose of data processing	Categories of data subjects
a) Names *b) Addresses* *c) Email Addresses* *d) Phone No.* *e) Communication content* *f) IP address and log history, User Data*	*The type and purpose of processing is for performance of the Quadient Cloud Services (customer communication and data quality services) as defined in the Main Contract.*	*The categories of data subjects comprise:* *a) employees including contingent workers, consultants, contractors* *b) clients, including prospects institutional clients and/or counterparty representatives* *c) authorized signatories* *d) professional advisers, agents, experts* *e) third-party vendors* *f) recipients of customer communication*

The processing of personal data shall be carried out exclusively within a member state of the EU or EEA or an adequate country. Each and every transfer of data to a country which is not a member state of either the EU or EEA or regarded as an adequate country, requires the prior consent of the Controller and shall only occur if the specific conditions of Article 44 et seq. UK GDPR have been fulfilled. If the Processor contracts such a transfer with the current EU Standard Contractual Clauses (EU Model Clauses), there shall be no separate prior consent required.

3. Scope of Application and Responsibility

(a) Processor shall process personal data on behalf of Controller. The foregoing shall include the activities enumerated and detailed in the Main Contract and its scope of the cloud services. Within the scope of the Main Contract, Controller shall be responsible for complying with the UK GDPR and/or other EU or applicable individual member state data protection provisions, hereinafter referred to as "**regulations on data protection**", including but not limited to the lawfulness of the transmission to the Processor and the lawfulness of processing personal data (Controller shall be the "responsible body" as defined in Article 4(7) of the GDPR).

(b) The instructions shall initially be specified in the Main Contract and may, from time to time thereafter, be amended, amplified, or replaced (individual instructions) as specified by Controller by individual instructions in writing or in electronic form (text form). Instructions that are not provided for in the Main Contract shall be handled as a change request. Verbal instructions must be immediately confirmed in writing or in text form.

4. Obligations of Processor

(a) Processor shall collect, process, and use data related to data subjects only in compliance with UK GDPR, and/or any other applicable Data Protection Law, within the scope of the Main Contract and the written processing instructions issued by Controller, except if it is an exceptional case within the meaning of Article 28(3) of the GDPR. Processor shall immediately notify Controller if it thinks that an instruction violates applicable laws. Processor may suspend implementation of the instruction until it is confirmed or amended by Controller.

(b) Within Processor's area of responsibility, Processor shall structure its internal organisation so it complies with the specific requirements of the protection of personal data. Processor shall implement and maintain technical and organisational measures to adequately protect Controller's data against misuse and loss in accordance with the requirements of the GDPR (in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR). Processor shall implement technical and organisational measures to ensure the confidentiality, integrity, availability, and resilience of the systems and services in the long term with respect to the processing of personal data as described in Appendix 1 of this Data Processing Addendum (Technical and Organisational Measures). Controller is aware of these technical and organisational measures and has no concerns as to their adequate level of protection for the risks of the data to be processed.

(c) Processor reserves the right to change the security measures, although it must ensure that they do not fall below the contractually agreed level of protection or the requirements of UK GDPR and Data Protection Law.

(d) Processor shall assist Controller within the scope of its abilities in addressing the inquiries and needs of data subjects in accordance with Chapter III of the GDPR as well as adherence to the obligations specified in Articles 33 to 36 of the GDPR. For this purpose, the parties may agree on an arrangement regarding compensation in the Main Contract.

(e) Processor shall ensure that any personnel entrusted with processing Controller's personal data and other persons working for Processor are prohibited from processing the data other than as instructed. Furthermore, Processor shall ensure that any personnel entrusted with processing Controller's personal data have agreed to maintain data secrecy or are subject to a statutory obligation to maintain confidentiality. The obligation to maintain data secrecy/confidentiality shall continue even after termination of the activities.

(f) Processor shall, without undue delay, inform Controller of any material breach of the regulations on data protection for the protection of Controller's personal data. Processor shall consult with Controller about it without delay and shall implement the agreed measures necessary to secure the data and to mitigate potential adverse effects on the data subjects.

(g) Processor shall provide Controller with a point of contact for all issues related to data protection and data processing within the scope of the Main Contract.

(h) Processor warrants that it will regularly review the effectiveness of the technical and organisational measures to adequately ensure the security of the data processing (Article 32(1)(d) of the GDPR).

(i) Processor may at any time or when Controller instructs it to do so, rectify or erase data in scope of the Main Contract. The agreed data processing activities do not contain any storage or archiving obligation of any personal data of the Controller. If a specific deletion upon request that is compliant with regulations on data protection or restriction of data processing is not reasonably or technically possible, Processor shall either delete the whole account or agree a special restriction or other measure with the Controller, unless stipulated differently in the Main Contract. Processor is entitled to regularly delete data in the cloud services for data minimization purposes as stipulated in the Main Contract.

(j) Upon Controller's reasonable instructions, Processor shall provide to Controller or delete any data, storage media, and other related materials after the termination or expiration of the Main Contract. Notwithstanding the foregoing, the Parties agree that, to the extent that electronic records containing confidential information is retained as data or records for the purposes of backup, recovery, contingency planning or are otherwise not accessible in the ordinary course of business, the Parties shall continue to comply with the terms of this Addendum. However, they shall not be required to access such data or records separately in order to delete them at the end of the Main Contract to be compliant with its obligations hereunder.

(k) In the event that a data subject asserts a claim against the Controller pursuant to Article 82 of the GDPR, Processor agrees to use reasonable efforts to assist Controller in the defence of the claim. For this purpose, the parties may agree on an arrangement regarding compensation in the Main Contract.

5. Obligations of Controller

(a) This Data Processing Addendum does not in any way oblige Controller to transfer any personal data to the Processor. For any data, Controller uploads into the cloud services, Controller warrants that it is authorised to transfer such personal data and that - when necessary - adequate consent has been obtained by Controller from the relevant data subjects.

(b) Controller shall, without delay and in a comprehensive fashion, inform Processor of any defect Controller may detect in Processor’s work results and of any irregularity in the implementation of regulations on data protection.

(c) In the event that a data subject asserts a claim against the Processor pursuant to Article 82 of the GDPR, Controller agrees to assist Processor in the defence of the claim.

(d) Controller shall keep its own back-up and storage of any data uploaded into the Cloud Services according to the Main Contract.

(e) Controller shall give Processor the name of the contact person responsible for data protection issues that may arise as part of the Main Contract.

6. Inquiries by Data Subjects

If a data subject requests that Processor rectify, access, erase, restrict or transmit data, Processor shall refer the data subject to Controller, provided that allocation to Controller is possible based on the data subject's information. Processor shall forward the data subject's request to Controller without undue delay. Processor shall assist Controller within the scope of its abilities as instructed, insofar as agreed. Processor shall not be liable if Controller does not answer the data subject's request, does not answer it correctly, or does not answer it within any given deadline.

7. Means of Proof

(a) Processor shall prove its compliance with the obligations specified in this Data Processing Addendum to Controller using suitable means by making available all information necessary to demonstrate compliance. If specific types of proof can be specified or used to prove compliance with the agreed obligations, Processor may submit the following information to Controller:

Variation 1 Results of an internal audit

Variation 2 Internal company codes of conduct including proof of compliance by an external auditor

Variation 3 Certification concerning data protection and/or information security (e.g. ISO 27001)

(b) Controller may approve the appointment of an independent external auditor by Processor, provided Processor provides Controller with a copy of the audit report. Processor may request remuneration for its assistance during the audit. Auditing shall be limited to one audit per calendar year, where reasonably possible.

Should, in individual cases, audits by Controller or by an auditor hired to perform an audit be required, they shall be performed during regular business hours, without disrupting Processor's business operations, and after reasonable advance notice. Processor may make them dependent on reasonable and timely advance agreement and on the signing of a confidentiality agreement with regard to the data of other customers and the implemented technical and organisational measures. If the auditor hired by Controller is a competitor of Processor, Processor shall have the right of veto.

(c) If a data protection supervisory authority or other supervisory authority of Controller performs an audit, clause 7(b) above shall apply accordingly. A confidentiality agreement does not need to be signed if the supervisory authority is already subject to professional or legal confidentiality under applicable laws.

8. Subcontractors

(a) The contractually agreed services or the deliverables defined below may be performed by the following pre-approved subcontractors:

Name of the subcontractor / third-party provider	**Description of the individual services**
Mailjet, FR	Email Messenger
MessageMedia, AUS	SMS Messenger

Microsoft Corporation, US	Azure hosting and cognitive analysis service in UK
Greenmini, NL	Dedicated Mac hosting service
GI Solutions Group, UK	Print and mail service provider

Processor has concluded EU Standard Contractual Clauses with the subcontractors that are subprocessors to the extent required, in order to ensure appropriate data protection and information security measures.

(b) Controller permits Processor to use the above subcontractors as applicable under the Main Contract. Processor shall notify Controller before hiring or replacing a subcontractor (if necessary, specifying a time limit and/or arrangement for emergency situations). Controller may refuse the change – within an appropriate period – for good cause. When no objection is made during this term, agreement to the change shall be deemed to be given. If there is good cause related to data protection and the parties are unable to reach an agreement, Controller shall be entitled to exercise a special right of termination (as an option).

(c) A subcontracting relationship that requires consent exists if Processor hires additional processors for performance, either in whole or in part, of the contractually agreed services outside of the named parties in subsection a) above or outside of the Quadient Group. Processor shall conclude appropriate data processing agreements with these third parties if they are subprocessors to the extent required in order to ensure appropriate data protection and information security measures.

(d) If the subcontractor provides the agreed service outside the EU/EEA or an adequate country, the Processor shall ensure compliance with the regulations on data protection and agree suitable safeguards (e.g. EU Standard Contractual Clauses).

9. Duties to Inform, Mandatory Written Form, Choice of Law

(a) Should Controller's personal data become subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while being processed, Processor shall inform Controller without delay. Processor shall, without delay, notify all pertinent parties in such action that any personal data affected thereby are in Controller's sole property and area of responsibility, that personal data are at Controller's sole disposition, and that Controller is the responsible body in the sense of the GDPR.

(b) Changes and amendments to this Data Processing Addendum and all of its components, including any commitment issued by Processor, must be made in writing (including in electronic format [text form]) to be legally binding, and must make express reference to there being a change or amendment to these provisions. This also applies to the waiver of mandatory written form.

(c) If there are any conflicts, the provisions of this Data Processing Addendum shall take precedence over the provisions of the Main Contract. Should individual provisions of this Data Processing Addendum be legally invalid, this shall not affect the validity of the remaining provisions.

(d) The governing law and submission to jurisdiction of this Data Processing Addendum shall be the law of England and Wales and the English courts.

10. Liability and Damages

Subject to the agreed liability caps and stipulations in the Main Contract, each party agrees to indemnify, keep indemnified and defend at its own expense the other party against all costs, claims, damages or expenses incurred by the other party or for which the other party may become liable due to any failure by the first party or its employees or agents to comply with any of its obligations under this Data Processing Addendum.

Nothing in this Data Processing Addendum shall limit or change the responsibility the Data Controller has under the UK GDPR.

Art. 82 UK GDPR shall apply accordingly.

11. Signatures

On behalf of the Processor:

Quadient UK LImited

Address: 3rd Floor Press Centre, Here East, 14 East Bay Lane, London, E15 2GW

Name : Duncan Groom

Position: Director

Signature.............................

On behalf of the Controller:

Company Name (written out in full):

Address:

Representative's Name:

Position:

Signature...

Other information necessary in order for the contract to be binding (if any):

(stamp of organisation)

Appendix 1 - Technical and Organisational Measures

Notwithstanding any additional measures agreed to in the Main Contract, the Processor ensures that at least the following technical and organisational measures are ensured:

1. Confidentiality (Article 32 Paragraph 1 Point b UK GDPR).

Data provided shall be considered as "CONFIDENTIAL" at the minimum.

- Physical Access Control.

No unauthorised access to Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems.

- Electronic Access Control.

No unauthorised use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media.

Access to the processor data is only on a "Need-to-know" basis. In particular access should be removed as soon as a person leaves the project (or the sub-contractor). A "Data Owner" able to judge if access is justified shall be identified.

- Internal Access Control (permissions for user rights of access to and amendment of data).

No unauthorised Reading, Copying, Changes or Deletions of Data within the system, e.g.: rights authorisation concept, need-based rights of access, logging of system access events.

Individuals authorized to have privileged access shall have committed themselves to maintain the confidentiality of the data they may have access to.

- Isolation Control.

The isolated Processing of Data, which is collected for differing purposes, e.g.: multiple Client support, sandboxing, test data.

- Pseudonymisation (Article 32 Paragraph 1 Point a UK GDPR; Article 25 Paragraph 1 UK GDPR).

The processing of personal data in such a method/way, that the data cannot be associated with a specific data subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.

- End of Contract.

All data shall be deleted and/or returned at the end of the processing services or if instructed by the processor.

2. Integrity (Article 32 Paragraph 1 Point b UK GDPR).

- Data Transfer Control.

No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature.

- Data Entry Control.

Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management.

3. Availability and Resilience (Article 32 Paragraph 1 Point b UK GDPR).

- Availability Control.

Prevention of accidental or wilful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning.

- Rapid Recovery (Article 32 Paragraph 1 Point c UK GDPR) (Article 32 Paragraph 1 Point c UK GDPR).

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d UK GDPR; Article 25 Paragraph 1 UK GDPR).

- Data Protection Management.

- Incident Response Management.

- Data Protection by Design and Default (Article 25 Paragraph 2 UK GDPR).

- Order or Contract Control.

No third-party data processing as per Article 28 UK GDPR without corresponding instructions from the Controller, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the Service Provider, duty of pre- evaluation, supervisory follow-up checks.

5. Security Incident management.

A proper process shall be in place to ensure that the processor will be informed of a Data Breach involving his data as soon as it is detected.