DATA PROCESSING AGREEMENT

Version: December 2021

This Data Protection Agreement ("**DPA**") sets out the parties' data protection obligations under Applicable Laws which arise where the Processor's Processing of Personal Data on behalf of the Controller under the Principal Agreement in respect of the Services.

The relevant LiveTiles entity which provides the Services ("**LiveTiles**"), as further described in the Principal Agreement, and the User are parties to the Principal Agreement whereby the User procures certain products and services from LiveTiles, or a related entity .

LiveTiles and the User will become bound by this DPA only where so specified in the Principal Agreement, and at the same time the Principal Agreement is entered into. This DPA will form an addendum to the Principal Agreement. This DPA becomes effective without any further action by the parties from the date of the Principal Agreement. This DPA will take effect as and from the date that the Principal Agreement commences ("**Effective Date**") (even where this DPA is entered into after that date).

The parties agree as follows:

1 INTERPRETATION

1.1 In this DPA, unless otherwise indicated by the context:

"**Commission**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**"	these terms shall have the same meaning as in the GDPR.
Applicable Laws	means (a) European Union or Member State laws with respect to any Personal Data in respect of which the parties are subject to EU Data Protection Laws; and (b) any other applicable privacy and data protection laws with respect to the use, storage, collection or Processing of Personal Data including other Data Protection Laws
Business Day	means a day that is not a Saturday, Sunday or public holiday or bank holiday in the city and state in which the Processor is incorporated
Contracted Processor	means the Processor or a Subprocessor
Controller	has the same meaning as in the GDPR, and includes the User who becomes bound under this DPA as the "Controller" party
Data Protection Laws	means EU Data Protection Laws, UK Data Protection Laws, and, to the extent applicable, the data protection or privacy laws of any other country
EU Data Protection Laws	means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR

GDPR	means the EU General Data Protection Regulation 2016/679
Personal Data	means any Personal Data Processed by a Contracted Processor on behalf of the Controller
Principal Agreement	means the agreement whereby the User procures certain products and services from LiveTiles, and which incorporates this DPA by reference. The Principal Agreement will either be a "Software Purchase Agreement" or "Master Services Agreement" (or similar agreement) between the parties or the Processor's end user licence agreement for its software
Processor	has the same meaning as in the GDPR, and includes the relevant LiveTiles entity who provides the Services, as further described in the Principal Agreement
Restricted Transfer	means: (a) a transfer of Personal Data from the Controller to a Contracted Processor; or (b) an onward transfer of Personal Data from a Contracted Processor to another Contracted Processor, or between two establishments of a Contracted Processor, or to a Subprocessor, in each case, where such transfer is to a country outside the United Kingdom and the European Economic Area which is not subject to an adequacy determination by the relevant supervisory authority
Services	means any goods or services provided from time to time by LiveTiles to the User, under the terms of the Principal Agreement
Standard Contractual Clauses or SCCs	means: (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021 ("**EU SCCs**"); and (ii) where the UK GDPR applies, the standard data protection clauses for processors adopted pursuant to or permitted under Article 46 of the UK GDPR ("**UK SCCs**"); in each case as may be amended, superseded or replaced from time to time
Subprocessor	means any person (including any third party) appointed by or on behalf of the Processor to Process Personal Data on behalf of the Processor and includes the entities listed in **Schedule 3**
UK Data Protection Laws	means the UK GDPR, the UK Data Protection Act 2018, the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended
UK GDPR	means the GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act

1.2 In this DPA, unless otherwise indicated by the context:

(a) words importing the singular include the plural and vice versa;

(b) headings are for convenience only and do not affect interpretation of this DPA;

(c) a reference to a clause, paragraph or schedule is a reference to a clause, paragraph or schedule of this DPA;

(d) where any word or phrase is given a definite meaning in this DPA, any part of speech or other grammatical form of that word or phrase has a corresponding meaning;

(e) an expression importing a natural person includes a body corporate, partnership, joint venture, association or other legal entity;

(f) a reference to a statute, statutory provisions or regulation includes all amendments, consolidations or replacements thereof;

(g) a reference to a party to a document includes that party's legal personal representatives, successors and permitted assigns;

(h) a covenant or agreement on the part of or for the benefit of two or more persons binds or benefits them jointly and severally; and

(i) a reference to a body, whether statutory or not:

(i) which ceases to exist; or

(ii) whose powers or functions are transferred to another body;

is a reference to the body which replaces it or which substantially succeeds to its powers or functions.

2 RELATIONSHIP OF PARTIES

2.1 LiveTiles as Processor

Where the User is a Controller of Personal Data, LiveTiles will be a Processor processing Personal Data on behalf of the User in accordance with the User's instructions set out in **clause 3.3** and this DPA will apply accordingly.

2.2 LiveTiles as Controller

To the extent that LiveTiles processes Personal Data as a Controller, LiveTiles will Process such Personal Data in accordance with its Privacy Policy.

2.3 Both parties as Controller

During the course of this DPA, both parties anticipate they will exchange Personal Data relating to their employees as necessary in connection with the provision of Services and account management. Each party is an independent Controller over such Personal Data.

3 PROCESSING OF PERSONAL DATA

3.1 Each party will comply with its obligations under Applicable Laws with respect to its Processing of Personal Data.

3.2 The Processor will:

(a) comply with all applicable Data Protection Laws in the Processing of Personal Data; and

(b) not Process Personal Data other than on the Controller's documented instructions (including those instructions given under **clause 3.3**) unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case the Contracted Processor, shall to the extent permitted by Applicable Laws inform the

Controller of that legal requirement before the relevant Processing of that Personal Data.

3.3 The Controller instructs the Contracted Processor (and authorises them to instruct each Subprocessor) to:

(a) process the Personal Data; and

(b) transfer the Personal Data to any country or territory,

as reasonably necessary for the provision of the Services, and to perform its obligations and exercise its rights under the Principal Agreement.

3.4 **Schedule 1** sets out the subject matter and details of the Processing of the Personal Data.

3.5 The Processor will reasonably assist the Controller with meeting the Controller's compliance obligations under the Data Protection Laws, taking into account the nature of the Processor's processing and the information available to the Processor, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with supervisory authorities under the Data Protection Laws.

3.6 The Processor will promptly notify the Controller of any changes to Data Protection Laws that may adversely affect the Processor's performance of the Services.

4 PERSONNEL

The Processor shall take reasonable steps to ensure each employee, agent or contractor of any Contracted Processor who may have access to Personal Data, only has access to the Personal Data on a need to know basis, as strictly necessary for the purposes of providing the Services, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor. Each Contracted Processor shall also ensure that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5 SECURITY

5.1 The Processor will, at all times, implement appropriate technical and organisational measures against unauthorised or unlawful Processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data as described in **Schedule 2**. The Processor will maintain an up to date written record of its then-current security measures, which it shall provide to the User on request, and review at least on a quarterly basis to ensure they remain current and complete. The Processor may update its security measures from time to time, provided they do not result in a reduction in the security over the Personal Data to which they apply.

5.2 The Processor will implement such measures to ensure a level of security appropriate to the risk involved, including, as appropriate, the pseudonymisation and encryption of Personal Data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and a process for regularly testing, assessing and evaluating the effectiveness of security measures.

6 SUBPROCESSING

6.1 The Controller authorises the Processor to appoint (and permit each Subprocessor appointed in accordance with this **clause 6** to appoint) Subprocessors in accordance with this **clause 6**.

6.2 The Controller may continue to use those Subprocessors already engaged by them as at the date of this DPA, subject to the Processor as soon as practicable meeting the obligations set out in **clause 6.46.4**. At the date of this DPA, the Processor uses the Subprocessors listed in **Schedule 3** to provide the Services.

6.3 The Processor shall provide at least ten (10) days prior written notice of the appointment of any new Subprocessor, who may process the Personal Data, including full details of the Processing to be undertaken by the Subprocessor. Such notice may be given by the Processor from time to time, publishing the names of Subprocessors which it uses to process Personal Data, on the Processor's website (and the Controller will be deemed to have been notified of the same at that time). If, within 5 Business Days of receipt of that notice, or date of publication on the Processor's website, the Controller notifies the Processor in writing of any objection (on data protection reasonable concerns) to the proposed appointment, the parties will discuss such concerns in good faith and whether they can be resolved. If the parties are not able to mutually agree to a resolution of such concerns, the Controller, as its sole and exclusive remedy, may terminate the Principal Agreement for convenience in accordance with the terms of the Principal Agreement.

6.4 With respect to each Subprocessor appointed by the Processor, the Processor shall take reasonable steps to ensure that the arrangement with the Subprocessor is governed by a written agreement including terms which offer at least the same level of protection for Personal Data as those set out in this DPA and which meet the requirements of Applicable Laws.

6.5 The Processor shall take reasonable steps to ensure that each Subprocessor observes each of the Processor's obligations under this DPA in relation to the Processing of Personal Data, as if those obligations were the principal obligations of the Subprocessor. The Processor remains liable to the Controller for the Subprocessor's performance of its agreement obligations.

7 DATA SUBJECT RIGHTS

7.1 The Processor shall assist the Controller by implementing appropriate technical and organisational measures (in the context of the nature of the Processing), as far as practicable, for the fulfilment of the Controller's obligations, to respond to requests from a Data Subject to exercise their rights under Data Protection Laws.

7.2 The Processor shall:

(a) promptly notify the Controller if a Contracted Processor receives a request from a Data Subject to exercise any of their rights under a Data Protection Law in respect of their Personal Data including subject access rights, the rights to rectify and erase Personal Data, object to the processing and automated processing of Personal Data, and restrict the processing of Personal Data; and

(b) ensure that the Contracted Processor does not respond to that request except on the documented instructions of the Controller, or as required by Applicable Laws to which the Contracted Processor is subject.

7.3 The Controller authorises the Processor to provide an acknowledgement to the Data Subject directly, and to inform the Data Subject that the correspondence has been referred to the Controller.

8 PERSONAL DATA BREACH

8.1 The Processor shall notify the Controller without undue delay upon the Processor or their Subprocessor becoming aware of a Personal Data Breach affecting the Personal Data disclosed by the Controller to the Processer, providing the Controller with sufficient

information to allow the Controller to meet any obligations to report or inform Data Subjects, or relevant authorities, of the Personal Data Breach under the Data Protection Laws.

8.2 The Processor shall co-operate with the Controller and take such reasonable commercial steps as are directed by the Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9 DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

9.1 The Processor will provide reasonable assistance to the Controller with meeting the Controller's compliance obligations under Applicable Laws including any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Controller reasonably considers to be required of it by Applicable Laws, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9.2 If a law, court, regulator or Supervisory Authority requires the Processor to Process or disclose Personal Data, the Processor will first use its reasonable endeavours to inform the User of the legal or regulatory requirement and give the User an opportunity to object or challenge the requirement, unless Applicable Law prohibits such notice.

10 DELETION OR RETURN OF GROUP MEMBER PERSONAL DATA

10.1 Subject to this clause, the Processor shall as soon as reasonably practicable following the completion of the Services involving the Processing of the Personal Data, upon written request from the Controller either:

(a) delete and procure the deletion of all copies of the Personal Data (as directed by the Controller); or

(b) deliver a copy of the Personal Data to the Controller,

or a combination of the above.

10.2 Each Contracted Processor may retain the Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that the Processor shall ensure the confidentiality of all such Personal Data and shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

11 AUDIT RIGHTS

11.1 No more than once during any consecutive 12 month period, the Processor shall make available to the Controller, following the Controller's reasonable request, all information reasonably and solely necessary to demonstrate compliance with this DPA (which may include information from an audit carried out internally or by a third party), and shall allow for and contribute to audits, including inspections, by the Controller or an auditor nominated by the Controller in relation to the Processing of Personal Data by the Contracted Processor. The Controller shall be entitled to ask questions of the Processor related to compliance with EU Data Protection Laws and UK Data Protection Laws in advance of the audit, which the Processor shall use its reasonable endeavours to respond to adequately when providing the audit results. Any request for information, or request for an audit, by the Controller under this **clause 11** shall only be made in good faith and for a bona fide purpose.

11.2 The Controller may only mandate an auditor for the purposes of **clause 11.1** if the auditor is approved by the Processor. The Processor shall not unreasonably withhold or delay its approval of the auditor.

11.3 The Controller shall give the Processor or the relevant Subprocessor reasonable notice of any audit or inspection to be conducted under **clause 11.1** and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

(a) to any individual unless he or she produces reasonable evidence of identity and authority;

(b) outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and the Controller has given notice to the Processor or the relevant Subprocessor that this is the case before attendance outside those hours begins; or

(c) for the purposes of more than one audit or inspection, in respect of each Contracted Processor, in any calendar year, except for any additional audits or inspections which:

(i) the Controller reasonably considers necessary because of genuine concerns as to the Processor's compliance with this DPA; or

(ii) the Controller is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

where the Controller has identified its concerns or the relevant requirement or request in its notice to the Processor or relevant Subprocessor of the audit or inspection.

11.4 The Controller will pay or reimburse the Processor for the Processor's reasonable costs in complying with this **clause 11**.

11.5 The Controller will maintain the confidentiality of all information disclosed to it by the Processor under this **clause 11** (**Confidential Information**), and will ensure that its auditors and other agents or personnel of the Controller who have access to such information (**Representatives**), also maintain confidentiality. The Controller will, and will ensure that its Representatives, only use or disclose the Confidential Information solely for the purposes of complying with Applicable Laws, and will only disclose the Confidential Information where required by Applicable Laws. The Controller, and the Controller shall ensure its Representatives, do not use or disclose Confidential Information for any other purpose.

12 RESTRICTED TRANSFERS AND THE STANDARD CONTRACTUAL CLAUSES

12.1 To the extent that the Controller's use of the Services and Processor's Processing of Personal Data in accordance with the Principal Agreement involves a Restricted Transfer and subject to **clause 12.3**, the Standard Contractual Clauses shall be incorporated by reference and form part of this DPA as if they had been set out in full, with the Controller as **"data exporter"** and each Contracted Processor, as appropriate, as **"data importer"**.

12.2 The Standard Contractual Clauses shall apply in the manner set out in **Schedule 4**.

12.3 **Clause 12.1** shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

12.4 In the case of any Processing of Personal Data outside of the GDPR jurisdictions as at the date of this DPA, the Processor has identified the Subprocessors listed in **Schedule 3** to which the Controller approves.

13 TERMINATION

13.1 Termination by mutual agreement

This DPA may be terminated at any time by a written document signed by all parties.

13.2 Termination by the Controller

(a) The Controller may terminate this DPA at any time, and for any reason, on the provision of written notice to the Processor.

(b) The Processor may terminate this DPA at any time by written notice to all other parties, provided that at the time such notice is given, the Processor:

(i) is no longer Processing any Personal Data on behalf of the Controller; and

(ii) the Contracted Processor has complied with **clause 10**.

13.3 Automatic termination

This DPA will automatically terminate if the Processor or its related entity are no longer providing Services to the Controller, or if the Principal Agreement otherwise terminates.

13.4 Provisions which survive termination

Upon the termination of this DPA, the obligations under **clauses 7**, **8**, **10**, **11** and **12** will continue to apply following termination.

14 GENERAL

14.1 Assignment

A party must not assign or novate this DPA without each other party's prior written consent.

14.2 Variation

This DPA may only be amended or modified by a document in writing signed by the parties.

14.3 Notices

Any notice or demand to be given or made under this DPA must be in writing signed by a party's authorised representative. A notice will be deemed to be received (a) in the case of a notice given by hand, on delivery; (b) in the case of a notice sent by pre-paid post, 5 days following the date of postage; and (c) in the case of a notice sent by email, upon the recipient or their mail server confirming receipt of the email.

14.4 Entire agreement

It is expressly acknowledged, by and between the parties, that the terms set out in this DPA, together with the Principal Agreement, contain the entire agreement concluded between the parties, and that this DPA supersedes any and all prior agreements, representations, or understandings between the parties, whether written or oral, in respect of the same subject matter.

14.5 Waiver

Any waiver of a right or remedy under this DPA will only be valid if the waiver is given in writing and signed by the party giving the waiver.

14.6 Severance

If a provision of this DPA or part thereof is unenforceable, then that provision (or relevant part) may be severed without affecting the enforceability of any other provision of this DPA.

14.7 Further Assurance

Each party will from time to time do all things (including executing all documents) necessary or desirable to give full effect to this DPA.

14.8 Counterparts

This DPA may be executed in any number of counterparts each of which will be an original but such counterparts together will constitute one and the same instrument and the date of the DPA will be the date on which it is executed by the last party.

14.9 No merger

Nothing in this DPA merges, extinguishes, postpones, lessens or otherwise prejudicially affects any right, power or remedy that a party may have against another party or any other person at any time.

14.10 Consents and approvals

Where this DPA gives any party a right or power to consent or approve in relation to a matter under this DPA, that party may withhold any consent or approval or give consent or approval conditionally or unconditionally. The party seeking consent or approval must comply with any conditions the other party imposes on its consent or approval.

14.11 Governing Law and Jurisdiction

(a) Subject to **clause 14.11(b)**, this DPA is governed by the same laws as the same jurisdiction which governs the Principal Agreement.

(b) To the extent required to comply with the GDPR and UK GDPR, and only in relation to matters relating to the compliance of this DPA or a party's actions under it in relation to GDPR or UK GDPR, this DPA shall also be governed by the laws of each Member State where EU Data Protection Laws and the UK Data Protection laws, as applicable.

(c) Each party irrevocably submits to the jurisdiction described in **clause 14.11(a)** with respect to any disputes or claims howsoever arising under this DPA.

Executed as an agreement

(As indicated in the pre-amble to this DPA, the parties may become bound to this DPA either under the Principal Agreement, or by signing this DPA where marked below)

Date signed:

SIGNED by the authorised person named below for and on behalf of the Processor:

Name of the Processor	Signature
	Name of person signing
	Date

SIGNED by the authorised person named below for and on behalf of the Controller:

Name of the Controller	Signature
	Name of person signing
	Date

Schedule 1

SUBJECT MATTER AND DETAILS OF THE PROCESSING OF PERSONAL DATA

Subject matter

The Personal Data to be Processed includes all Personal Data disclosed from time to time by the Controller pursuant to this DPA or in relation to the Services.

Duration of the Processing of the Personal Data

From termination of the Principal Agreement and this DPA until the deletion of all Personal Data by the Processor in accordance with this DPA.

The nature and purpose of the Processing of Personal Data

The effective provision of the Services in accordance with the Principal Agreement.

The nature of the Processing shall be agreed between each Contracted Processor and the Controller from time to time. The Processor does not sell Personal Data.

The types of Personal Data to be Processed

Personal Data may include personal information (first name, last name, sign-in credentials, email address, username and password, contact information, IT information (IP addresses, usage data, cookies data, location data, browser data), financial information (credit card details, bank account details, payment information), employment details (employer, job title, geographic location, area of responsibility), CRM data concerning sales leads and customer lists, and any notes provided by the data exporter regarding the foregoing.

The categories of Data Subject to whom the Personal Data relates

- Potential and actual customers of LiveTiles;
- Third parties that have, or may have, a commercial relationship with the Controller / data exporter (e.g. software providers, strategic partnerships, joint ventures and contractors); and
- Employees and other personnel of LiveTiles and the above entities.

Schedule 2

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Where applicable, this Schedule 2 shall be taken to be Annex II to the Standard Contractual Clauses. The following is a description of the technical and organisational measures implemented by the Processor / data importer to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the Processing, and the risks for the rights and freedoms of natural persons.

The data importer will maintain appropriate organizational and technical security measures (which may include, with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, incident response, encryption of Personal Data while in transit and at rest) designed to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of Personal Data.

The data importer will take reasonable steps to confirm that all of its personnel are protecting the security, privacy, and confidentiality of Personal Data consistent with the requirements of this document and the DPA.

The data importer continuously trains employees on best security practices, including how to identify social engineering, phishing scams, and hackers.

The data importer will maintain internal policies that include but not limited to access control; information security; mobile device security; cloud computing and network security, recognising and implementing industry best practices such as multi factor authentication, encryption, and least privilege access controls.

LiveTiles is ISO27001 certified.

Access control to premises and facilities

Measures taken to prevent unauthorized physical access to premises and facilities holding personal data shall include:

- Storage of personal data is outsourced to Microsoft (see Sub-processors) and is not stored at any physical facilities
- All offices and associated entry points where information systems reside will be protected under lock and key or similar access control measures with logging. All employees of offices without key card logging will sign-in upon entry, and sign-out upon exit to maintain and monitor logs of physical access

Access control to systems

Measures taken to prevent unauthorized access to IT systems include the following technical and organizational measures for user identification and authentication:

- Secure lo on procedures including minimum password requirements (special characters, minimum length) and multi-factor authentication
- No access for guest users or anonymous accounts
- Central management of system access
- Access to IT systems subject to approval from HR management and IT system administrators
- Onboarding and offboarding processes for user provisioning and system access
- Regular review of access rights

Access control to data

Measures taken to prevent authorized users from accessing data beyond their authorized access rights and prevent the unauthorized input, reading, copying, removal modification or disclosure of data include:

- Least privilege access control policy
- Access rights defined according to duties
- Azure PIM (Privileged Identity Management) used for temporary access to data and systems
- Automated log of user access via IT systems
- Classification labelling and email exchange measures to ensure the automated data-processing systems are not accessed by unauthorized persons

Disclosure control

Measures taken to prevent the unauthorized access, alteration or removal of data during transfer, and to ensure that all transfers are secure and are logged shall include:

- Anonymization and pseudonymization measures applied to data processing
- Encryption using a VPN for remote access to environments
- Audit trail of data transfers

Input control

Measures put in place to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom must be maintained include:

- Logging user activities on IT systems
- User activity history and version control to verify and establish the input into automated data-processing systems by whom the when

Job control

Measures put in place to ensure that data is processed strictly in compliance with the data importer's instructions include:

- Unambiguous wording of contractual instructions
- Standard security clauses for suppliers and partners
- Monitoring of contract performance and supplier data security compliance

Availability control

Measures put in place designed to ensure that data are protected against accidental destruction or loss include:

- Cloud first, geo-redundant systems built on Microsoft 365 and Azure
- Real time monitoring of systems and faults
- Stored personal data cannot be corrupted by means of a malfunctioning of the system
- Business Continuity procedures including backup and disaster recovery
- Anti-virus/firewall systems installed on corporate devices and servers

Segregation control

Measures put in place to allow data collected for different purposes to be processed separately include:

- Restriction of access to data stored for different purposes according to staff duties
- Segregation of business IT systems
- Segregation of IT testing and production environments

Schedule 3

LIST OF SUBPROCESSORS

Subprocessors engaged in the Processing of Personal Data on behalf of the Controller in connection with the Processor's provision of Services include the following entities:

Sub-Processor	Country	Purpose	Contact details
1password	Europe	Secure credential management	dpo@1password.com
Asana	USA	Project mgmt.	privacy@asana.com or dpo@asana.com
Azure (Microsoft)	USA / Australia / Europe	Hosting	AskHR@microsoft.com or https://aka.ms/privacyresponse
E-conomic	Denmark	Financial operations	privacy@e-conomic.com
Hubspot	USA	Marketing	General Data Protection Regulation | HubSpot
Intercom	USA	Chat support	legal@intercom.io
Lastpass	Europe	Secure credential management	privacy@logmein.com
Marketo	Australia	Marketing	privacyofficer@marketo.com
Mixpanel	USA	Marketing	compliance@mixpanel.com or dpo@mixpanel.com
Oasis	USA	Personnel administration	+1 (800) 822-8635
Office365 (Microsoft)	Australia	Collaboration	AskHR@microsoft.com or https://aka.ms/privacyresponse
Salesforce	Australia	CRM	privacy@salesforce.com
Segment.io	USA	Marketing	privacy@segment.com
Timelog	Denmark	Time capture	
Xero	Australia	Financial operations Personnel administration	Privacy at Xero – Xero Central
Zendesk	USA	Support	https://www.zendesk.com/company/privacy-and-data-protection/ or privacy@zendesk.com

Schedule 4

RESTRICTED TRANSFERS (INTERNATIONAL TRANSFERS)

1 INTRODUCTION TO THIS RESTRICTED TRANSFERS SCHEDULE

1.1 Paragraph 2 of this Schedule completes the template elements of the Standard Contractual Clauses which are incorporated into this Schedule in full.

1.2 If and to the extent the Standard Contractual Clauses conflict with any provision of this DPA regarding the transfer of Personal Data from the Controller to the Processor, the Standard Contractual Clauses shall prevail to the extent of such conflict.

1.3 Paragraph 3 of this Schedule reflects the parties' endeavours to address the recommendations of the European Data Protection Board in their public consultation document 01/2020, adopted on 18 June 2021 and entitled "measures that supplement transfer tools to ensure compliance with the EU level of protection of Personal Data".

2 EU STANDARD CONTRACTUAL CLAUSES

2.1 For data transfers from the European Economic Area that are subject to the EU SCCs, Module 2 (Controller to Processor) of the EU SCCs will apply where the User is a Controller and LiveTiles is the Processor as follows:

Exporter contact details	Those of the User as set out in the Principal Agreement
Importer contact details	Those of LiveTiles as set out in the Principal Agreement
Governing Law	As set out in the Principal Agreement
Data Exporter	The User
Data Importer	LiveTiles

(a) in Clause 7, the option docking clause will apply;

(b) in Clause 9, Option 2 will apply, and the time period for prior notice of Subprocessor changes will be as set forth in Clause 6 (Subprocessing) of this DPA;

(c) in Clause 11, the optional language will not apply;

(d) in Clause 17 (Option 1), the EU SCCs will be governed by Irish law.

(e) in Clause 18(b), disputes will be resolved before the courts of Ireland;

(f) In Annex I, Part A:

(i) See above for details of the Data Exporter and Data Importer; and

(ii) Signature & Date: By entering into the Principal Agreement and this DPA, Data Exporter and Data Importer are deemed to have signed these Standard Contractual Clauses incorporated by reference into the DPA, including their Annexes, as of the Effective Date of the Principal Agreement;

(g) In Annex I, Part B:

(i) The categories of data subjects are described in Schedule 1 of this DPA;

(ii) The frequency of the transfer is a continuous basis for the duration of the Principal Agreement;

(iii) The nature of the processing is described in Schedule 1 of this DPA;

(iv) The purpose of the processing is described in Schedule 1 of this DPA; and

(v) The duration of the processing is described in Schedule 1 of this DPA;

(h) In Annex I, Part C: The Irish Data Protection Commission will be the competent supervisory authority; and

(i) Schedule 2 of this DPA is to be read as Annex II for the purposes of the Standard Contractual Clauses.

2.2 The illustrative indemnity set out in the Standard Contractual Clauses is deemed deleted.

2.3 Any replacement to the Standard Contractual Clauses adopted in accordance with Article 93(2) of the GDPR shall supersede the Standard Contractual Clauses incorporated into this Schedule, and this Schedule shall be interpreted so as to give full effect to such replacement Standard Contractual Clauses.

2.4 LiveTiles may unilaterally vary this DPA to the extent necessary to incorporate any replacement to the Standard Contractual Clauses. If LiveTiles exercises such variation right, it shall promptly provide the User with a copy of the updated version of this DPA.

3 UK STANDARD CONTRACTUAL CLAUSES

3.1 For data transfers from the United Kingdom that are subject to the UK SCCs, the UK SCCs will be deemed entered into (and incorporated into this DPA by reference) and completed as follows:

(a) The UK Controller to Processor SCCs will apply where the Processor is processing Personal Data.

(b) The illustrative indemnification clause will not apply.

(c) Schedule 1 of this DPA is to be read as Appendix 1 for the purposes of the UK Controller to Processor SCCs.

(d) Schedule 2 of this DPA is to be read as Appendix 2 for the purposes of the UK Controller to Processor SCCs.

4 SUPPLEMENTARY MEASURES ADOPTED TO ADDRESS TO EUROPEAN DATA PROTECTION BOARD'S RECOMMENDATIONS

Challenges to information requests

4.1 In addition to the Standard Contractual Clauses, in the event the Data Importer receives an order from any third party for compelled disclosure of any Personal Data it is Processing for the Data Exporter, the Processor shall:

(a) use every reasonable effort to redirect the third party to request data directly from the Data Exporter;

(b) promptly notify the Data Exporter, unless prohibited under applicable law (and, if prohibited from notifying the Data Exporter, use all lawful efforts at the Data Exporter's sole cost and expense to obtain the right to waive the prohibition in order to communicate as much information to the Data Exporter) as soon as possible; and

(c) use all lawful efforts at the Data Exporter's sole cost to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with the law of the European Union or applicable EU member state law.

4.2 For purposes of paragraph 4.1 of this Schedule, lawful efforts means exercising the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a provider engaged in a similar type of undertaking under the same or similar circumstances and shall not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

Notification of Orders

4.3 In addition to the Standard Contractual Clauses, the Data Importer shall provide reasonable cooperation to the Data Exporter in order for the Data Exporter to inform Data Subjects about any legally binding order for disclosure of their Personal Data by an authority, unless:

(a) providing such information proves impossible or unreasonable;

(b) it can be reasonably expected that the Data Subject already has the information; or

(c) such disclosure is otherwise legally prohibited (and in such case, the Data Importer shall use all lawful efforts at the Data Exporter's sole cost to obtain the right to waive the prohibition in order to communicate as much information to the Data Exporter as soon as possible).

Transparency Reporting

4.4 The Data Importer shall inform the Data Exporter about access orders received from authorities concerning Personal Data Processed under this DPA. Such information will consist at least of the number of orders, the nature of data demanded, the legal basis for such orders, and the identity of the ordering bodies, unless such information proves impossible for the Data Importer to provide, or the disclosure of such information is otherwise legally prohibited.

4.5 If the disclosure contemplated at paragraph 4.4 of this Restricted Transfers Schedule is legally prohibited, then the Data Importer shall use its reasonable endeavours (at the Data Exporter's cost) the enable the lawful disclosure. The Data Importer shall distinguish between cases where copies of Personal Data is and is not requested. In its law enforcement transparency reporting, it shall provide additional details on the types of responses where it legally can do so, such as by providing information on the number of United States demands versus demands from other countries.