DATA PROCESSING AGREEMENT

This DPA is entered into between the Controller and the Processor and is incorporated into and governed by the terms of the Agreement.

1. Definitions

Any capitalised term not defined in this DPA shall have the meaning given to it in the Agreement.

"**Affiliate**"	means any entity that directly or indirectly controls, is controlled by, or is under common control of a party. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of a party;
"Agreement"	means the customer services agreement between the Controller and the Processor for the provision of the Services;
"CCPA"	means the California Consumer Privacy Act of 2018, along with its regulations and as amended from time to time;
"Controller"	means the Customer;
"Customer"	means for the purposes of this DPA the non-Highlight entity entering into the Agreement with the Processor;
"Customer Data"	means all data imported into the Services for the purpose of using the Services or facilitating use of the Services by the Customer or its authorised users;
"Data Protection Law"	means all laws and regulations, including laws and regulations of the European Union, the European Economic Area, their member states and the United Kingdom any amendments, replacements or renewals thereof, applicable to the processing of Personal Data, including where applicable the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020, the EU GDPR, the UK GDPR, the FADP, the UK Data Protection Act 2018, US State Privacy Laws and any applicable national implementing laws, regulations and secondary legislation relating to the processing of the Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426);
"Data Subject"	shall have the same meaning as in Data Protection Law or means a "Consumer" or "individual" as those terms are defined in US State Privacy Laws;
"DPA"	means this data processing agreement together with Exhibits A and B;
"EEA"	means the European Economic Area;
"EU GDPR"	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (General Data Protection Regulation);
"FADP"	means the Swiss Federal Act on Data Protection of the 1st of September 2023, and as amended from time to time;
"Personal Data"	shall have the same meaning as in Data Protection Law and includes "personally identifiable information", as that term is defined in US State Privacy Laws;
"Processor"	means Highlight, including as applicable any "Service Provider" as that term is defined in US State Privacy Laws;

"Restricted Transfer"	means: (i) where the EU GDPR applies, a transfer of Personal Data via the Services from the EEA either directly or via onward transfer, to any country or recipient outside of the EEA not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of Personal Data via the Services from the United Kingdom either directly or via onward transfer, to any country or recipient outside of the UK not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) a transfer of Personal Data via the Services from Switzerland either directly or via onward transfer, to any country or recipient outside of the EEA and/or Switzerland not subject to an adequacy determination by the European Commission;
"Services"	means all services and software applications and solutions provided to the Controller by the Processor under and as described in the Agreement;
"SCCs"	means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries published at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN/ , ("**EU SCCs**"); and (ii) where the UK GDPR applies, the international data transfer addendum to the EU SCCs adopted pursuant to Article 46(2)(c) of the UK GDPR, international-data-transfer-addendum.pdf, ("**UK SCCs**"); and (iii) where Personal Data is transferred from Switzerland to outside of Switzerland or the EEA, the EU SCCs as amended in accordance with guidance from the Swiss Data Protection Authority; ("**Swiss SCCs**"); as they may be amended, superseded or replaced from time to time;
"Sub-processor"	means any third party (including Processor Affiliates) engaged directly or indirectly by the Processor to process Personal Data under this DPA in the provision of the Services to the Controller;
"Supervisory Authority"	means a governmental or government chartered regulatory body having binding legal authority over a party;
"UK GDPR"	means the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018;.
"US State Privacy Laws"	means the following US state data protection or privacy laws and regulations applicable to the party's Processing of Personal Data: California Consumer Privacy Act **(CCPA)** as amended by the California Privacy Rights Act (**CPRA**), Virginia Consumer Data Protection Act (**VCDPA**), Colorado Privacy Act (**CPA**), Connecticut Data Privacy Act (**CTDPA**), and Utah Consumer Privacy Act (**UCPA**) and the Connecticut Data Privacy Act (**CTDPA**), the Montana Consumer Data Privacy Act (**MCDPA**), Iowa Consumer Data Protection (**Iowa CDPA**), the Delaware Personal Data Privacy Act (**DPDPA**), the Nebraska Data Privacy Act (**NDPA**), the New Hampshire Expectation of Privacy Act (**NHPA**) and the New Jersey Act Concerning Online Services, Consumers, and Personal Data (**NJDPA**), Florida Data Privacy and Security Act (**FDPSA**), Oregon Consumer Privacy Act (**OCPA**), Texas Data Privacy and Security Act (**TDPSA**), Tennessee Information Protection Act

(**TIPA**), Minnesota Consumer Data Privacy Act (**MCDPA**), Maryland Online Data Protection Act (**MODPA**), in each case as may be amended or superseded from time to time.

2. Purpose

2.1 The Processor has agreed to provide the Services to the Controller in accordance with the terms of the Agreement. In providing the Services, the Processor shall process Customer Data on behalf of the Controller. Customer Data may include Personal Data. The Processor will process and protect such Personal Data in accordance with the terms of this DPA.

3. Scope

3.1 In providing the Services to the Controller pursuant to the terms of the Agreement, the Processor shall process Personal Data only to the extent necessary to provide the Services in accordance with the terms of the Agreement, this DPA and the Controller's instructions documented in the Agreement and this DPA, as updated from time to time.

3.2 The Controller and Processor shall take steps to ensure that any natural person acting under the authority of the Controller or the Processor who has access to Personal Data does not process Personal Data except on the instructions from the Controller, unless required to do so by any Data Protection Law.

4. Processor Obligations

4.1 The Processor may collect, process or use Personal Data only within the scope of this DPA.

4.2 The Processor confirms that it shall process Personal Data on behalf of the Controller in accordance with the documented instructions of the Controller.

4.3 The Processor shall promptly inform the Controller, if in the Processor's opinion, any of the instructions regarding the processing of Personal Data provided by the Controller, breach any Data Protection Law.

4.4 The Processor shall ensure that all employees, agents, officers and contractors involved in the handling of Personal Data: (i) are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential; (ii) have received appropriate training on their responsibilities as a data processor; and (iii) are bound by the terms of this DPA.

4.5 The Processor shall implement appropriate technical and organisational measures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

4.6 The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

4.7 The technical and organisational measures detailed in Exhibit B shall at all times be adhered to as a minimum security standard. The Controller accepts and agrees that the technical and organisational measures are subject to development and review and that the Processor may use alternative suitable measures to those detailed in the attachments to this DPA, provided such measures are at least equivalent to the technical and organisational measures set out in Exhibit B and appropriate pursuant to the Processor's obligations in clauses 4.5 and 4.6 above.

4.8 The Controller acknowledges and agrees that, in the course of providing the Services to the Controller, it may be necessary for the Processor to access the Personal Data to respond to any technical problems or Controller queries and to ensure the proper working of the Services. All such access by the Processor will be limited to those purposes.

4.9 Taking into account the nature of the processing and the information available to the Processor, the Processor shall assist the Controller by having in place appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights and the Controller's compliance with the Controller's data protection obligations in respect of the processing of Personal Data.

4.10 The Processor may not: (i) sell Personal Data; (ii) retain, use, or disclose Personal Data for commercial purposes other than providing the Services under the terms of the Agreement; or (iii) retain, use, or disclose Personal Data outside of the Agreement.

5. Controller Obligations

5.1 The Controller represents and warrants that: (i) it shall comply with this DPA and its obligations under Data Protection Law; (ii) it has obtained any, and all, permissions and authorisations necessary to permit the Processor and Sub-processors, to execute their rights or perform their obligations under this DPA; and (iii) all Affiliates of the Controller who use the Services shall comply with the obligations of the Controller set out in this DPA.

5.2 The Controller shall implement appropriate technical and organisational measures to protect Personal Data, taking into account: (i) the state of the art; (ii) the costs of implementation; (iii) the nature, scope, context and purposes of processing; and (iv) the risk of varying likelihood and severity for the rights and freedoms of natural persons.

5.3 The Controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

5.4 The Controller acknowledges and agrees that some instructions from the Controller including the Processor assisting with audits, inspections, DPIAs or providing any assistance under this DPA, may result in additional fees. In such case the Processor shall notify the Controller of its fees for providing such assistance in advance and shall be entitled to charge the Controller for its reasonable costs and expenses in providing such assistance, unless agreed otherwise IN writing.

6. Sub-processors

6.1 The Controller agrees that the Processor may engage Sub-processors in connection with the provision of the Services.

6.2 All Sub-processors who process Personal Data in the provision of the Services to the Controller shall comply with the obligations of the Processor set out in this DPA.

6.3 The Controller authorises the Processor to use the Sub-processors included in the list of Sub-processors published at http://highlight.net/legal/sub-processors to process the Personal Data. During the term of this DPA, the Processor shall provide the Controller with 30 days prior notification, via email, of any changes to the list of Sub-processors before authorising any new or replacement Sub-processor to process Personal Data in connection with provision of the Services.

6.4 The Controller may object to the use of a new or replacement Sub-processor, by notifying the Processor promptly in writing within ten (10) Business Days after receipt of the Processor's notice. If the Controller objects to a new or replacement Sub-processor, the Controller may terminate the Agreement with respect to those Services which cannot be provided by the Processor without the use of the new or replacement Sub-processor. The Processor will refund the Controller any prepaid fees covering the remainder of the term of the Agreement following the effective date of termination with respect to such terminated Services.

6.5 All Sub-processors who process Personal Data shall comply with the obligations of the Processor set out in this DPA. The Processor shall prior to the relevant Sub-processor carrying out any processing activities in respect of the Personal Data: (i) appoint each Sub-processor under a written contract containing materially the same obligations to those of the processor in this DPA enforceable by the Processor; and (ii) ensure each such Sub-processor complies with all such obligations.

6.6 The Controller agrees that the Processor and its Sub-processors may make Restricted Transfers of Personal Data for the purpose of providing the Services to the Controller in accordance with the Agreement. The Processor confirms that such Sub-processors: (i) are located in a third country or territory recognised by the EU Commission or a Supervisory Authority, as applicable, to have an adequate level of protection; or (ii) have entered into the applicable SCCs with the Processor; or (iii) have other legally recognised appropriate safeguards in place.

7. Restricted Transfers

7.1 The parties agree that, when the transfer of Personal Data from the Controller to the Processor or from the Processor to a Sub-processor is a Restricted Transfer, it shall be subject to the applicable SCCs.

7.2 The parties agree that the EU SCCs shall apply to Restricted Transfers from the EEA. The EU SCCs shall be deemed entered into (and incorporated into this DPA by reference) and completed as follows:

(i) Module One (Controller to Controller) shall apply where Highlight is processing Customer account data for its own purposes;

(ii) Module Two (Controller to Processor) shall apply where the Customer is a Controller of Customer Data and Highlight is processing Customer Data;

(iii) Module Three (Processor to Processor) shall apply where Highlight is a Processor of Customer Data and Highlight uses a Sub-processor to process the Customer Data;

(iv) Module Four (Processor to Controller) shall apply where Highlight is processing Personal Data and the Customer uses a Sub-Processor to process Personal Data;

(v) In Clause 7 of the EU SCCs, the optional docking clause shall not apply;

(vi) In Clause 9 of the EU SCCs Option 2 applies, and the time period for giving notice of Sub-processor changes shall be as set out in clause 6.3 of this DPA;

(vii) In Clause 11 of the EU SCCs, the optional language shall not apply;

(viii) In Clause 17 of the EU SCCs, Option 1 applies and the EU SCCs shall be governed by Irish law;

(ix) In Clause 18(b) of the EU SCCs, disputes shall be resolved by the courts of Ireland;

(x) Annex I of the EU SCCs shall be deemed completed with the information set out in Exhibit A of this DPA;

(xi) Annex II of the EU SCCs shall be deemed completed with the information set out in Exhibit B of this DPA;

7.3 The parties agree that the EU SCCs as amended in clause 7.2 above, shall be adjusted as set out below where the FADP applies to any Restricted Transfer:

(i) The Swiss Federal Data Protection and Information Commissioner ("FDPIC") shall be the sole Supervisory Authority for Restricted Transfers exclusively subject to the FADP;

(ii) Restricted Transfers subject to both the FADP and the EU GDPR, shall be dealt with by the EU Supervisory Authority named in Exhibit A of this DPA;

(iii) The term 'member state' must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs;

(iv) Where Restricted Transfers are exclusively subject to the FADP, all references to the GDPR in the EU SCCs are to be understood to be references to the FADP;

(v) Where Restricted Transfers are subject to both the FADP and the EU GDPR, all references to the GDPR in the EU SCCs are to be understood to be references to the FADP insofar as the Restricted Transfers are subject to the FADP;

7.4 The parties agree that the UK SCCs shall apply to Restricted Transfers from the UK and the UK SCCs shall be deemed entered into (and incorporated into this DPA by reference), completed as follows:

(i) Table 1 of the UK SCCs shall be deemed completed with the information set out in Exhibit A of this DPA; and

(ii) Table 2 of the UK SCCs shall be deemed completed with the information set out in clauses 7.2(i) to (viii) of this DPA.

(iii) Table 3 of the UK SCCs shall be deemed completed with the information set out in Exhibits A and B of this DPA; and

(iv) Either party may end the UK SCCs as set out in clause 19 of the UK SCCs.

7.5 If changes are made to the EU SCCs or UK SCCs in the future, the parties shall negotiate in good faith necessary amendments to the DPA and the Agreement to ensure compliance with applicable Data Protection Law.

7.6 In the event that any provision of this DPA contradicts directly or indirectly any SCCs, the provisions of the applicable SCCs shall prevail over the terms of the DPA.

7.7 Should countries other than those in the EEA, UK or Switzerland adopt cross-border data transfer clauses similar to the SCCs, the Controller and Processor agree to execute such clauses when necessary.

8. Data Subject Access Requests

8.1 The Controller may require correction, deletion, blocking and/or making available the Personal Data during or after termination of the Agreement. The Controller acknowledges and agrees that the Processor will process the request to the extent it is lawful and will reasonably fulfil such request in accordance with its standard operational procedures to the extent possible.

8.2 In the event that the Processor receives a request from a Data Subject in relation to Personal Data, the Processor will refer the Data Subject to the Controller unless otherwise prohibited by law. The Controller shall reimburse the Processor for all costs incurred resulting from providing reasonable assistance in dealing with a Data Subject request. In the event that the Processor is legally required to respond to the Data Subject, the Controller will fully cooperate with the Processor as applicable

9. Audit

9.1 The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with its processing obligations and allow for and contribute to audits and inspections.

9.2 Any audit conducted under this DPA shall consist of examination of the most recent reports, certificates and/or extracts prepared by an independent auditor bound by confidentiality provisions similar to those set out in the Agreement. In the event that provision of the same is not deemed sufficient in the reasonable opinion of the Controller, the Controller may conduct a more extensive audit which shall be: (i) at the Controller's expense; (ii) limited in scope to matters specific to the Controller and agreed in advance; (iii) carried out during the Processor's usual business hours and upon reasonable notice which shall be not less than 4 weeks unless an identifiable material issue has arisen; and (iv) conducted in a way which does not interfere with the Processor's day-to-day business.

9.3 This clause shall not modify or limit the rights of audit of the Controller, instead it is intended to clarify the procedures in respect of any audit undertaken pursuant thereto.

10. Personal Data Breach

10.1 The Processor shall notify the Controller without undue delay after becoming aware of (and in any event within 72 hours of discovering) any breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to any Personal Data ("**Personal Data Breach**").

10.2 The Processor shall take all commercially reasonable measures to secure the Personal Data, to limit the effects of any Personal Data Breach, and to assist the Controller in meeting the Controller's obligations under applicable law.

11. Compliance, Cooperation and Response

11.1 The Processor will notify the Controller promptly of any request or complaint regarding the processing of Personal Data, which adversely impacts the Controller, unless such notification is not permitted under applicable law or a relevant court order.

11.2 The Processor may make copies of and/or retain Personal Data in compliance with any legal or regulatory requirement including, but not limited to, retention requirements.

11.3 The Processor shall reasonably assist the Controller in meeting the Controller's obligation to carry out data protection impact assessments (DPIAs), taking into account the nature of the processing and the information available to the Processor.

11.4 The Controller shall notify the Processor within a reasonable time, of any changes to applicable data protection laws, codes or regulations which may affect the contractual duties of the Processor. The Processor shall respond within a reasonable timeframe in respect of any changes that need to be made to the terms of this DPA or to the technical and organisational measures to maintain compliance. If the Processor is unable to accommodate necessary changes, the Controller may terminate the part or parts of the Services which give rise to the non-compliance. To the extent that other parts of the Services provided are not affected by such changes, the provision of those Services shall remain unaffected.

11.5 The Controller and the Processor and, where applicable, their representatives, shall cooperate, on request, with a Supervisory Authority in the performance of their respective obligations under this DPA and Data Protection Law.

12. Liability

12.1 The limitations on liability set out in the Agreement apply to all claims made pursuant to any breach of the terms of this DPA.

12.2 The parties agree that the Processor shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Sub-processors to the same extent the Processor would be liable if performing the services of each Sub-processor directly under the terms of the DPA, subject to any limitations on liability set out in the terms of the Agreement.

12.3 The parties agree that the Controller shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Affiliates as if such acts, omissions or negligence had been committed by the Controller itself.

12.4 The Controller shall not be entitled to recover more than once in respect of the same loss.

13. Term and Termination

13.1 The Processor will only process Personal Data for the term of the DPA. The term of this DPA shall coincide with the commencement of the Agreement and this DPA shall terminate automatically together with termination or expiry of the Agreement.

14. Deletion and Return of Personal Data

14.1 The Processor shall delete all copies of Personal Data in its systems within 90 days of the effective date of termination of the Agreement unless : (i) applicable law or regulations require storage of the Personal Data after termination.; or (ii) partial Personal Data of the Controller is stored in backups, then such Personal Data shall be deleted from backups up to 1 year after the effective date of termination of the Agreement.

15. General

15.1 This DPA sets out the entire understanding of the parties with regards to the subject matter herein.

15.2 Should a provision of this DPA be invalid or become invalid then the legal effect of the other provisions shall be unaffected. A valid provision is deemed to have been agreed which comes closest to what the parties intended commercially and shall replace the invalid provision. The same shall apply to any omissions.

15.3 Subject to any provision of the SCCs to the contrary, this DPA shall be governed by the laws of England and Wales. The courts of England shall have exclusive jurisdiction for the settlement of all disputes arising under this DPA.

12.4 The parties agree that this DPA is incorporated into and governed by the terms of the Agreement.

Exhibit A

List of Parties, Description of Processing and Transfer of Personal Data, Competent Supervisory Authority

A. LIST OF PARTIES

The Exporter:

means the Customer.	
Address:	As set out for the Customer in the Agreement.
Contact person's name, position and contact details:	As provided by the Customer in its account and used for notification and invoicing purposes.
Activities relevant to the data transferred under the SCCs:	Use of the Services.
Signature and date:	By entering into the Agreement, the Exporter is deemed to have signed the SCCs incorporated into this DPA and including their Annexes, as of the Effective Date of the Agreement.
Role:	Controller.
Name of Representative (if applicable):	Any UK or EU representative named in the Exporter's privacy policy.

The Importer:

means Highlight: Highlight (SLM) Limited	
Address:	The Granary, Abbey Mill Business Park, Lower Eashing, Godalming, Surrey, GU7 2QW, England.
Contact person's name, position and contact details:	Richard Thomas dataprotection@highlight.net
Activities relevant to the data	The provision of cloud computing solutions to the Exporter under which the Importer processes Personal Data upon the

transferred under the SCCs:	instructions of the Exporter in accordance with the terms of the Agreement.
Signature and date:	By entering into the Agreement, the Importer is deemed to have signed the SCCs, incorporated into this DPA, including their Annexes, as of the Effective Date of the Agreement.
Role:	Processor
Name of Representative (if applicable):	https://www.datarep.com/data-request/

B. DESCRIPTION OF PROCESSING AND TRANSFERS

Categories of data subjects:	Employees, agents, advisors, consultants, freelancers of the Controller (who are natural persons). Users, Affiliates and other participants authorised by the Controller to access or use the Services in accordance with the terms of the Agreement. Prospects, customers, clients, business partners and vendors of the Controller (who are natural persons) and individuals with whom those end users communicate with by email and/or other messaging media. Employees or contact persons of Controller's prospects, customers, clients, business partners and vendors. Suppliers and service providers of the Controller. Other individuals to the extent identifiable in the context of emails of their attachments or in archiving content.
Categories of Personal Data:	The Controller may submit Personal Data to the Services, the extent of which is determined and controlled by the Controller. The Personal Data includes but is not limited to: • Personal details, names, email addresses of users of the Services. • Unique identifiers such as username, or password. • Personal Data derived from a user's use of the Services such as records and business intelligence information. • Personal Data within email and messaging content which identifies or may reasonably be used to identify, data subjects. • Meta data including sent, to, from, date, time, subject, which may include Personal Data. • IP address. • Geolocation based upon IP address. • Survey, feedback and assessment messages • Information offered by users as part of support enquiries • Other data added by the Controller from time to time

The frequency of the processing and transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous basis for the duration of the Agreement.
Nature of the processing:	Processing operations include but are not limited to: registering and authenticating users to the Services, providing updates on Services' features and usage changes, alerting users to network problems, and communicating with users in response to support requests.
Purpose(s) of the data transfer and further processing:	Personal Data is transferred to sub-contractors who need to process some of the Personal Data in order to provide their services to the Processor as part of the Services provided by the Processor to the Controller.
The period for which the Personal Data will be retained:	For the duration of the Agreement, subject to clause 14 of the DPA.
For transfers to (Sub-) processors, also specify subject matter, nature and duration of the processing:	The Sub-processor list accessed via http://highlight.net/legal/sub-processors sets out the Personal Data processed by each Sub-processor and the services provided by each Sub-processor.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies (e.g. in accordance with Clause 13 of the SCCs)	Where the EU GDPR applies, the Irish Data Protection Authority - The Data Protection Commission (DPC). Where the UK GDPR applies, the UK Information Commissioner's Office, (ICO). Where the FDPA applies, the Swiss Federal Data Protection and Information Commissioner, (FDPIC).

M

Exhibit B

Technical and Organisational Security Measures
(Including Technical and Organisational Measures to Ensure the Security of Data)

Below is a description of the technical and organisational measures implemented by the Processor (including any relevant certifications) 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.

Where applicable this Exhibit B will serve as Annex II to the SCCs.

Measure	**Description**
Measures of pseudonymisation and encryption of Personal Data	Passwords are not stored in plaintext but are hashed using an industry-standard algorithm. Data in transit is encrypted using TLS and browsers used to access the Services are forced to use a recent version of this encryption standard.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Availability: A mirror copy of the platform used to provide the Services is maintained in real-time using Azure mirror/backup facilities. Highlight has role-based access control with cascading privileges to provide granular control of user and administrator access. In accordance with “least privilege” and "need-to-know" principles, each user has only those rights which are necessary for the fulfilment of the task to be performed by the individual person. Users are required to re-validate their logins every 3 months through an email-based check. Data collection through SNMP is done using resilient pairs of collectors, and in the event of loss of the core platform, collectors will continue to collect data and buffer it locally until the main platform is restored.
Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident	The Services are bult using mirrored databases in geographically separate data centres. Access is by secure VPN and can be done from multiple diverse locations. The data centres can be switched in the event of flooding, earthquake, fire or other physical destruction or power outage protect Personal Data against accidental destruction and loss.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	The Processor has a third-party carry out a penetration and security audit of the platforms used to run the Services every 12 months. The Services are built using a development environment which uses unit testing, with a high degree of coverage, where a segment of the testing validates security effectiveness. These tests are automated and carried out on every build of the software.
Measures for user identification and	Users are identified using a login name (email address or, if

authorisation	implemented, using Secure Sign-On (SSO) via a user portal. Users are required to validate their logins, at intervals definable by the Controller / upstream Processor, using their email address. Administrator users (those with the necessary assigned privileges on the system) can manage the privileges of users within their domain or sub-folder on the Services, assigning privileges up to and including their own but never beyond it.
Measures for the protection of data during transmission	Data in transit is protected by Transport Layer Security ("TLS"). The front-end code from the Services insists that a user's browser uses a recent, approved version of TLS and will not allow a user session to be created if this condition is not met.
Measures for the protection of data during storage	Personal Data is only retained internally, and on the third party data centre servers, which are covered by Microsoft certifications.
Measures for ensuring physical security of locations at which Personal Data are processed	Microsoft Azure data centres are secured according to Microsoft standard, as set out at https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security
Measures for ensuring events logging	The Services automatically log a range of events, including security-related events for user accounts containing Personal Data: - User Login - User account Create, Update, Delete, Move - User Password change - User Administrative privileges change In addition, changes throughout the system are recorded in the events log together with the time, date, and user account which carried out the change.
Measures for ensuring system configuration, including default configuration	Creation of configurable elements within the system is done using a standard set of default, based on the action being carried out and the privileges of the user making the change.
Measures for internal IT and IT security governance and management	The Processor uses Microsoft Azure to host internal IT systems. Access to all systems and tools from outside the physical offices of the Processor is via secure VPN, and strict controls are placed on equipment used to connect to the company network including 100% encryption of disks on portable devices using Bitlocker, and enforcement of policies using InTune. WiFi access is done through a separate firewalled network and non-registered devices are forced to connect to an isolated WiFi environment which connects outside the firewall.
Measures for	The Processor utilises third party data centres that maintain

certification/assurance of processes and products	current ISO 27001 certifications. The Processor will only use third party data centres that maintain the aforementioned certifications and/or attestations, or that have other substantially similar or equivalent certifications and/or attestations. See:https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security
Measures for ensuring data minimisation	Personal Data (login information) which is not actively used for user authentication for a given period is first suspended, so that account is not accessible, and then after a confirmation period will be deleted.
Measures for ensuring data quality	All of the data processed is provided by the Controller. The Processor does not assess the quality of the data provided by the Controller. The Processor provides reporting tools within its product to help the Controller understand and validate the data that is stored. The Processor also uses a third party managed firewall in front of the server infrastructure which checks data for potential threats and blocks requests as required.
Measures for ensuring limited data retention	When a user account containing Personal Data is deactivated it will be permanently removed from the Processor's active databases. The data is retained in backups until they are replaced by more recent backups.
Measures for ensuring accountability	The Processor regularly reviews its information security policies to ensure they are still relevant and are being followed. The proper processing, security, management and ultimate deletion of user data is considered whenever changes to the Services affect it.
Measures for allowing data portability and ensuring erasure	The Services have built-in tools that allow the export of user data (for administrators with the correct privileges). The Services permanently delete user information from the primary platform when requested to do so by an administrator, and delete it from the secondary (backup) platform after a short interval.
Measures to be taken by the (Sub-) processor to be able to provide assistance to the Controller (and, for transfers from a Processor to a Sub-processor, to the Data Exporter).	The transfer of Personal Data to a third party (e.g. customers, sub-contractors, service providers) is only made if a corresponding contract exists, and only for the specific purposes. If Personal Data is transferred outside the EEA, the Processor provides that an adequate level of data protection exists at the target location or organisation in accordance with the European Union's data protection requirements, e.g. by employing contracts based on the EU SCCs.