Data Processing Agreement

The Customer enters into this Data Processing Agreement (**DPA**) on behalf of itself and, to the extent required under applicable Data Protection Legislation, in the name and on behalf of members of its Group to reflect the parties' agreement with regard to the Processing of Personal Data in relation to the provision of the Services by Benifex.

DATA PROCESSING TERMS

1. Definitions and interpretation

The following definitions and rules of interpretation apply to this DPA, in addition to the definitions set out in the Agreement (capitalised terms not defined below have the meaning given to them in the Agreement).

1.1 Definitions:

"Account Data" means Personal Data that relates to Customer's business relationship with Benifex, including to access Customer's billing information, Customer identity verification, or to fulfil Benifex's legal obligations (i.e. tax obligations);

"Business Purposes" the Software and Services to be provided by Benifex to the Customer, as set out in the Agreement;

"Commissioner" the Information Commissioner in the United Kingdom (see Article 4(A3), UK GDPR and section 114, DPA 2018);

"Controller, Processor, Data Subject, Processing and Supervisory Authority" have the meanings given to them in the Data Protection Legislation;

"Data Protection Legislation" means all applicable data protection and privacy legislation applicable to Benifex's Processing of Personal Data under this DPA, including but not limited to:

a) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2019 and the Data Protection Act 2018 (**UK GDPR**);

b) the General Data Protection Regulation ((EU) 2016/679) (**EU GDPR**);

c) the Swiss Federal Data Protection Act and its implementing regulations (**Swiss DPA**), and

d) all other legislation and regulatory requirements in force from time to time which apply to the Processing of Personal Data required in connection with the delivery and/or receipt of the Services.

"**Data Retention Policy**" means Benifex's Data Retention Policy available on the Benifex Legal Suite;

"EEA" the European Economic Area;

"Personal Data" means any personal data (as that term is defined in the Data Protection Legislation) that is processed by Benifex on behalf of the Customer in performance of the Services;

"Personal Data Breach" a breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data;

"Privacy Policy" means Benifex's privacy policy for the Services available on the Benifex Legal Suite.

"Restricted Transfer" means:

a) where the EU GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission;

b) where the UK GDPR applies, a transfer of personal data from the UK to any other country which is not based on adequacy regulations pursuant to Section 17A of the Data Protection Act 2018; and

c) where the Swiss DPA applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

"Standard Contractual Clauses (**SCCs**)**"** means:

a) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (**EU SCCs**);

b) where the UK GDPR applies:

   a. with the application of EU GDPR, the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, as such Addendum may be revised under Section 18 therein; or

   b. without the application of the EU GDPR, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c);

   (the **UK SCCs**);

c) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognised by the Swiss Federal Data Protection and Information Commissioner (in each case, as updated, amended or superseded from time to time).

"Sub-processor" means any sub-processor of Personal Data engaged by Benifex to assist it in fulfilling the Business Purposes, as set out in the list of Sub-processors available on the Benifex Legal Suite; and

"Usage Data" means technical and transactional data provided by or collected during the Customer's and Employee's use of the Services;

"UK Addendum" means the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, as such Addendum may be revised under Section 18 therein.

1.2 The Schedules form a binding part of the DPA.

1.3 In the case of conflict or ambiguity between the Agreement and this DPA, the following provisions shall take precedence:

(a) the DPA;

(b) the Agreement;

(c) the Privacy Policy.

To the extent there is any conflict between the Standard Contractual Clauses, and any other terms in this DPA, the Agreement, or the Privacy Policy, the provisions of the Standard Contractual Clauses will prevail.

2. Role of Benifex and Customer

2.1 The parties agree that Benifex is a processor (acting on behalf of the Customer as Controller), except where Benifex processes Personal Data, Account Data, or Usage Data as a Controller as set out in section 3. Benifex's processing of Personal Data as a Processor is set out section 4 for the purpose of the Data Protection Legislation:

3. Benifex as Controller

3.1 Customer and Benifex acknowledge and agree that Benifex acts as an independent Controller when Processing Personal Data, Account Data, and Usage Data for the purposes set out below:

(a) for the followings legitimate business purposes:

(i) to manage billing and Benifex's relationship with Customer, including performing Know-Your-Customer (KYC) and identity verification checks required to access or use the Services;

(ii) to carry out Benifex's core business operations, such as accounting, auditing, and tax calculations;

(iii) to prevent, detect, or investigate security incidents and manage the security of Benifex's platform and services;

(iv) to prevent, detect, or investigate abuse or misuse of the Services, including spam, fraud, illegal activities, or to assist telecommunications providers, regulators, or law enforcement agencies with, fraud, or illegal activities;

(v) for business analytics, internal reporting, financial reporting, forecasting capacity and revenue planning, and product strategy;

(vi) to develop and improve our products and services and to improve the performance, functionality, safety, and security of the Services; and

(vii) to comply with Benifex's legal and regulatory obligations;

(b) to provide digital gift cards when purchased by an Employee via the Discounts & Cashback Module,

provided that such Processing is in accordance with the Agreement, the Benifex Privacy Policy, and applicable law or regulation

3.2 Benifex will apply measures to minimise, anonymise, de-identify, and/or aggregate Usage Data, and to the extent practicable Personal Data and Account Data, used for the purposes set out in section 3.1, such that it does not (a) identify the Customer, Customer's Employees, or any Data Subject and (b) does not constitute Personal Data under applicable Data Protection Legislation. Benifex will not re-identify, or attempt to re-identify, any Personal Data, Account Data, and Usage Data.

3.3 Personal Data, Account Data, and Usage Data that is anonymised, de-identified, and/or aggregated by Benifex in accordance with section 3.2 is not Personal Data and any resulting derivative data created or arising out of or in connection shall not be Customer Data.

3.4 Further details are available within our Privacy Policy.

4. Benifex as Processor

4.1 The Customer retains control of the Customer Personal Data and remains responsible for its compliance obligations under applicable Data Protection Legislation, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to Benifex.

4.2 Schedule 1 describes the subject matter, duration, nature and purpose of the Processing and the Personal Data categories and Data Subject types in respect of which Benifex may process the Personal Data to fulfil the Business Purposes.

4.3 Benifex will in relation to Personal Data:

(a) only process the Personal Data as is necessary for the Business Purposes in accordance with the Customer's written instructions, as set out in this Agreement. Benifex must promptly notify the Customer if, in its opinion, the Customer's instructions do not comply with the Data Protection Legislation;

(b) additional instructions outside the scope of the Agreement or this DPA will be mutually agreed between the parties in writing, including any additional fees that may be payable by the Customer to Benifex to carry out such additional Processing instructions;

(c) maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third parties unless the Customer or this DPA specifically authorises the disclosure, or as required by domestic law, a court or a regulator (a **Permitted Disclosure**). In the event of a Permitted Disclosure, Benifex must first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the domestic law prohibits giving that notice;

(d) reasonably assist the Customer with its obligations under the Data Protection Legislation, taking into account the nature of Benifex's Processing and the information available to Benifex, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Commissioner or other relevant regulator under the Data Protection Legislation;

(e) implement and maintain, at its cost and expense, appropriate technical and organisational measures in relation to the Processing of Personal Data by Benifex so as to ensure a level of security in respect of the Personal Data Processed by it is appropriate to the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed (Benifex's current technical and organisational measures are set out in Schedule 2). Customer acknowledges that the security measures are subject to technical progress and development and that Benifex may update or modify the security measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services;

(f) ensure that all of its employees engaged and authorised by Benifex to process Personal Data commit to keeping the Personal Data confidential;

(g) notify the Customer without undue delay (and in any event within 48 hours) after becoming aware of any Personal Data Breach. Benifex will provide reasonable assistance to Customer in the event that Customer is required under applicable Data Protection Law to notify a regulatory authority or any data subjects impacted by a Personal Data Breach;

(h) keep detailed, accurate and up-to-date written records regarding any Processing of the Personal Data (the **Records**). Benifex will make the Records available to the Customer on their reasonable request and, subject to the audit provisions set out in the Terms and Conditions, allow for and contribute to audits, including inspections, conducted by the Customer or its audit agents, for the purpose of demonstrating compliance by Benifex with its obligations under Data Protection Legislation and under this DPA.

5. Obligations of Customer

5.1 Customer shall be responsible for ensuring that:

(a) all such notices have been given, and all such authorisations have been obtained, as required under applicable Data Protection Legislation, for Benifex (including its Group and Sub-processors) to process Customer Personal Data as contemplated by the Agreement and this DPA;

(b) it has complied, and will continue to comply, with all applicable Data Protection Legislation; and

(c) it has, and will continue to have, the right to transfer, or provide access to, Customer Personal Data to Benifex for Processing in accordance with the terms of the Agreement and this DPA.

5.2 The Customer acknowledges that as part of the Services being provided by Benifex, Personal Data may be transferred to third parties (including Benefit Providers and/or discounts providers accessible through the Discounts & Cashback Module) by Benifex on behalf of the Customer. The Customer acknowledges that such third parties are not sub-processors of Benifex.

6. Cross-border transfers of personal data

6.1 The Customer agrees that Benifex and its Sub-processors may transfer Personal Data to locations in which Benifex, its Group and Sub-processors maintain data processing operations, as set out in the Sub-Processor list.

6.2 The parties agree that when the transfer of Personal Data from Customer (as "data exporter") to Benifex (as "data importer") is considered a Restricted Transfer, applicable Data Protection Legislation may require that appropriate safeguards are put in place. For the purposes of such Restricted Transfers from Customer to Benifex, the transfer shall be subject to the appropriate Standard Contractual Clauses set out in Schedule 3, which shall be deemed incorporated into and form part of this DPA.

7. Sub-processors

7.1 Customer acknowledges and agrees that:

(a) members of the Benifex Group may be retained as Sub-processors (the existing Benifex Group Sub-processors are set out in the Sub-processor list); and

(b) Benifex and members of the Benifex Group may engage third-party Sub-processors to support the provision of the Services;

7.2 The engagement of Sub-processors is conditioned on the following requirements:

(a) Benifex will restrict the Sub-processor's access to Customer Personal Data only to what is strictly necessary to support the provision of the Services and in accordance with the Agreement, and Benifex will prohibit the Sub-processor from Processing the Customer Personal Data for any other purpose;

(b) Benifex will impose contractual data protection obligations, including appropriate technical and organisational measures to protect the Personal Data, on any Sub-processor it appoints and require such Sub-processor to protect Customer Personal Data to the standard required by applicable Data Protection Legislation; and

(c) Benifex shall remain fully liable to the Customer for any breach of this DPA which is caused by an act, error, or omission of its Sub-processors.

7.3 The Customer consents to the Sub-processors, their locations and Processing activities as set out in the Sub-processor list.

7.4 If Benifex updates its list of Sub-processors to change the identity of, or appoint a new, Sub-processor and that Sub-processor will be Processing Personal Data (a **New Sub-processor**):

(a) Benifex shall give Customer not less than thirty (30) days prior written notice of the intended appointment of the New Sub-processor, including reasonable information on the identity and location of the New Sub-processor and the nature of the Processing;

(b) Customer may object to Benifex's use of a New Sub-processor by notifying Benifex in writing within thirty (30) days of receipt of Benifex's notice referred to in clause 7.4(a) on the grounds that the Customer reasonably believes that the appointment of the New Sub-processor will have an adverse impact on the protection afforded to the Personal Data;

(c) if the Customer raises objections in accordance with clause 7.4(b), Benifex shall not appoint (or disclose any the Personal Data to) the New Sub-processor to process the Personal Data until Benifex and the Customer have agreed on reasonable steps to address the objections raised by the Customer;

(d) in the event that no such reasonable steps can be agreed between the Customer and Benifex within sixty (60) days from Benifex's receipt of the Customer's notice, then Benifex shall either:

(i) continue to process the Personal Data but shall not engage the New Sub-processor for such purpose; or

(ii) notify the Customer that it is unable to process the Personal Data without using the New Sub-processor in which event, notwithstanding anything in this DPA, the Customer may by written notice to Benifex with immediate effect terminate this DPA to the extent that it relates to the Software and Services which require the use of the New Sub-processor. Any discontinued use of the affected Software and Services will be without prejudice to any fees incurred by Customer prior to the discontinued use; and

(e) if the Customer does not object within the time period identified in clause 7.4(b), or where the Customer withdraws its objection, Benifex will deem the Customer to have authorised the New Sub-Processor and Benifex may appoint the New Sub-processor immediately.

8. Term and termination

8.1 This DPA will remain in force until the later of:

(a) the Term of the Agreement; or

(b) Benifex having deleted or returned the Personal Data in its possession or control.

9. Liability

9.1 Each party's liability whether in contract, tort (including negligence), breach of statutory duty, misrepresentation, restitution or otherwise shall be limited to the liability cap and subject to the exclusions set out in the Agreement.

9.2 Any claims arising out of or in connection with this DPA will be subject to the terms of the Agreement.

10. Data return and destruction

10.1 On the Customer's instructions and subject to Benifex's Data Retention Policy, Benifex shall without delay, securely delete all of the Personal Data unless:

(a) storage of any data is required by the Data Protection Legislation and, if so, Benifex shall inform the Customer of any such requirement; or

(b) Benifex requires storage of any data for the establishment, exercise or defence of legal claims.

11. Miscellaneous

11.1 The parties agree that this DPA shall replace and supersede any prior data processing agreement that Benifex and Customer may have previously entered into in connection with the Services.

11.2 In no event does this DPA restrict or limit the rights of any data subject or of any competent supervisory authority.

11.3 In the event of a conflict (whether actual or perceived) between applicable Data Protection Legislation, the parties shall comply with the higher requirement or standard.

11.4 Notwithstanding anything to the contrary in the Agreement, Benifex reserves the right to make any modification to this DPA as required to comply with applicable Data Protection Legislation. Benifex will provide Customer with at least thirty days' written notice of such amendments, during which time the Customer may reasonably object. If the Customer raises a reasonable

objection, the parties will work together to agree appropriate measures to ensure compliance with the applicable Data Protection Legislation.

Schedule 1

Data Processing Details

The following table sets out the Data Processing Details regarding each of the Services.

Service/Module	Subject Matter, Nature & Purpose	Duration, Frequency	Type of Personal Data*	Categories of Data Subject
Online Benefits	Benifex provides a global platform which incorporates several software modules to facilitate employee benefits, reward and engagement services for its customers and their employees. Personal Data will be processed as necessary to provide the Services under the Agreement. Benifex does not sell customers' personal data or employees' personal data and does not share such personal data with third parties for compensation or for those third parties' own business interests.	The duration of the Agreement. Continuous provision of Personal Data.	Employee ID; first name; last name; email address; job title; department; business unit; country; date of birth; gender; manager; user claim receipts; salary details; passport number (where expressly instructed by the Customer).	Employees (as defined in the Agreement) and their dependents.
Online Total Reward Statements			Employee ID; first name; last name; salary details	Employees (as defined in the Agreement).
Pension Auto-Enrolment (Enroller)			Employee ID; first name; last name; date of birth; address; email address; salary details; national insurance details; gross qualifying earnings	
Discounts & Cashback			Employee ID; first name; last name; email address; billing address; debit card details; bank details	
Benefit Accounts			Employee ID; first name; last name; email address; job title; department; business unit; country; date of birth; gender; health details (where required by the insurance provider, applicable to APAC only)	

Communications Manager			First name; last name; email address; email contents	
Recognition			Employee ID; first name; last name; email address; job title; department; business unit; country; date of birth; gender; manager	
Reward			Employee ID; first name; last name; email address; job title; department; business unit; country; date of birth; gender; manager	
Wellbeing			Employee ID; first name; last name; email address	
Wallet			Employee ID; first name; last name; initials; date of birth; email address; job title; mobile number; billing address; delivery address; card number; IBAN; IP address	
Communications, Global Foundation Campaign, Global Campaign and Global Communications Toolkit Services			First name; last name; email address; email contents	

* The types of personal data set out above are a non-exhaustive example of the personal data required to deliver the Services. Additional personal data may be processed depending on the Customer's specific Processing instructions. A complete list of the Personal Data shall be agreed between the parties and form part of the data input specification documentation, created during implementation of the Services.

Schedule 2

Technical and Organisational Security Measures

Benifex's technical and organisational security measures are set out below. Where applicable, this Schedule 2 will serve as Annex II to the EU Standard Contractual Clauses and the Table 3 of the UK International Data Transfer Agreement.

Benifex employs a continuous improvement programme in relation to its technical and organisational security. As such, the technical and organisational security measures shall be amended from time to time; however, such amendments shall not diminish the existing level of security in place protecting our customers' data.

Technical and Organisational Security Measure	Evidence of Technical and Organisational Security Measures
Measures of pseudonymisation and encryption of personal data	• All data sent to or from Benifex is encrypted in transit using TLS 1.2. • Customer Personal Data is encrypted at rest using 256-bit encryption. • All Benifex datastores used to process Customer Data are configured and patched to industry-recognised system-hardening standards and our associated procedures laid out by ISO 27001 code of practice for Information Security controls.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services	• Benifex has implemented formal procedures for handling security events. Benifex operates a 24x7 Security Operations Centre (**SOC**) with an incident escalation function, ready to immediately respond to, and mitigate, any Customer impacting issues. When the SOC detect security events, it is escalated to the internal platform and security teams who will notify the Emergency Response Team (**ERT**) to assemble and rapidly address the event and where necessary will include a forensics team. After a security event is contained and mitigated, relevant teams shall document the incident in full including a Root Cause Analysis (**RCA**). All incident reports will be reviewed and distributed to senior management and infrastructure teams to ensure action items identified will make the detection and prevention of a similar event easier should the event occur again. • All Customer Data is stored in the UK, EEA and Singapore (only on specific request by our customers). All sites have local and regional backup facilities for disaster recovery. • Benifex infrastructure uses Google Cloud Platform (**GCP**) and Azure, both reputable Infrastructure-as-a-Service providers. Benifex leverages their globally redundant services to ensure Services run reliably. Benifex benefits from the ability to dynamically scale up, or completely re-provision its infrastructure resources on an as-needed basis across our allocated geographical areas for production services, using GCP and its associated tools and Azure within the EU. This includes computing resources, storage and database resources, networking, and associated security. Every component in Benifex infrastructure is designed and built for high availability. • Benifex data security, high availability, and built-in redundancy are designed to ensure application availability and protect information from accidental loss or destruction. Benifex disaster recovery plan incorporates both zonal and geographic failover between Google UK and EU data centres and where necessary Singapore. All Benifex recovery and resilience mechanisms are tested regularly, and processes are updated as required. • Although Benifex has offices, we are not reliant on specific office locations to sustain operations. All operational access to infrastructure resources can be exercised at any location on the Internet. Benifex leverages a range of technologies and security related cloud tools to deliver uninterrupted remote work for all employees. • All Customer Data is encrypted at rest within the infrastructure and associated keys are rotated regularly to ensure continued security. • All Customer Data deleted by Benifex is deleted in accordance with our ISO 27001, 27017 and 27018 procedures to ensure data is deleted securely and in accordance with best practice from our GCP and Azure services.
Measures for ensuring the ability to restore the availability and access to personal data in a timely	• Benifex is certified to a combined management system for ISO 27001 and 22301 providing disaster recovery and continuity policy, procedures, and plans. The

manner in the event of a physical or technical incident	infrastructure has zonal and regional failover services to ensure the availability and restoration of Customer Data in the event of an incident.
Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the Processing	• Benifex regularly tests their security systems and processes to ensure they meet the requirements of our security policy and procedures and ensures that the physical and environmental security controls are audited to meet ISO 27001, 27017, 27018, 22301 and the UK Cyber Essentials certification. • Vulnerability scanning. The production infrastructure is scanned via GCP to ensure vulnerabilities are identified and reported to the platform team for action. The office infrastructure is monitored and reported by Defender. All associated logs will be correlated into Sentinel and monitored by the SOC team. All remediation will be conducted in good time and based on the associated criticality risk. • Penetration tests. Benifex contracts an independent CREST accredited third-party vendor to conduct 6 monthly penetration tests on their application and infrastructure services.
Measures for user identification and authorisation	• Single Sign-On (**SSO**) is used both internally by Benifex and can be used by customers to access our applications. • Logical Access Controls. Benifex assigns a unique ID to each employee utilising industry standard Identity Access Management services to control access rights to systems and systems Processing Customer Data. • All access to the Benifex infrastructure and systems Processing Customer Data is protected by Multi Factor Authentication (**MFA**). • Benifex restricts access to Customer Data to only those people with a "need-to-know" for a permitted purpose and following least privileges principles. • Benifex regularly reviews (at least every 90 days) the list of people and systems with access to Customer Data and removes accounts upon termination of employment or a change in job status that results in employees no longer requiring access to Customer Data. • Benifex mandates and ensures the use of system-enforced "strong passwords" in accordance with the best practices (described below) on all systems hosting, storing, Processing, or that have or control access to Customer Data and will require that all passwords and access credentials are kept confidential and not shared among personnel. • Password best practices are implemented by Benifex. Initial passwords must contain at least 9 characters, thereafter, further access requires a minimum of 12 characters. Passwords must meet the following criteria: a. must contain lowercase and uppercase letters, numbers, and a special character; b. cannot be part of a vendor provided list of common passwords. • Benifex maintains and enforces "account lockout" by disabling accounts with access to Customer Data when an account exceeds more than ten consecutive incorrect password attempts. • Benifex operates an internal Wi-Fi network for conditional internet access only. All access to Benifex resources and systems storing customer data is protected by strong passwords and MFA. • Benifex monitors both the office and production systems and implements and maintains security controls and procedures designed to prevent, detect, and respond to identified threats and risks. • Strict privacy controls exist in the application and associated databases, they are logically separated to ensure data privacy and to prevent one customer from accessing another customer's data.
Measures for the protection of data during transmission	• All email communication is conducted over a TLS1.2 connection. Any transmission of data files will also be AES 256 zip encrypted. All user interaction with web applications is protected by SHA 256 certificates and all SFTP transactions are also protected by SHA 256 certificates.
Measures for the protection of data during storage	• Intrusion Prevention: Benifex implements and maintains both physical and virtual network firewalls to protect data accessible via the Internet and will keep all Customer Data protected by the firewall at all times. • Benifex maintains its systems, software, and applications to ensure they are up to date with the latest upgrades, updates, bug fixes, patched vulnerabilities and other modifications necessary to ensure security of the Customer Data.

	• Security Awareness Training: Benifex employees conduct information Security and data protection training on joining and must take annual security, data protection and privacy training, whether they have access to Customer Data or not.
	• Benifex also uses the following:
	  • Anti-malware software and detection is provided at the mail gateway and is installed on all user devices and servers, with all anti-malware being updated on a regular basis.
	  • Endpoint security software is used via cloud services, enabling monitoring and reporting.
	  • All System events are logged, correlated, and monitored by the SOC.
	  • All access is logged, reported, and monitored by the SOC.
	  • MFA is used for all access into the infrastructure and customer data.
	• Benifex encrypts all backups of all customer data.

Measures for ensuring physical security of locations at which personal data are processed	• Physical Access Control. Benifex services and data are hosted in GCP facilities in the UK, Europe and Singapore and are protected by GCP in accordance with their security protocols. • Benifex has strict controls in place to ensure access to office infrastructure areas is controlled and only for approved personnel.
Measures for ensuring events logging	• All issued devices, servers, network infrastructure and applications have monitoring, reporting and correlated logging. These are all monitored by the SOC who will take appropriate action should anything be identified that poses a threat to Benifex and its customers.
Measures for ensuring system configuration, including default configuration	• Change and Configuration Management: Benifex has procedures in place for core services that are business as usual (**BAU**) to ensure services and applications are maintained and updated. Where services are likely to require a non-standard update, Benifex has change management procedures in place that requirs the associated Executive or nominated person to approve the change. Change management is conducted either as planned or emergency changes. In both cases, they must be approved by document or verbally initially for emergencies and then documented on completion of the change. • Change requirements are managed under ISO 27001 and 27002 to ensure Benifex has appropriate controls and documentation. Documents include Access control procedures, change management procedures, vulnerability management procedures, network, and server management procedures.
Measures for internal IT and IT security governance and management	• Information security management procedures are in accordance with the ISO 27001 standard and will be updated where required to meet the standard updates when released. • Information-related business operations continue to be carried out in accordance with the ISO 27001and ISO 22301 to ensure the continuity and recovery of Customer Data. • Benifex has documented an integrated Security and Continuity Management System with the associated controls for ISO 27001 and 22301. This includes an information security policy, business continuity policy and data protection policies. Benifex has multiple procedural documents that meet and exceed the mandatory document requirements for the certified standards held. They include but are not limited to: Risk management, incident reporting, data breach notification, asset management, data management, data destruction, server and network management, cloud service management, logging and monitoring, access control, corrective action, and change management.
Measures for certification/assurance of processes and products	• Benifex is certified to ISO 27001, ISO 22301 and the UK Cyber Essentials scheme. To ensure they are maintained in accordance with the standards, Benifex conducts internal audits annually and are externally audited by a UKAS accredited certification body annually. The ISO standards are recertified every 3 years and the UK Cyber Essentials is recertified annually.
Measures for ensuring data minimisation	• Data collection is limited to the purposes of Processing (or the data that the Customer chooses to provide).

	• Security measures are in place to provide only the minimum amount of access (least privilege) necessary to perform required functions. • Upon termination or expiry of this Agreement, Benifex will delete or return to Customer (at the Customer's election) all Customer Data (including copies) in its possession or control as soon as reasonably practicable and in any event within 90 days of termination or expiry of the Agreement, save that this requirement will not apply to the extent that Benifex is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data Benifex will securely isolate and protect from any further Processing, except to the extent required by applicable law.
Measures for ensuring data quality	• The customer (the data controller) provides the data to Benifex for the Services, and it is their responsibility for the accuracy and integrity of the Customer Data. • Benifex has processes in place to assist Customers and Data Subjects if they exercise their privacy rights. (Including a right to amend and update their Personal Data).
Measures for ensuring limited data retention	• See "*Measures for ensuring data minimization*" above.
Measures for ensuring accountability	• Benifex has implemented data protection policies. • Benifex follows a compliance by design approach. • Benifex maintains documentation of our Processing activities. • Benifex has appointed a Data Protection Officer, who is supported by the Benifex Legal Team. • Benifex adheres to relevant codes of conduct and signing up to certification schemes (see "Measures for certification/assurance of processes and products" above).
Measures for allowing data portability and ensuring erasure	• Secure Disposal: Return or Deletion, Benifex will permanently and securely delete all instances of the Customer Data in accordance with the Benifex data retention policy, unless Benifex and the Customer have agreed a separate exit plan or the Customer has instructed deletion in writing. • Archival data: When required by law to retain archival copies of Customer Data for regulatory purposes, it will be saved in our M365 or Azure file storage with appropriate back up, it will not be used for anything unless requested for audit purposes. • Benifex has a process that assists the Customer in responding to requests by Data Subjects to exercise their privacy rights (including a right to amend and update their Personal Data).

Technical and organizational measures to be taken by the processor to provide assistance to the controller and, for transfers from a processor to a Sub-processor.	• Should Benifex engage a third party as a Sub-processor, the following will take place:
	  • Prior to engaging new third-party service providers or vendors who will have access to Benifex / Customer Data, Benifex conducts a risk assessment of vendors' data security practices in accordance with the Benifex supplier management procedure.
	  • Benifex will restrict the onward Sub-processor's access to Customer Data only to what is strictly necessary to provide the Services, and Benifex will prohibit the Sub-processor from Processing the Personal Data for any other purpose.
	  • Benifex imposes contractual data protection obligations, including appropriate technical and organizational measures to protect personal data, on any Sub-processor it appoints that require such Sub-processor to protect Customer Data to the standard required by Applicable Data Protection Legislation.

Schedule 3

Standard Contractual Clauses

Cross-border transfers subject to the EU GDPR

1. The EU Standard Contractual Clauses will apply to Personal Data that is transferred via the Services from the EEA, Switzerland, Guernsey, or Jersey, either directly or via onward transfer, to any country or recipient outside the EEA, Switzerland, Guernsey, or Jersey that is not recognised by the relevant competent authority as providing an adequate level of protection for Personal Data.

2. For data transfers that are subject to the EU Standard Contractual Clauses, the EU Standard Contractual Clauses will be deemed entered into, and incorporated into this Addendum by this reference, and completed as follows:

   2.1. Module One (Controller to Controller) of the EU Standard Contractual Clauses will apply where Benifex is processing Personal Data pursuant to clause 3;

   2.2. Module Two (Controller to Processor) of the EU Standard Contractual Clauses will apply where Customer is a controller of Customer Personal Data, and Benifex is processing Personal Data pursuant to clause 4; and

   2.3. For each Module, where applicable:
   - 2.3.1. in Clause 7 of the EU Standard Contractual Clauses, the optional docking clause will not apply;
   - 2.3.2. in Clause 9 of the EU Standard Contractual Clauses, Option 2 will apply and the time period for prior written notice of sub-processor changes will be as set forth in clause 7.4(a);
   - 2.3.3. in Clause 11 of the EU Standard Contractual Clauses, the optional language will not apply;
   - 2.3.4. in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by Irish law;
   - 2.3.5. in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Ireland;
   - 2.3.6. in Annex I, Part A of the EU Standard Contractual Clauses:
     - **Data Exporter**: Customer
     - **Contact details**: The email address(es) designated by Customer in the Agreement.
     - **Data Exporter Role**: The Data Exporter's role is set forth in clauses 2.
     - **Signature and Date**: By entering into the Agreement, Data Exporter is deemed to have signed these EU Standard Contractual Clauses incorporated herein, including their Annexes, as of the effective date of the Agreement.
     - **Data Importer**: Benifex Limited.
     - **Contact details**: Benifex Legal Team - LegalTeam@Benifex.com
     - **Data Importer Role**: The Data Importer's role is set forth in 2, as applicable.

   - 2.3.7. in Annex I, Part B of the EU Standard Contractual Clauses:
     - The categories of data subjects are set forth in Schedule 1.
     - No Sensitive Data will be transferred.
     - The frequency of the transfer is a continuous basis for the duration of the Agreement.
     - The nature and purpose of the processing is set Schedule 1.
     - The period for which the personal data will be retained is set out in Benifex's Data Retention Policy (a copy of available on the Benifex Legal Suite).
     - For transfers to sub-processors, the subject matter, nature, and duration of the processing is set out in the Sub-processor List;

   - 2.3.8. in Annex I, Part C of the EU Standard Contractual Clauses: The Irish Data Protection Commission will be the competent supervisory authority; and
   - 2.3.9. Schedule 2 (Technical and Organizational Security Measures) serves as Annex II of the EU Standard Contractual Clauses.

Cross-border transfers subject to the UK GDPR

1. Customer and Benifex agree that the UK International Data Transfer Agreement will apply to Personal Data that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognised by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for Personal Data.

2. For data transfers from the United Kingdom that are subject to the UK International Data Transfer Agreement, the UK International Data Transfer Agreement will be deemed entered into, and incorporated into this Addendum by this reference, and completed as follows:

2.1. In Table 1 of the UK International Data Transfer Agreement, Customer's and Benifex's details and key contact information are set forth in the Commercial Terms;

2.2. In Table 2 of the UK International Data Transfer Agreement, information about the version of the Approved EU SCCs, modules, and selected clauses, which the UK International Data Transfer Agreement is appended to, are set forth in Section 2.4 (EU Standard Contractual Clauses) of this Schedule 3;

2.3. In Table 3 of the UK International Data Transfer Agreement:

- The list of Parties is set forth in the Commercial Terms.
- The description of the transfer is set forth in Schedule 1.
- Annex II is located in Schedule 2.
- The list of sub-processors is available on the Benifex Legal Suite; and

2.4. In Table 4 of the UK International Data Transfer Agreement, both the Importer and the Exporter may end the UK International Data Transfer Agreement in accordance with the terms of the UK International Data Transfer Agreement.

Cross-border transfers subject to an Alternative Transfer Mechanism

To the extent that Benifex adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses adopted pursuant to applicable Data Protection Legislation) (**"Alternative Transfer Mechanism"**), the Alternative Transfer Mechanism shall, upon notice to Customer and an opportunity to object, apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with applicable Data Protection Legislation applicable to Europe and extends to territories to which Customer Personal Data is transferred).