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

Further details of 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 transmitted to or from Benifex systems is encrypted in transit using Transport Layer Security (TLS) 1.2 or higher. • Customer Personal Data is encrypted at rest using strong, industry-standard algorithms such as AES 256-bit. • Encryption keys are managed through a controlled key-management process aligned with ISO 27001 Annex A controls, with access restricted to authorised personnel under multi-factor authentication. • Pseudonymisation is applied whenever processing does not require direct identifiers, which is achieved by separating identifying data from attribute data and using system-generated references. • Non-production environments use only pseudonymised or synthetic data unless explicitly requested by the customer and agreed by Benifex.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services	• Benifex maintains formal procedures for identifying, reporting and managing information-security and data-protection incidents in accordance with its internal Policies. Security events are centrally logged and monitored through managed alerting systems, with defined escalation paths for incidents detected outside regular business hours. Confirmed incidents are classified by severity and escalated to operational and security teams under the coordination of an Emergency Response Team, which oversees containment, eradication and communication with relevant customers, authorities and stakeholders. Following mitigation, incidents are documented with a root-cause analysis, and resulting action items are tracked to completion through a senior management review. • All Customer Personal Data is processed within secure Benifex-managed hosting environments located in the UK, EEA or the EU. Singapore-based hosting is also available upon specific customer request. • The production infrastructure is designed for high availability through redundancy and geographical separation, providing automatic failover and continuous service availability. Backup data is replicated across distinct secure locations and periodically tested to verify integrity and restorability. Customer environments are logically segregated to prevent unauthorised access or data mixing. Physical and environmental controls are implemented at all hosting facilities, and operational access is granted in accordance with controlled change-management procedures. • Benifex's infrastructure and information-security design emphasises resilience through layered redundancy, zonal and geographic failover, and tested disaster-recovery procedures. Recovery mechanisms and continuity plans are regularly reviewed, tested, and updated as needed to reflect changes in technology or risk. • Benifex's operations are not dependent on specific office locations. All critical systems and administrative interfaces are securely accessible via the internet, utilising strong authentication and authorisation controls, which enable continuity of operations in a remote work scenario. • Customer Personal Data is encrypted at rest, and encryption keys are rotated periodically in accordance with Benifex's key-management policies. Data deletion follows ISO 27001 aligned procedures to ensure secure and irreversible removal of data from our storage media.
Measures for ensuring the ability to restore the availability and access to personal data in a	• Benifex maintains an integrated management system compliant with ISO 27001 (Information Security) and ISO 22301 (Business Continuity). These frameworks define and govern the disaster-recovery and continuity procedures for all environments where Customer Personal Data is being processed.

timely manner in the event of a physical or technical incident	• Business continuity and disaster-recovery plans define responsibilities, escalation routes, and communication channels to ensure coordinated response in the event of an incident affecting system availability or data access. • The hosting infrastructure incorporates zonal and regional redundancy, as well as automatic failover capabilities, to ensure service continuity. Backup data is encrypted, stored in secure and geographically separate locations within the UK, EU, EEA and Singapore (only on specific request by our customers), and routinely tested to verify restorability and data integrity. • Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are defined for critical services and are periodically reviewed to confirm that targets remain achievable as systems evolve. Restoration tests are scheduled at least annually, and lessons learned are incorporated into updated procedures. • Benifex performs supplier-continuity reviews to confirm that key service providers maintain equivalent business-continuity capabilities, ensuring that recovery of dependent systems and data can be achieved within defined timeframes.
Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	• Benifex maintains a structured programme for testing and evaluating the effectiveness of its technical and organisational controls in accordance recognised international standards (i.e. ISO). • Security systems, configurations and processes are regularly reviewed to confirm compliance with internal information-security policies and procedures. Physical and environmental controls are included in internal and external audits conducted as part of the ISO certification cycle. • Automated vulnerability scanning is performed on production systems and network infrastructure to identify potential weaknesses. Findings are prioritised and remediated based on risk and criticality, with progress tracked through defined change management and risk treatment procedures. • Office endpoints and networks are continuously monitored using enterprise-grade detection tools to identify malicious or unauthorised activity. • Independent third-party penetration testing of Benifex applications and infrastructure is conducted regularly by accredited security specialists. The frequency and scope of these tests are periodically reviewed to ensure comprehensive coverage of all relevant assets and technologies. • Results from all security assessments are documented, risk-rated and reported to senior management, with corrective actions tracked to completion and used to inform continual improvement of our ISMS. • Restoration exercises include periodic, scoped recovery tests from backups to verify the recoverability of critical services and data under the principle of least privilege.
Measures for user identification and authorisation	• Benifex operates a centralised Identity and Access Management (IAM) platform that integrates with its internal HR and personnel directory systems for automated provisioning and de-provisioning of user accounts. Each user is issued a unique corporate identity; shared or generic accounts are prohibited. • Access to internal and production systems is authenticated through Single Sign-On (SSO) backed by Multi-Factor Authentication (MFA) using either hardware tokens or secure authenticator applications. • Role-Based Access Control (RBAC) governs access to applications, infrastructure and data stores. Roles are defined per function, reviewed quarterly, and approved by system owners following the principle of least privilege. • Privileged administrative access requires additional approval and is limited to authorised personnel within the Information Security or Platform Operations teams. Such sessions are logged in full and monitored through central security tooling. • Password policies align with NIST SP 800-63 B and ISO requirements. • Account lockout is triggered after several consecutive failed authentication attempts. Locked accounts require an administrative reset and verification. Idle sessions are automatically terminated after a defined period of inactivity. • Access to Customer Personal Data is granted strictly on a need-to-know basis. All access requests and approvals are recorded and retained for audit. Access rights are reviewed formally at least once a year and upon any change in role or employment. • Internal office networks are logically segmented from production networks. Access to environments processing Customer Personal Data occurs only through secure management gateways that enforce MFA, device-compliance checks, and conditional-access rules.

	• Continuous monitoring detects unauthorised or anomalous authentication events, with alerts integrated into Benifex's central incident-management process. • Within Benifex's applications and databases, tenant-level logical separation ensures that each Customer's Personal Data is isolated from others and accessible only within its designated context.
Measures for the protection of data during transmission	• All email communication is protected by Transport Layer Security (TLS) 1.2 or higher during transmission. • User data files are transferred using Secure File Transfer Protocol (SFTP) over SSH with key-based authentication. When required, files are additionally encrypted with OpenPGP using AES-256 encryption. • End-user interactions with Benifex web applications are protected by TLS 1.2 or higher, using modern cipher suites such as AES-256-GCM or ChaCha20-Poly1305. TLS certificates used in Benifex systems are signed using SHA-256 or stronger algorithms to maintain confidentiality and integrity. • Internal communication between Benifex offices and hosting environments is secured through routed encrypted tunnels using industry-standard protocols, providing mutual authentication between trusted endpoints.
Measures for the protection of data during storage	• Benifex maintains both physical and virtual firewalls, intrusion-prevention systems, traffic filtering, and behavioural-monitoring solutions to protect internet-facing systems processing Customer Personal Data. • Systems, software and applications are kept up to date through regular updates, upgrades, and vulnerability remediation to maintain the security of stored Customer Personal Data. • All backups of Customer Personal Data are encrypted at rest using strong algorithms such as AES-256. • Multi-Factor Authentication (MFA) is required for all access to infrastructure and systems processing Customer Personal Data. • Anti-malware protection is deployed at the mail gateway, on all internal user devices and servers, and updated automatically. Cloud-based endpoint security services offer continuous monitoring and reporting capabilities. • Use of removable media for storing Customer Personal Data is technologically restricted. Any authorised use for exceptional operational purposes is subject to approval, encryption, and secure sanitisation or destruction with evidence logged. • Encryption-key lifecycle includes periodic rotation, separation of duties, and dual-control for key-management activities.
Measures for ensuring physical security of locations at which personal data are processed	• Customer Personal Data is hosted in secure data centre environments operated by ISO-certified third-party providers. These environments implement layered physical security controls appropriate to their risk profile, which include physical access control systems, CCTV surveillance, intrusion detection, and 24/7 monitoring. • Physical access to secure data centre environments is restricted to authorised personnel, based on operational necessity, and is logged and periodically reviewed. The physical security posture of all hosting providers is regularly assessed as part of Benifex's supplier risk management process. • Facilities operate multiple security zones to restrict movement within sensitive areas. Visitors are registered and, where applicable, escorted while on the premises. • Environmental protections include continuous monitoring of temperature and humidity, automatic fire detection and suppression systems, and redundant power supply through uninterruptible power systems (UPS) and backup generators. • Security systems, including intrusion alarms, fire suppression, and power redundancy, are regularly inspected and tested to verify their effectiveness. • Access to Benifex offices is controlled through individual access-card systems, restricted to authorised personnel, and reviewed at least annually. Areas housing on-premises network or infrastructure equipment are physically separated from the general office space.
Measures for ensuring events logging	• Benifex maintains formal change and configuration-management processes to ensure that all systems, infrastructure, and applications are deployed, configured, and updated securely. • Standard changes, which are part of normal operations, follow documented procedures to verify testing, peer review, and approval before implementation.

	• Non-standard or emergency changes require prior authorisation from an executive or designated approver and are recorded with full details of scope, timing, and risk assessment. • System configurations follow secure baseline standards that disable unnecessary services and enforce security-hardened defaults. • All changes are logged and subject to post-implementation review to confirm successful completion and identify any required corrective actions. • Configuration and change controls are aligned with ISO 27001 requirements and are periodically reviewed to ensure continued effectiveness.
Measures for ensuring system configuration, including default configuration	• Change and Configuration Management: Benifex have documented procedures in place for core services and applications to ensure they are maintained and updated. Where services are likely to require a non-standard update, Benifex have change management procedures in place that requires 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 management processes are governed by ISO27001 and follow industry best practices to ensure changes are risk-assessed, authorized, tested, and documented in a controlled manner. Documents include Access control procedures, change management procedures, vulnerability management procedures, network, and server management and hardening principles,
Measures for internal IT and IT security governance and management	• Benifex maintains an integrated Security and Continuity Management System, aligned with ISO 27001 and ISO 22301, which defines governance, oversight, and continual improvement processes for information security and business continuity. • Security governance is overseen by the Group Chief Information Security Officer, with support from management representatives from Technology, Legal, and Operations. Responsibilities and authority for information security are clearly defined and communicated. • Information-security objectives, key risk indicators, and performance metrics are established and regularly reviewed by management. • Benifex conducts internal audits, management reviews, and risk assessments to verify the suitability and effectiveness of its security controls. • Information-security management procedures are reviewed and updated as required to remain aligned with ISO 27001 and evolving operational or regulatory requirements. • Secure development and deployment practices are integrated into the management system, including secure coding standards, peer code review, automated vulnerability scanning, dependency control, and segregation of development, testing, and production environments. • New systems and suppliers undergo security and privacy assessments before implementation. Third-party services with access to Customer Personal Data are subject to supplier-risk reviews and ongoing monitoring. • Access rights, system configurations, and other technical controls are reviewed regularly to ensure compliance with internal standards. • Employees and contractors receive mandatory information security, data protection, and privacy training upon onboarding and regularly thereafter. • The management system includes defined processes for incident management, risk treatment, corrective action, and continuous improvement to ensure timely response and learning from security events. • Governance of information-related operations is supported by regular management reviews, internal assessments, and improvement actions to maintain the effectiveness of security and continuity measures.
Measures for certification/assurance of processes and products	• Benifex maintains an Information Security Management System and a Business Continuity and Risk Programme. • Compliance with these standards is ensured through an integrated audit and review programme, including: (i) Internal audits are conducted at least annually to verify the implementation and effectiveness of the management system;

	(ii) External surveillance audits are performed; and (iii) Audit findings and improvement actions tracked through the management system to ensure continual enhancement of security, privacy, and continuity processes.
Measures for ensuring data minimisation	• Access to systems and Customer Personal Data is restricted according to the principle of least privilege. • Authorisations are role-based, reviewed regularly, and revoked immediately upon termination or role change. • Administrative access requires MFA and is logged, monitored, and periodically reviewed to ensure appropriateness. • Automated and policy-driven retention schedules ensure that Customer Personal Data is stored only for as long as necessary to fulfil the defined processing purpose or legal obligations. • The collection and processing of Customer Personal Data are limited to what is required to deliver contracted services and to the purposes defined by the Customer in the applicable Data Processing Agreement. • Upon termination or expiry of the Agreement, Benifex securely deletes or returns Customer Personal Data in accordance with the Data Processing Agreement, ensuring all copies, including backups, are removed from active systems within defined retention periods as set out in our Data Retention Policy.
Measures for ensuring data quality	• Benifex processes Customer Personal Data strictly in accordance with the instructions provided by the Customer, who acts as data controller and remains responsible for ensuring the initial accuracy and completeness of the data. • To support data consistency and reduce the risk of malformed or incomplete records, Benifex systems apply format and structure validation at the point of import (e.g., required fields, correct data and file types, and value patterns). However, such technical safety measures do not assess the correctness of the underlying data, which remains the Customer's responsibility • Procedures are in place to support correction or update of Customer Personal Data upon verified request from the Customer or a data subject, ensuring that inaccurate or outdated information is rectified without undue delay. • All corrections and updates are logged and auditable in accordance with Benifex's information-security and privacy-management controls.
Measures for ensuring limited data retention	• Customer Personal Data is retained only for as long as necessary to fulfil the contractual purpose or to comply with applicable legal or regulatory obligations. • Retention periods are defined and enforced through automated and policy-driven deletion routines that ensure the timely removal of data no longer required for processing. • Upon termination or expiry of the contractual relationship, Benifex securely deletes or returns Customer Personal Data in line with our Data Retention Policy, subject to our legal or regulatory obligations. • Back-ups containing Customer Personal Data are encrypted, isolated, and permanently deleted once their defined retention period expires. • Deletion processes are logged and periodically verified to confirm secure and complete removal of Customer Personal Data from active systems and storage media.
Measures for ensuring accountability	• Processing activities are documented and periodically reviewed through Records of Processing Activities (RoPA). • Benifex has appointed a Group Data Protection Officer, who is supported by the Benifex Legal Team. • Employees and contractors receive mandatory data protection and information security training at onboarding and regularly thereafter to ensure continued awareness and compliance. • Regular internal audits and risk assessments are conducted to evaluate adherence to policies, legal requirements, and contractual obligations. • Data protection and information security policies, procedures, and breach management processes are version-controlled, reviewed on a scheduled basis, and enforced through operational governance.

	• Any change to processing operations, including the introduction of new systems, technologies, or processing purposes, triggers formal review and, where necessary, a documented data processing impact assessment to ensure ongoing compliance.
Measures for allowing data portability and ensuring erasure	• Customer Personal Data can be extracted in a structured, commonly used, and machine-readable format to support data-portability requests initiated by the Customer or its data subjects. • Verified erasure requests are processed through documented internal procedures to ensure accurate, complete, and secure deletion across all relevant systems. • All portability and erasure actions are logged for auditability and processed within defined timelines in accordance with applicable data protection legislation. • Customer Personal Data is deleted at the end of the retention period unless continued storage is legally required or contractually agreed with the customer. • Where retention is required for regulatory purposes, data is archived in secure, access-restricted environments and used solely for compliance purposes.
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.	• Prior to engaging any new sub-processor, Benifex conducts a formal supplier risk assessment to evaluate the vendor's technical and organisational security measures and data-protection compliance. • Access to Customer Personal Data is restricted to what is strictly necessary for the sub-processor to perform the contracted services, and sub-processors are contractually prohibited from Processing the Personal Data for any other purpose. • Benifex and each of its Sub-Processors enter into a data processing agreement that contain the requirements set out in applicable data protection legislation and any additional requirements as agreed with our customers. • Benifex applies privacy-by-design and privacy-by-default principles across its service architecture to ensure that data protection, transparency, and data-subject rights can be effectively supported. • Benifex reasonably, and without undue delay, supports the Customer in the management and investigation of potential personal data breaches, according to applicable Data Protection Legislation, by undertaking comprehensive investigations in accordance with our Security Breach Policy . • Benifex shall reasonably assist the Customer, upon request, with data protection impact assessments or prior consultations with supervisory authorities, as applicable, taking into account the nature of processing and the information available to the processor, according to applicable data protection legislation. • Benifex shall reasonably assist the Customer in fulfilling data-subject rights requests under applicable data-protection law, including access, rectification, erasure, restriction, and portability. • Benifex maintains documentation of implemented information-security and data protection controls, relevant ISO certifications, internal audit findings, and Records of Processing Activities (RoPA). • Benifex notifies the Customer in advance of any intended addition or replacement of Subprocessors in accordance with the Data Processing Agreement.

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).