# Data Processing Agreement

This Data Processing Addendum (**DPA**), including its Schedules, forms part of and is incorporated into the Agreement entered into between Benefex and the Customer for the purchase of Software and Services from Benefex (identified in the Customer's Order Form).

The Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Legislation, in the name and on behalf of the Authorised Affiliates to reflect the parties' agreement with regard to the Processing of Personal Data. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates.

In the course of providing the Software and Services, Benefex may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data.

## AGREED 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.

1.1 Definitions:

**"Account Data"** means any Personal Data that relates to the Customer's relationship with Benefex, including any billing information and Personal Data used to maintain or improve performance of the Services, provide support, investigate and prevent system abuse or to fulfil our legal obligations;

**"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

**"Authorised Affiliate"** means any of Customer's Affiliate(s) which:

a) is subject to Data Protection Legislation, and

b) is permitted to use the Software Services pursuant to the Agreement between Customer and Benefex, but has not signed its own Order Form with Benefex;

**"Business Purposes"** the Software and Services to be provided by Benefex to the Customer, as set out in the Customer's Order Form;

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

**"Complaint"** means a complaint or request relating to either party's obligations under Data Protection Legislation relevant to this Agreement, including any compensation claim from a Data Subject or any notice, investigation or other action from a Supervisory Authority;

**"Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Processing"** have the meanings given to them in the Data Protection Legislation;

**"Customer Data"** shall have the meaning given to it in Schedule 1(b);

**"Data Protection Legislation"** means:

a) to the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of Personal Data; and

b) to the extent the EU GDPR applies, the law of the European Union or any member state of the European Union to which the Customer or Provider is subject, which relates to the protection of Personal Data;

**"Data Subject"** the identified or identifiable living individual to whom the Personal Data relates;

**"Discount Providers"** any discounts provider providing discounts in in the form of special offers, discounts, voucher codes and cashback, whose services are accessible through the Software.

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

**"EEA"** the European Economic Area;

**"International Data Transfer Agreement (IDTA)"** means the International Data Transfer Agreement issued by the Commissioner, as amended from time to time;

**"IDTA Addendum"** means the International Data Transfer Addendum to the Standard Contractual Clauses issued by the Commissioner's office under s.119A(1) of the Data Protection Act 2018, as such Addendum may be revised under Section 18;

**"Information Security Standards"** *the Information Security Standards*, as updated from time to time, and accessible via Benefex's webpage;

**"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;

**"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; and

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;

**"Standard Contractual Clauses (SCCs)"** means 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, as amended from time to time;

**"Sub-processor"** means any sub-processor engaged by Benefex;

**"Usage Data"** means data on the User's usage of the Software and Services, which Benefex monitors, aggregates and anonymises; and

**"UK GDPR"** has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

1.2 The Schedules form part of this DPA and will have effect as if set out in full in the body of this DPA.

1.3 A reference to writing or written includes email.

1.4 In the case of conflict or ambiguity between, the following provisions shall take precedence:

(a) the main body of the DPA;

(b) the Schedules within the DPA;

(c) SCC (if applicable); and

(d) the Agreement.

**2. Personal data types and processing purposes**

2.1 The Customer and Benefex agree and acknowledge that for the purpose of the Data Protection Legislation:

(a) the Customer is a Controller;

(b) Benefex acts as both a Processor and a Controller:

(i) Processor – Benefex acts as a Processor in relation to the Customer Data provided by the Customer, except where Benefex acts as a Controller;

(ii) Controller – Benefex acts as a Controller in relation to the: (x) Personal Data provided directly by the User for a specified purpose (including wellbeing analysis and cashback redemption), (y) the Account Data; and (z) Usage Data which Benefex aggregates and anonymises to provide the Analytics Module.

(c) Where the Customer is a Controller, the Customer retains control of the Personal Data and remains responsible for its compliance obligations under the 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 Benefex;

(d) where Benefex is a Controller, it shall undertake such processing in accordance with its legal obligations to Data Subjects under the Data Protection Legislation; and

(e) 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 Benefex may process the Personal Data to fulfil the Business Purposes.

**3. Obligations of Benefex**

3.1 Benefex will only process the Customer's Personal Data as is necessary for the Business Purposes in accordance with the Customer's written instructions, as amended from time to time. Benefex must promptly notify the Customer if, in its opinion, the Customer's instructions: (i) do not comply with the Data Protection Legislation or (ii) Benefex is unable to follow the Customer's instructions for Processing of Personal Data.

3.2 The Customer acknowledges that some elements of the Software and Services may require Benefex to disclose all or part of the Customer Data to third-party providers (i.e. discount providers) in accordance with Business Purposes.

3.3 If Benefex is required to process Personal Data other than in accordance with the Customer's instructions, Benefex shall notify the Customer of any such requirement before Processing the Personal Data (unless the Data Protection Legislation prohibits such information on important grounds of public interest).

3.4 Benefex must comply promptly with any of the Customer's written instructions requiring Benefex to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised Processing.

3.5 Benefex will 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, court or regulator (including the Commissioner). If a domestic law, court or regulator (including the Commissioner) requires Benefex to process or disclose the Personal Data to a third party, Benefex 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 the giving of such notice.

3.6 Benefex will reasonably assist the Customer, at no additional cost to the Customer, with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of Benefex's processing and the information available to Benefex, 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.

**4. Benefex employees**

4.1 Benefex will ensure that all of its employees are committed to confidentiality obligations and have received appropriate training on compliance with the Data Protection Legislation.

**5. Security**

5.1 Benefex shall implement and maintain, at its cost and expense (taking into account those factors which it is entitled to take into account pursuant to the Data Protection Legislation) appropriate technical and organisational measures in relation to the

Processing of Personal Data by Benefex 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.

**6. Personal Data Breach**

6.1 Benefex will notify the Customer without undue delay (and in any event within 48 hours after becoming aware) of any Personal Data Breach.

6.2 Where Benefex becomes aware of a Personal Data Breach it shall, also provide the Customer with the following information:

(a) the nature of the Personal Data Breach, including the categories and approximate numbers of Data Subjects and Personal Data records concerned;

(b) the likely consequences of the Personal Data Breach; and

(c) any measures taken, or that Benefex recommends, to address the Personal Data Breach, including to mitigate its possible adverse effects,

provided that, if Benefex cannot provide all the above details within the 48 hour timeframe, it shall (before the end of this timeframe) provide the Customer with reasons for the delay and when it expects to be able to provide the relevant details (which may be phased) and shall give the Customer regular updates on these matters.

6.3 Taking into account the nature of processing and information available to Benefex, provide reasonable assistance to the Customer to assist the Customer in complying with its obligations pursuant to the Data Protection Legislation.

6.4 Benefex will not inform any third party, other than its advisors, insurers, or other members of the Benefex Group (or their advisors and insurers), of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data Breach without first obtaining the Customer's written consent, except when required to do so by domestic law.

**7. Cross-border transfers of personal data**

7.1 The Customer hereby acknowledges and agrees that Benefex and its Sub-processors may transfer Personal Data and Account Data to locations in which Benefex, its affiliates and Sub-processors maintain data processing operations, as set out in our *Sub-Processor list*.

7.2 Benefex shall only undertake a transfer of any Personal Data to an organisation outside both the United Kingdom and the EEA (an **International Recipient**) if the Customer has consented to the transfer and to the mechanism of the transfer in writing (such consent not to be unreasonably withheld or delayed) or if such transfer is to a member of the Benefex Group.

7.3 If Benefex does transfer any Personal Data to an International Recipient, Benefex shall do so under the following conditions:

(a) the Personal Data is being processed in a territory which is subject to a then current finding under the Data Protection Legislation that the territory provides adequate protection of the privacy rights of individuals;

(b) Benefex participates in a valid cross-border transfer mechanism under the Data Protection Laws, and has entered into an agreement with each Data Processor or Sub-processor (where applicable) which includes valid cross-border transfer mechanism for transfers from the UK or the EU to Data Processors established in third countries, as made available by the relevant Supervisory Authority from time to time; or

(c) Benefex has implemented appropriate safeguards in accordance with Article 46 UK GDPR.

7.4 If any Personal Data or Account Data transfer between the Customer and Benefex requires valid cross-border transfer mechanisms in order to comply with the Data Protection Legislation (where the Customer is the entity exporting Personal Data to Benefex outside the EEA), Schedule 2 shall apply, and the parties shall take all other actions required to legitimise the transfer.

**8. Sub-processors**

8.1 Subject to clauses 8.2 and 8.3, Benefex shall not engage another Processor for carrying out any processing activities in respect of the Personal Data without the Customer's prior written consent.

8.2 The Customer consents to the appointment of the Sub-processors and to the Processing of Personal Data as set out in Schedule 1. If Benefex proposes to change the identity of, or appoint a new, Processor (in addition to the Sub-processors) and that Processor will be Processing the Personal Data (**New Sub-processor**):

(a) Benefex shall give the Customer not less than 20 Business 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) the Customer may object to the appointment of the New Sub-processor within 20 Business Days of receipt by the Customer of the notice referred to in clause 8.2(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 8.2(b) Benefex shall not appoint (or disclose any the Personal Data to) the New Sub-processor to process the Personal Data until Benefex and the Customer have agreed on reasonable steps to address the objections raised by the Customer (including, where necessary) by Benefex providing additional information;

(d) in the event that no such reasonable steps can be agreed between the Customer and Benefex within 40 Business Days from Benefex's receipt of the Customer's notice, then Benefex shall either:

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

(ii) shall 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 Benefex 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; and

(e) if the Customer does not object within the time period identified in clause 8.2(b), or where the Customer withdraws its objection, Benefex may appoint the New Sub-processor immediately.

8.3 Where Benefex engages a Sub-processor to carry out activities which involve the processing of Personal Data, Benefex shall:

(a) carry out appropriate due diligence of such Sub-processor;

(b) engage such Sub-processor on written terms which comply with the Data Protection Legislation; and

(c) remain fully liable to the Customer for the Sub-processor's failure to fulfil its obligations in relation to Personal Data.

**9. Complaints, data subject requests and third-party rights**

9.1 Each party shall promptly inform the other party if it receives a Complaint and provide the other party with full details of such Complaint.

9.2 Benefex shall:

(a) taking into the nature of the processing, assist the Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to Data Subject's requests;

(b) record and then refer all Data Subject requests it receives to the Customer, without undue delay (and in any event within 48 hours of receipt);

(c) provide such assistance to the Customer as the Customer reasonably requests in relation to a Data Subject request; and

(d) not respond to any Data Subject request without the Customer's prior written approval.

**10. Term and termination**

10.1 This DPA will remain in full force and effect so long as:

(a) the Agreement remains in effect; or

(b) Benefex retains any of the Personal Data related to the Agreement in its possession or control.

10.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Agreement in order to protect the Personal Data will remain in full force and effect.

**11. Liability**

11.1 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.

**12. Data return and destruction**

12.1 In accordance with the Customer's instructions and subject to Benefex's data retention policy, Benefex 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, Benefex shall inform the Customer of any such requirement; or

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

**13. Records**

13.1 Benefex shall keep detailed, accurate and up-to-date written records regarding any Processing of the Personal Data, including but not limited to, the access, control and security of the Personal Data, approved Sub-processors, the Processing purposes, categories of Processing, any transfers of personal data to a third country and related safeguards, and a general description of the technical and organisational security measures referred to in clause 5 (the **Records**).

13.2 Benefex will ensure that the Records are sufficient to enable the Customer to verify Benefex's compliance with its obligations under this DPA and Benefex will provide the Customer with copies of the Records upon request.

**14. Audit**

14.1 Subject to any audit provisions set out in the Agreement, Benefex shall allow for and contribute to audits, including inspections, conducted by the Customer or its audit agents, for the purpose of demonstrating compliance by Benefex with its obligations under Data Protection Legislation and under this DPA.

**15. Notice**

15.1 Any notice given to a party under or in connection with this DPA must be provided in accordance with the notice provisions set out in the Agreement.

## Schedule 1

### Details of Processing

#### A. List of Parties

| | |
|---|---|
| Name of Data exporter: | The party identified as the "Customer" in the Agreement and this DPA |
| Address: | As set forth in the Agreement |
| Contact person's name, position, and contact details: | As set forth in the Agreement |
| Activities relevant to the data transferred under these Clauses: | See (B) below |
| Signature and date: | This DPA (including the Schedules) shall automatically be deemed executed when the Agreement is executed by Customer |
| Role (controller/processor): | Controller |

| | |
|---|---|
| Name of Data Importer: | As set forth in the Agreement |
| Address: | As set forth in the Agreement |
| Contact person's name, position, and contact details: | Benefex Legal Team – LegalTeam@benefex.co.uk |
| Activities relevant to the data transferred under these Clauses: | See (B) below |
| Signature and date: | This DPA (including the Schedules) shall automatically be deemed executed when the Agreement is executed by Benefex. |
| Role (controller/processor): | Processor and Controller |

#### B. Description of Processing/ Transfer

| | |
|---|---|
| **Categories of Data Subjects whose personal data is transferred** | **Modules One and Two**<br>Customer's Users who access the Software and Services. |
| **Categories of Personal Data transferred** | **Module One**<br>Account Data to the extent it constitutes Personal Data. |
| | **Module Two**<br>Any Customer Data processed by Benefex in connection with the Software and Services which constitutes Personal Data (including forename, surname, and contact details (etc)). |
| **Sensitive data transferred (if applicable) and applied restrictions or safeguards** | Benefex does not knowingly collect (and Customer shall not submit) any sensitive data or any special category data (as defined under the Data Protection Legislation). |
| **Frequency of the transfer** | Continuous. |
| | **Module One**<br>Personal data contained in Account Data will be processed to monitor, aggregate and anonymise |

| | |
|---|---|
| **Nature and purpose(s) of the data transfer and Processing** | data relating to the Users' usage of the Software and Services to: (i) continuously improve the software and services and (ii) enable the performance of the Benefex Analytics Module. |
| | **Module Two**<br>Personal Data contained in the Customer Data will be Processed as part of the following activities:<br><br>(1) Benefex provides numerous Software Modules to facilitate communication, interaction and engagement between the Customer and its Users. The Service will consist of providing the Software to the Customer in order to improve its employee engagement in accordance with the Agreement.<br><br>(2) Benefex will Process such Personal Data as is necessary to provide the Software and Services under the Agreement. |
| **Retention period (or, if not possible to determine, the criterial used to determine the period)** | **Module One**<br>Once the Account Data is aggregated and anonymised it shall no longer constitute Personal Data. The Account Data shall be retained as long as is required (a) to provide the Services to the Customer, (b) for Benefex's lawful and legitimate business needs; and (c) in accordance with the Data Protection Legislation. |
| | **Module Two**<br>Upon termination or expiry of this Agreement, Benefex will (at the Customer's election) delete or return to the Customer all Customer Data (including copies) in Benefex's possession or control as soon as reasonably practicable and in accordance with Benefex's data retention policy, save that this requirement will not apply to the extent that Benefex 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 Benefex will securely isolate and protect from any further Processing, except to the extent required by applicable law. |
| **For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing** | **Module Two**<br>Benefex will restrict the onward Sub-processor's access to Customer Data only to what is strictly necessary to provide the Software and Services in accordance with the Agreement, and Benefex will prohibit the Sub-processor from processing the Personal Data for any other purpose.<br><br>Benefex imposes contractual obligations, including appropriate technical and organisational measures to protect Personal Data, on any Sub-processors it appoints that require such Sub-processor to protect Customer Data to the standard required by the Data Protection Legislation. |
| **Identify the competent supervisory authority/ies in accordance with Clause 13** | Where the EU GDPR applies, the competent supervisory authority shall be (i) the supervisory authority applicable to the data exporter in its EEA country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located.<br><br>Where the UK GDPR applies, the competent supervisory authority shall be the Commissioner. |

## Schedule 2

### Restricted Transfers of Personal Data

1. The parties agree that, if a Restricted Transfer of Personal Data from the Customer (as "**data exporter**") to Benefex (as "**data importer**") occurs, applicable Data Protection Legislation requires that appropriate safeguards be put in place.

2. In relation to Restricted Transfers of Account Data protected by the EU GDPR and processed in accordance with clause 2.1(b)(ii) of this DPA, the SCCs shall apply, completed as follows:

    a. Module One will apply;

    b. in Clause 7, the optional docking clause will apply;

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

    d. in Clause 17, Option 1 will apply, and the SCCs will be governed by Irish law;

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

    f. Annex I of the SCCs shall be deemed completed with the information set out in Schedule 1 to this DPA; and

    g. Subject to clause 5 of this DPA, Annex II of the SCCs shall be deemed completed with the information set out in Schedule 3 to this DPA;

3. In relation to Restricted Transfers of Personal Data that is protected by the EU GDPR, the SCCs shall apply, completed as follows:

    a. Module Two shall apply;

    b. in Clause 7, the optional docking clause will apply;

    c. in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in clause 8.2(a) of this DPA;

    d. in Clause 11, the optional language will not apply;

    e. in Clause 17, Option 1 will apply, and the SCCs will be governed by the law of the EU Member State in which the data exporter is established and if no such law by Irish law;

    f. in Clause 18(b), disputes shall be resolved before the courts of the EU Member State in which the data exporter is established and otherwise the courts of Ireland;

    g. Annex I of the SCCs shall be deemed completed with the information set out in Schedule 1 of this DPA; and

    h. Subject to clause 5 of this DPA, Annex II of the SCCs shall be deemed completed with the information set out in Schedule 3 to this DPA;

4. In relation to Restricted Transfers of Personal Data protected by the UK GDPR and EU GDPR, the SCCs as implemented under paragraphs 2 and 3 above will apply as amended by the IDTA Addendum. The IDTA Addendum shall be completed as follows:

    a. table 1 shall be deemed completed with the details set out in Schedule 1 of this DPA;

    b. table 2 shall be deemed completed with the information about the approved SCCs, modules and selected clauses which the IDTA Addendum shall be appended to as set out in paragraph 2 and 3 above.

    c. table 3 of the IDTA Addendum shall be completed as follows:

        i. the list of parties shall be deemed completed with the details set out in Schedule 1 of this DPA;

ii. Annex II shall be deemed completed with the details set in Schedule 3 of this DPA;

iii. the list of sub-processors shall be deemed completed with the *Sub-Processor List* and

iv. table 4 of Part One shall be completed as neither party may end the IDTA Addendum when it changes.

5. In relation to Restricted Transfers of Personal Data protected by the UK GDPR, the International Data Transfer Agreement shall apply, completed as follows:

a. table 1 shall be deemed completed with the details set out in Schedule 1 of this DPA;

b. in table 2:

i. the governing law and primary place of claims shall be England and Wales;

ii. the status of the exporter and importer is set out in Schedule 1 of this DPA;

iii. the linked agreement shall be completed with the details set out in the Agreement;

iv. neither party may end the International Data Transfer Agreement as a result of an approved change or before the end of the Agreement;

v. the data importer may transfer on the Transferred Data and there are no specific restrictions; and

vi. the parties shall review the International Data Transfer Agreement each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment.

c. table 3 shall be deemed completed with the details set out in Schedule 1 of this DPA; and

d. table 4 shall be deemed completed with the details set out in Schedule 3 of this DPA.

## Schedule 3

## Technical and Organisational Security Measures

Further details of technical and organisational security measures used by Benefex to protect Customer Data is available at:

- *Information Security Standards*

Where applicable, this Schedule 3 will serve as Annex II to the SCCS. The following table provides more information regarding the technical and organisational security measures set forth below.

| Technical and Organizational Security Measure | Evidence of Technical and Organisational Security Measures |
|---|---|
| Measures of pseudonymisation and encryption of personal data | • All data sent to or from Benefex is encrypted in transit using TLS 1.2.<br>• Customer Personal Data is encrypted at rest using 256-bit encryption.<br>• All Benefex datastores used to process Customer data are configured and patched to industry-recognised system-hardening standards and our associated procedures laid out by ISO 27002 code of practice for Information Security controls. |
| Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services | • Benefex has implemented formal procedures for handling security events. Benefex 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.<br>• All Customer Data is stored in the UK, EEA and Singapore. All sites have local and regional backup facilities for disaster recovery.<br>• Benefex infrastructure uses Google Cloud Platform (**GCP**) and Azure, both reputable Infrastructure-As-A-Service providers. Benefex leverages their globally redundant services to ensure Services run reliably. Benefex 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 Benefex infrastructure is designed and built for high availability.<br>• Benefex data security, high availability, and built-in redundancy are designed to ensure application availability and protect information from accidental loss or destruction. Benefex disaster recovery plan incorporates both zonal and geographic failover between Google UK and EU data centres and where necessary Singapore. All Benefex recovery and resilience mechanisms are tested regularly, and processes are updated as required.<br>• Although Benefex 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. Benefex leverages a range of technologies and security related cloud tools to deliver uninterrupted remote work for all employees.<br>• All Customer Data is encrypted at rest within the infrastructure and associated keys are rotated regularly to ensure continued security.<br>• All Customer Data deleted by Benefex 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 manner in the event of a physical or technical incident | • Benefex are certified to a combined management system for ISO 27001 and 22301 providing disaster recovery and continuity policy, procedures, and plans. The 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 | • Benefex 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. |

| | |
|---|---|
| and organisational measures in order to ensure the security of the processing | • 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.<br>• Penetration tests. Benefex contracts an independent CHECK 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**) this is used both internally by Benefex and can be used by customers to access our applications.<br>• Logical Access Controls. Benefex 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.<br>• All access to the Benefex infrastructure and systems processing Customer Data is protected by Multi Factor Authentication (**MFA**).<br>• Benefex restricts access to Customer Data to only those people with a "need-to-know" for a permitted purpose and following least privileges principles.<br>• Benefex 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.<br>• Benefex 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.<br>• Password best practices are implemented by Benefex. Initial passwords must meet the following and contain at least 9 characters, thereafter, further access requires a minimum of 12 characters; They 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.<br>• Benefex maintains and enforces "account lockout" by disabling accounts with access to Customer Data when an account exceeds more than ten (3) consecutive incorrect password attempts.<br>• Benefex operates an internal Wi-Fi network for conditional internet access only. All access to Benefex resources and systems storing customer data is protected by strong passwords and MFA.<br>• Benefex 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.<br>• 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: Benefex 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.<br>• Benefex 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.<br>• Security Awareness Training: Benefex conducts information Security and data protection training on joining and requires all employees to take the annual security and data protection and privacy training, whether they have access to customer data or not.<br>• To further protect and report events Benefex uses the following:<br>  • 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.<br>  • Endpoint security software is used via cloud services, enabling monitoring and reporting.<br>  • All System events are logged, correlated, and monitored by the SOC. |

| | |
|---|---|
| | • All access is logged, reported, and monitored by the SOC.<br>• MFA is used for all access into the infrastructure and customer data.<br>• Benefex encrypts all backups of all customer data. |
| Measures for ensuring physical security of locations at which personal data are processed | • Physical Access Control. Benefex 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.<br>• Benefex have own 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 Benefex and its customers. |
| Measures for ensuring system configuration, including default configuration | • Change and Configuration Management: Benefex have 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, Benefex 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.<br>• Change requirements are managed under ISO 27001 and 27002 to ensure Benefex have 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.<br>• 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.<br>• Benefex have documented an integrated Security and Continuity Management System with the associated controls for ISO 27001 and 22301. They include an information security policy, business continuity policy and data protection policies associated with UK and EU data protection law. Benefex have 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 | • Benefex are certified to ISO 27001, ISO 22301 and The UK Cyber Essentials scheme. To ensure they are maintained in accordance with the standards, Benefex conduct internal audits biannually and are externally audited by a UKAS accredited third party biannually. 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).<br>• Security measures are in place to provide only the minimum amount of access (least privilege) necessary to perform required functions.<br>• Upon termination or expiry of this Agreement, Benefex will (at Customer's election) delete or return to Customer all Customer Data (including copies) in its possession or control as soon as reasonably practicable and within the agreed termination period or expiry of the Agreement, save that this requirement will not apply to the extent that Benefex 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 Benefex will securely isolate and protect from any further processing, except to the extent required by applicable law.<br>• More information about how Benefex Processes Personal Data is set forth in the Customer Privacy Policy. |

| | |
|---|---|
| Measures for ensuring data quality | • In most cases it is the customer (the data controller) who provides the data to Benefex for the contracted services, and it is their responsibility for the accuracy of the data. Benefex will conduct data validation during the import process.<br>• Where Benefex are the data controller, Benefex will only use the data within the service provided to conduct controller services and responsibilities. Where additional information is required, the data requested will come direct from the data subject.<br>• Benefex have processes in place to assist the customers and data subjects if they exercise their privacy rights. (Including a right to amend and update their Personal Data), as described in the Benefex Privacy notice or Customer Privacy notice. |
| Measures for ensuring limited data retention | • See "*Measures for ensuring data minimization*" above. |
| Measures for ensuring accountability | • Benefex has implemented data protection policies.<br>• Benefex follows a compliance by design approach.<br>• Benefex maintains documentation of your processing activities.<br>• Benefex has appointed a data protection representative and internal Legal Counsel<br>• Benefex 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, Benefex will permanently and securely delete all instances of the Customer Data within 90 days of the termination date, unless Benefex and the customer have agreed a separate exit plan.<br>• 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.<br>• Benefex has a process that allows data subjects to exercise their privacy rights (including a right to amend and update their Personal Data), as described in the Benefex / customer Privacy Notices and the Benefex Data Protection Policy. |
| 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 Benefex engage a third party as a sub processor, the following will take place:<br>• Prior to engaging new third-party service providers or vendors who will have access to Benefex / Customer Data, Benefex conducts a risk assessment of vendors' data security practices in accordance with the Benefex supplier management procedure.<br>• Benefex will restrict the onward sub-processor's access to Customer Data only to what is strictly necessary to provide the Services, and Benefex will prohibit the sub-processor from processing the Personal Data for any other purpose.<br>• Where possible, Benefex 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.<br>• Where an additional sub processor is necessary, Benefex will inform the affected customers in good time.<br>• Benefex will remain liable and accountable for any breach of this DPA that is caused by an act or omission of its sub-processors. |