Data Processing Addendum

Updated: 18th December 2023

About this document

This document formalises the agreement for how we process your data to provide the Ben platform.

Table of Contents

This Data Processing Addendum including its Annexes ("DPA") forms part of the Terms of Service between Thanks Ben and Customer to reflect the Parties' agreement regarding the Processing of Personal Data.

This DPA sets out the additional terms, requirements and conditions on which Thanks Ben shall process Personal Data when providing services under the Master Services Agreement. This DPA contains the mandatory clauses required by Article 28(3) of the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (UK GDPR) for contracts between controllers and processors and the General Data Protection Regulation ((EU) 2016/679).

1. Agreed terms

The following definitions and rules of interpretation apply in this DPA:

1. **Business Purposes:** the services to be provided by Thanks Ben to the Customer as described in the Master Service Agreement and any other purpose specifically identified in Annex A.
2. **Commissioner:** the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).
3. **Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Processing:** have the meanings given to them in the Data Protection Legislation.
4. **Controller:** has the meaning given to it in section 6, DPA 2018.
5. **Data Protection Legislation:** 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 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 Thanks Ben is subject which relates to the protection of personal data.
6. **Data Subject:** the identified or identifiable living individual to whom the Personal Data relates.
7. **EU GDPR:** the General Data Protection Regulation ((EU) 2016/679).
8. **Personal Data:** means any information relating to an identified or identifiable living individual that is processed by Thanks Ben on behalf of the Customer as a result of, or in connection with, the provision of the services under the Master Service Agreement; an identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
9. **Processing, processes, processed, process:** any activity that involves the use of the Personal Data. It includes, but is not limited to, any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Personal Data to third parties.
10. **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.
11. **Processor:** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.
12. **Records:** has the meaning given to it in Clause 12.

13. **Term:** this DPA's term as defined in Clause 10.
14. **UK GDPR:** has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

This DPA is subject to the terms of the Master Service Agreement and is incorporated into the Master Service Agreement. Interpretations and defined terms set forth in the Master Service Agreement apply to the interpretation of this DPA.

The Annexes form part of this DPA and shall have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Annexes.

In the case of conflict or ambiguity between any of the provisions of this DPA and any executed SCC the provisions of the executed SCC will prevail.

2. Personal data types and processing purposes

The Customer and Thanks Ben agree and acknowledge that for the purpose of the Data Protection Legislation:

(a) the Customer is the controller and Thanks Ben is the processor.

(b) 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 Thanks Ben.

(c) Annex A describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which Thanks Ben may process the Personal Data to fulfil the Business Purposes

3. Our obligations

Thanks Ben shall only process the Personal Data to the extent, and in such a manner as is necessary for the Business Purposes in accordance with the Customer's written instructions. Thanks Ben shall not process the Personal Data for any other purpose or in a way that does not comply with this DPA or the Data Protection Legislation. Thanks Ben must promptly notify the Customer if in its opinion the Customer's instructions do not comply with the Data Protection Legislation.

Thanks Ben must comply promptly with any Customer written instructions requiring Thanks Ben to amend, transfer, delete or otherwise process the Personal Data or to stop, mitigate or remedy any unauthorised processing.

Thanks Ben shall maintain the confidentiality of the Personal Data and shall 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 Thanks Ben to process or disclose the Personal Data to a third party, Thanks Ben 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.

Thanks Ben shall reasonably assist the Customer with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of Thanks Ben's processing and the information available to Thanks Ben 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.

Thanks Ben must promptly notify the Customer of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting Thanks Ben's performance of the Master Service Agreement or this DPA.

4. Our employees

Thanks Ben shall ensure that all its employees:

(a) are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;
(b) are aware both of Thanks Ben's duties and their personal duties and obligations under the Data Protection Legislation and this DPA.

5. Security

Thanks Ben shall implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including but not limited to the security measures set out in Annex B.

Thanks Ben shall implement such measures to ensure a level of security appropriate to the risk involved including as appropriate:

(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
(d) a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

6. Personal data breach

Thanks Ben shall without undue delay notify the Customer if it becomes aware of:

(a) the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data. Thanks Ben shall restore such Personal Data at its own expense as soon as possible.
(b) any accidental, unauthorised or unlawful processing of the Personal Data; or
(c) any Personal Data Breach.

Where Thanks Ben becomes aware of (a), (b) and/or (c) above it shall without undue delay provide the Customer with the following information:

(a) description of the nature of (a), (b) and/or (c), including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;
(b) the likely consequences; and

(c) a description of the measures taken or proposed to be taken to address (a), (b) and/or (c), including measures to mitigate its possible adverse effects.

Immediately following any accidental, unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties shall co-ordinate with each other to investigate the matter. Further, Thanks Ben shall reasonably co-operate with the Customer in the Customer's handling of the matter, including but not limited to:

(a) assisting with any investigation;
(b) where necessary providing the Customer with physical access to any facilities and operations affected;
(c) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and
(d) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Personal Data processing.

Thanks Ben shall not inform any third party 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

Where agreed with the Customer, Thanks Ben may process the Personal Data outside the UK/EEA under the following conditions:

(a) Thanks Ben processes the Personal Data in a territory which is subject to adequacy regulations or decisions under the Data Protection Legislation in that the territory provides adequate protection for the privacy rights of individuals.
(b) Thanks Ben participates in a valid cross-border transfer mechanism under the Data Protection Legislation to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Data Protection Legislation in Article 46 of the UK GDPR and EU GDPR.

8. Sub-processors

Thanks Ben has the Customer’s general authorisation for the engagement of sub-processors. Thanks Ben shall inform the Customer in writing of any intended changes to its sub-processors through the addition or replacement of sub-processors at least 20 working days in advance thereby giving the Customer sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). Thanks Ben shall provide the Customer with the information necessary to enable the Customer to exercise its right to object.

Where Thanks Ben engages a sub-processor to carry out specific processing activities it shall do so by way of a written contract that provides for in substance the same data protection obligations as those binding Thanks Ben under these clauses including in terms of third-party beneficiary rights for data subjects.

Thanks Ben shall remain fully responsible to the Customer for the performance of the sub-processor's obligations under its contract with Thanks Ben. Thanks Ben shall notify the Customer of any failure by the sub-processor to fulfil its obligations under that contract.

Thanks Ben shall agree a third-party beneficiary clause with the sub-processor whereby in the event Thanks Ben has factually disappeared, ceased to exist in law or has become insolvent the Customer shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

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

Thanks Ben shall take such technical and organisational measures as may be appropriate and promptly provide such information to the Customer as the Customer may reasonably require to enable the Customer to comply with:

(a) the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

(b) information or assessment notices served on the Customer by the Commissioner or other relevant regulator under the Data Protection Legislation.

Thanks Ben shall notify the Customer immediately in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

Thanks Ben shall notify the Customer within 3 business days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.

Thanks Ben shall give the Customer, its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

10. Term and termination

This DPA will remain in full force and effect so long as the Master Service Agreement remains in effect.

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

If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Master Service Agreement obligations, the parties may agree to suspend the processing of the Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection

Legislation 30 business days, either party may terminate the Master Service Agreement on written notice to the other party.

11. Data return and destruction

At the Customer's request Thanks Ben shall give the Customer or a third party nominated in writing by the Customer a copy of or access to all or part of the Personal Data in its possession or control in a format agreed between the parties.

On termination of the Master Service Agreement for any reason or expiry of its term Thanks Ben shall securely delete or destroy or, if directed in writing by the Customer, return and not retain all or any of the Personal Data related to this DPA in its possession or control unless any law, regulation, or government or regulatory body requires Thanks Ben to retain any documents or materials or Personal Data that Thanks Ben would otherwise be required to return or destroy.

12. Records

Thanks Ben 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 subcontractors, 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 5 (Records).

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

13. Audit

Thanks Ben shall permit the Customer and its third-party representatives to audit Thanks Ben's compliance with its DPA obligations, on at least 30 working days' notice, during the Term. Thanks Ben shall give the Customer and its third-party representatives all necessary assistance to conduct such audits. The assistance may include, but is not limited to:

(a) physical access to, remote electronic access to, and copies of the Records and any other information held at Thanks Ben's premises or on systems storing the Personal Data; and

(b) reasonable inspection of all Records and the infrastructure, electronic data or systems, facilities, equipment or application software used to store, process the Personal Data.

14. Warranties

Thanks Ben warrants and represents that:

(a) it and anyone operating on its behalf shall process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

(b) it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Master Services Agreement's contracted services; and

(c) considering the current technology environment and implementation costs, it shall take appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:

(i) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage;

(ii) the nature of the Personal Data protected; and

(iii) comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in 5.1.

The Customer warrants and represents that Thanks Ben's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.

This DPA has been entered into on the date stated in the Order Form.

Appendix A: Personal Data processing purposes and details

Type	Description
Business Purposes	As described in the Terms of Service Agreement
Subject matter of processing	Personal data of the Customer's employees for the purpose of providing the services
Nature of Processing	As described in the Terms of Service Agreement
Data Subject Types	Employees and contractors of the Customer
Personal Data Categories	Name, contact details, e-mail address
Duration of Processing	The duration of the Terms of Service

Appendix B: Technical and Organisational Measures

Thanks Ben implements technical and organisational measures for secure and compliant processing of personal data. Thanks Ben processes three general categories of personal data:

- Personal details
- Employment details
- System usage details

Certifications and Standards

Thanks Ben maintains an ISO 27001 accredited ISMS, and as such continually reviews its security posture, performing regular audits as required by the compliance cycle.

Confidentiality

Physical Entry Control

Our premises are not freely accessible. They are locked when employees are away and utilise a keycard system for access. Thanks Ben implements the following measures:

- Locked building.
- Locked office.
- Keycard access.
- Receptionist.
- Visitors accompanied by employees.

Thanks Ben does not maintain servers or server rooms, instead making use of Amazon Web Services (AWS). AWS maintains SOC 2, ISO 27001, and PCI DSS Level 1 certifications.

Access Control

Thanks Ben implements the following measures for access to software systems:

- For every employee, a personally assigned user is set up with a password bound to strict requirements (at least 15 characters long with special characters).
- Passwords must be unique and may not be used for other accounts.
- Central authentication with username and password, incl. mandatory 2-factor authentication, with risk-based heuristics.
- Access is monitored and logged, including unsuccessful login attempts.

- Access is provided on a principle of least privilege and is regularly reviewed to mitigate scope creep.

Usage Control

Thanks Ben implements the following measures when working within software systems:

- The password rules for access control must also be followed for usage control.
- Role-based authorisation, administrative user profiles are kept to a minimum.
- Encrypted access via TLS 1.2 at minimum.
- User-dependent authentication with single sign-on (SSO) where possible.
- The use of personal data is limited, so that only authorised individuals can use the personal data necessary for their task (De Minimis Principle).
- Logging of usage and changes.
- Paperless work by principle and compliant destruction of paper documents with a shredder where applicable.
- Regular training and instruction on handling of information and secure communication.

Pseudonymisation

Thanks Ben pseudonymises information as much as possible when processing in scenarios where the connection to the individual is not absolutely necessary for the result of the service provided.

Separation Control

Logical separation is applied to customer data stored on the Ben platform:

- Separation of production and test environments.
- Logical segmentation within the application with redundant checks, to ensure multi-tenancy.
- Physical database separation, where required in exceptional cases.

Integrity

Transfer Control

No unauthorised reading, copying, modification or removal during electronic transmission is ensured by:

- The use of USB flash drives or related data carrier tools is prohibited.
- Encryption.
- Information should only be printed out if absolutely needed. Printed copies must be shredded immediately as soon as they are no longer needed.

Input Control

Thanks Ben implements the following measures for its software systems:

- Traceability of inputs, changes, and deletions by personalised users.
- Traceability in assigning, changing, and deleting user authorisations.

Availability and Reliability

Thanks Ben protects against accidental or wilful destruction or loss of personal data is ensured by an active-passive backup strategy across the Ben platform.

Additionally:

- Personal data is processed on data processing systems that are subject to regular and documented patch management. No systems may be linked on the network that are outside of the manufacturer's maintenance cycles (e.g. no Win95, XP, etc). Automatic updates are activated on the computers.
- Antivirus software is maintained on each endpoint, and an equivalent system is implemented on servers.
- Continuous availability of high-speed internet is ensured for office environments. (Cloud system services can be used with any internet connection.)
- Cloud provider data centres are state of the art (temperature control, fire protection, water penetration, uninterrupted power supply).

Employee Workplace

Thanks Ben implements the following measures via central device management:

- Employees must encrypt their hard drives.
- Emails must be scanned by the provider default virus, spam, and phishing filter.
- Employees must enable their device inbuilt firewall.
- Screen savers must be set at the shortest time period until activation.

Procedure for Regular Review, Assessment and Evaluation

Data protection and IT security within Thanks Ben is reviewed regularly and based on these assessments, continuously improved. Internal auditing may include data privacy requirements such as:

- Obligation of employees to maintain data secrecy, additional training and education.
- Regular auditing of data processing procedures.
- Procedures in case of data breaches and the protection of data subjects' rights.

Thanks Ben has implemented the following internal measures:

- Regular auditing of procedures.
- Regular review of technical advancements in accordance with Article 32 UK/EU GDPR.
- No data processing within the meaning of Article 28 UK/EU GDPR without corresponding instructions from the controller, ensured by clear contract design, strict selection of the service provider and follow-up inspections.