Data processing agreement
(DPA)

According to UK GDPR and the Data Protection Act 2018

Prepared in accordance with the requirements of the UK Information Commissioner's Office (ICO)

Version Mar 2025

between

Company:

Street:

Postal Code, City:

Country:

- In the following referred to as the "controller(s) or client" -

and

BEE360 SERVICES LTD
10 John Street
London WC1N 2EB
United Kingdom

- hereinafter: "Processor(s) or Contractor" -

SECTION I

Clause 1 - Purpose and scope of application

a) These Standard Contractual Clauses (hereinafter "Clauses") are intended to ensure compliance with **Article 28(3) and (4) of the UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**, as applicable in the United Kingdom.

b) The Controllers and Processors listed in Annex I have agreed to these Clauses to ensure that the processing of personal data complies with the requirements of UK data protection law, specifically the UK GDPR and the Data Protection Act 2018.

c) These Clauses apply to the processing of personal data as described in Annex II, where such processing falls within the territorial and legal scope of the **UK GDPR**, whether carried out by a Controller or Processor established in the United Kingdom, or where UK data subjects are affected.

d) Annexes I to IV form an integral part of these Clauses. These Clauses are binding upon both parties and apply without prejudice to the responsibilities and obligations under UK data protection law.

e) These Clauses do not on their own ensure compliance with international data transfer obligations under **Chapter V of the UK GDPR**. Where applicable, transfers of personal data to third countries must comply with the UK's international transfer regime, including use of the **UK International Data Transfer Agreement (IDTA)** or **UK Addendum to the EU SCCs**.

Clause 2 - Unalterability of the clauses

a) The Parties undertake not to modify these Clauses, except to update the information contained in the Annexes.

b) However, the Parties may include these Clauses in a broader contract and add other clauses or additional safeguards, provided that these do not directly or indirectly contradict the substance of these Clauses or infringe upon the fundamental rights or freedoms of data subjects under **UK GDPR** and **DPA 2018**.

Clause 3 - Interpretation

a) Where terms used in these Clauses are defined in the **UK GDPR** or the **Data Protection Act 2018**, they shall be interpreted in accordance with those definitions.

b) These Clauses shall be interpreted in the light of the provisions of the **UK GDPR** and the **DPA 2018**.

c) These Clauses may not be interpreted in a way that limits or contradicts the rights and obligations set out in the **UK GDPR** or **DPA 2018**, or that restricts the fundamental rights or freedoms of data subjects.

Clause 4 - Priority

a) In the event of a conflict between these Clauses and the provisions of any other agreement between the Parties, whether existing or concluded thereafter, the provisions of these Clauses shall prevail with respect to the subject matter of data processing and protection under UK law.

Clause 5 - Tying clause

a) An entity that is not a Party to these Clauses may, with the consent of all existing Parties, accede to these Clauses at any time as a Controller or Processor by completing and signing Annex I.

b) Once the new party has completed and signed the necessary annexes, it shall be bound by the Clauses and shall enjoy the rights and assume the obligations of a Controller or Processor, in accordance with its designation in Annex I.

c) No rights or obligations shall arise for the acceding party under these Clauses in relation to the period prior to accession.

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 6 - Description of the processing

a) The specific details of the processing activities, including the categories of personal data and the purposes for which they are processed on behalf of the Controller, are described in **Annex II**.

b) These Clauses apply only to the processing described in Annex II and must be updated as required to reflect any changes.

Clause 7 - Obligations of the parties

7.1 Instructions

a) The Processor shall process personal data only on documented instructions from the Controller, unless required to do so by **UK law**. If such a legal requirement arises, the Processor must inform the Controller unless prohibited by law for reasons of public interest. All instructions must be documented.

b) The Processor shall immediately inform the Controller if it considers that any instruction infringes the **UK GDPR**, **DPA 2018**, or any other applicable UK data protection regulation.

7.2 Earmarking

a) The Processor shall only process personal data for the specific purposes set out in Annex II, unless it receives further lawful instructions from the Controller.

7.3 Duration of the processing of personal data

a) The Processor shall process the data only for the period specified in **Annex II**, unless instructed otherwise by the Controller or required under UK law.

7.4 Security of processing

a) The Processor shall implement the technical and organisational measures set out in **Annex III** to ensure the security of personal data. This includes protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

b) Access to personal data shall be limited to personnel who require access for the performance of the contract and are bound by confidentiality.

7.5 Sensitive data

a) If the processing concerns personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health, sex life or sexual orientation of a person, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the Processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance with the clauses

a) The parties must be able to prove compliance with these clauses.

b) The Processor shall process requests from the Controller regarding the processing of data in accordance with these Clauses promptly and appropriately.

c) The Processor shall provide the Controller with all information necessary to demonstrate compliance with the obligations set out in these Clauses and arising directly from the UK GDPR and the Data Protection Act 2018. At the request of the Controller, the Processor shall also authorise and contribute to an audit of the processing activities covered by these Clauses at appropriate intervals or where there are indications of non-compliance. When deciding on an inspection or audit, the controller may take into account relevant certifications of the processor.

d) The controller may carry out the audit itself or commission an independent auditor. The audits may also include inspections of the processor's premises or physical facilities and shall be carried out with reasonable prior notice where appropriate.

e) The Parties shall make the information referred to in this clause, including the results of audits, available to the competent supervisory authority(ies) upon request.

7.7 Use of subcontracted processors

a) The Processor shall not subcontract any of its processing operations that it carries out on behalf of the Controller pursuant to these Clauses to a subprocessor without the prior separate written authorization of the Controller. The Processor shall submit the request for the separate authorization prior to engaging the relevant sub-processor, together with the information necessary for the Controller to decide on the authorization. The list of sub-processors authorized by the Controller can be found in **Annex IV**. The Parties shall keep **Annex IV** up to date.

b) Where the Processor engages a sub-processor to carry out certain processing activities (on behalf of the Controller), such engagement shall be by way of a contract which imposes on the sub-processor substantially the same data protection obligations as those applicable to the Processor under these Clauses. The Processor shall ensure that the Sub-Processor fulfils the obligations to which the Processor is subject under these Clauses and under UK GDPR and the Data Protection Act 2018.

c) The Processor shall provide the Controller with a copy of any such subcontracting agreement and any subsequent amendments at the Controller's request. To the extent necessary to protect trade secrets or other confidential information, including personal data, the Processor may obscure the wording of the agreement before providing a copy.

d) The Processor shall be fully liable to the Controller for ensuring that the Sub-Processor fulfils its obligations under the contract concluded with the Processor. The Processor shall notify the Controller if the Sub-Processor fails to fulfil its contractual obligations.

e) The processor agrees a third-party beneficiary clause with the sub-processor, according to which the controller - in the event that the processor no longer exists in fact or in law or is insolvent - has the right to terminate the subcontracting agreement and instruct the sub-processor to delete or return the personal data.

7.8 International data transfers

a) Any international transfer of personal data by the Processor shall be carried out only in accordance with documented instructions from the Controller and must comply with the applicable international data transfer provisions of the **UK GDPR**, including the use of the **UK International Data Transfer Agreement (IDTA)** or the **UK Addendum to the EU SCCs**, where appropriate.

b) The Controller agrees that where sub-processors are used for transfers outside the UK, the Processor shall ensure that appropriate safeguards are implemented in line with the UK's transfer regime.

Clause 8 - Support of the person responsible

a) The Processor shall notify the Controller immediately upon receiving any request from a data subject to exercise their rights under the UK GDPR (including access, rectification, erasure, restriction, data portability, or objection). The Processor shall not respond to the request unless authorised by the Controller.

b) Taking into account the nature of the processing, the Processor shall assist the Controller in fulfilling its obligations to respond to such requests under the UK GDPR.

c) In addition to the above, and taking into account the nature of the processing and the information available, the Processor shall assist the Controller with:

   1) Conducting a **Data Protection Impact Assessment (DPIA)**;

   2) Consulting the **Information Commissioner's Office (ICO)** prior to high-risk processing;

   3) Ensuring the accuracy and timeliness of personal data;

   4) Obligations under Article 32 of the UK GDPR

   5) Implementing appropriate security measures in accordance with **Article 32 UK GDPR**.

d) The technical and organisational measures to support this assistance are detailed in **Annex III**.

Clause 9 - Notification of personal data breaches

a) In the event of a personal data breach involving data processed on behalf of the Controller, the Processor shall support the Controller in:

   1) Timely notification to the **ICO** and, if applicable, the affected data subjects in accordance with **Articles 33 and 34 UK GDPR**;

   2) Gathering and documenting the following information:

      i) The nature of the breach and, where possible, the categories and approximate number of data subjects and data records affected;

      ii) Likely consequences of the breach;

      iii) Measures taken or proposed to mitigate its effects.

b) If full information is not immediately available, the Processor shall provide it in stages without undue delay.

9.1 Violation of the protection of data processed by the controller

In the event of a personal data breach in connection with the data processed by the controller, the processor shall assist the controller as follows:

a) in notifying the personal data breach to the competent supervisory authority or authorities without undue delay after the controller becomes aware of the personal data breach, where relevant (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

b) when obtaining the following information to be provided in accordance with Article 33(3) of Regulation (EU) 2016/679] or in the controller's notification, which shall include at least the following information:

   1) the nature of the personal data, where possible, indicating the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

   2) the likely consequences of a personal data breach;

   3) the measures taken or proposed to be taken by the controller to address the personal data breach and, where appropriate, measures to mitigate its possible adverse effects.

If and to the extent that not all such information can be provided at the same time, the initial notification will contain the information available at that time and further information will be provided as soon as it becomes available without undue delay thereafter;

c) in complying with the obligation under Article 34 of Regulation (EU) 2016/679] or [to notify the data subject without undue delay of a personal data breach where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Violation of the protection of data processed by the processor

If the breach concerns data processed independently by the Processor, the Processor shall notify the Controller without undue delay and provide:

1. A description of the nature of the breach;
2. Contact details for further information;
3. The likely consequences and remediation measures.

Further information shall be provided as it becomes available. The Parties may define additional breach notification requirements in **Annex III**.

SECTION III - FINAL PROVISIONS

Clause 10 - Breaches of the clauses and termination of the contract

a) If the Processor fails to comply with these Clauses, the Controller may instruct the Processor to suspend processing activities until compliance is restored or the agreement is terminated. The Processor shall immediately inform the Controller if it cannot comply with these Clauses for any reason.

b) The Controller may terminate this agreement, insofar as it concerns personal data processing, if:

   1) The Processor fails to restore compliance within a reasonable timeframe (no later than one month after suspension);

   2) The Processor materially or repeatedly breaches these Clauses or its obligations under UK GDPR and DPA 2018;

   3) The Processor fails to comply with a binding decision by a competent court or supervisory authority.

c) The Processor may terminate this agreement if the Controller insists on executing instructions that the Processor reasonably believes to be unlawful under UK data protection law and has previously informed the Controller accordingly.

d) Upon termination, at the Controller's choice, the Processor shall either:

   1) Return all personal data and erase existing copies, or

   2) Erase all personal data and certify to the Controller that this has been done.

   This excludes situations where UK law requires retention. Until deletion or return, the Processor shall ensure continued compliance with these Clauses.

ANNEX I
List of parties

Responsible persons:

Name:

Address:

Contact:

Name:

Position:

Place, Date:

_____

Name:

Position:

Place, Date:

_____

Data Processor:

Name:	**BEE360 SERVICES Ltd.**
Address:	**10 John Street • London WC1N 2EB, United Kingdom**
Contact:	**security_and_compliance@bee360.com**

Philipp Hansert

Chief Revenue Officer

London,

_____

Alexander Schuster

Chief Technology Officer

London,

_____

ANNEX II

Description of the processing

Categories of data subjects whose personal data are processed

- Employees
- Customers
- Suppliers

Categories of personal data that are processed

- Personal master data
- Project roles
- Employee capacities
- Usage data

Type of processing

- Disclosure by transmission

Purpose(s) for which the personal data are processed on behalf of the controller

- Visualization and management of internal processes
- Maintenance & care of IT systems
- Development/Optimization
- Hosting

Duration of processing

- Contract duration

In the case of processing by (sub)processors, the object, type and duration of the processing must also be stated.

- Bee360 GmbH provides development, maintenance and support, hosting through disclosure by transmission

ANNEX III

Technical and organizational measures, including to ensure the security of data

GENERAL

Procedures for regularly reviewing, assessing and evaluating the effectiveness of technical and organizational measures to ensure the security of processing

The regular review, assessment and evaluation of the effectiveness of the technical and organizational measures is carried out as part of information security management based on the established ISMS (see also Measures for internal governance and management of IT and IT security).

Regular review, assessment and evaluation are performed as part of the information security management system (ISMS). These processes are implemented digitally, without reliance on physical infrastructure in the UK.

Measures to ensure the system configuration, including the default configuration

The existing policy on communication security as part of the ISMS describes the network topology and network separation as well as the installed security software and other security measures, such as encryption, in relation to the design and configuration of the separated networks. The standard configuration of system access is derived from the user profiles defined in the access control policy and the policy for secure passwords. In addition, there are further standard configurations for all systems and applications, taking into account information security requirements and the GDPR. Compliance with the configuration standards is supported and regularly checked by the use of automated configuration management tools. Regular maintenance of the systems ensures the supply of current security updates and patches. The responsible employees are regularly sensitized to the importance of secure system configuration.

-

Measures for the internal governance and management of IT and IT security

The internal governance and management of IT and IT security is based on an established information security management system (ISMS) in line with the TISAX/ISO27001 framework. This includes conducting risk analyses and managing vulnerabilities, as well as implementing security policies to control access to IT systems and data, ensuring the integrity and confidentiality of information and complying with data protection laws.

Measures for the certification/quality assurance of processes and products

The existing TISAX label (Standard Scope 2.0) published on ENX. In addition, an external data protection officer has been appointed who is also certified accordingly (TÜV, CIPP/E).

Measures to ensure data minimization and to avoid data retention

Data minimization is ensured in consultation with the external data protection officer in the form of an individual erasure concept for the various information assets. The deletion concept is implemented in relation to the data processing processes carried out as a processor, taking into account the purpose limitation and legality. Existing national retention periods are observed.

Measures to ensure accountability

Collaboration with the external data protection officer takes place via digital platforms in which all key documents are stored in written form. This includes the documentation of data processing activities, the implementation of data protection guidelines, the training and sensitization of employees (certificates) as well as legal enquiries and processes.

Measures to enable data portability and to ensure erasure

The portability of personal data is made possible through the use of standardized data formats. Data subjects have the option of receiving their personal data in a machine-readable format. The implementation of the erasure concepts is supported by automated erasure procedures. Personal data is erased in accordance with legal requirements.

CONFIDENTIALITY

Measures for pseudonymization and encryption of personal data

The existing guideline for system procurement and development as part of the ISMS regulates the pseudonymization of personal data. In the case of pseudonymization, personal, direct identifiers are replaced by randomly generated pseudonyms. The original identifiers are stored in data records that are separate from the pseudonyms. A role-based authorization concept with strictly separate user profiles ensures that only authorized persons are able to link pseudonyms and identifiers.

The existing policy on encryption as part of the ISMS specifies the use of strong encryption algorithms in accordance with current standards and regulates secure key management. Based on the algorithms and protocols permitted by the policy, data transmission via networks is always TLS-encrypted. Remote access takes place via VPN or SSH. Hard drive encryption is guaranteed via FileVault or Bitlocker.

Measures to identify and authorize users

The existing policy on access and access options as part of the ISMS prohibits the creation of collective user accounts and the sharing of accounts. Accordingly, only individual user accounts that guarantee unique identification are used. Strong authentication methods such as MFA and secure passwords in accordance with an organization-wide password policy further increase the security of identification. Single sign-on simplifies login from the user's perspective and increases the acceptance of secure passwords. The user's identity is verified automatically or manually during the registration process and when passwords are changed.

The existing access policy as part of the ISMS defines user profiles according to the principle of least privilege. These user profiles and the role and authorization concept anchored in the Bee360 application form the basis of role-based access control (RBAC). User authorization is logged and limited to the required period of time. As part of authorization management, the assignment, modification and cancellation of access rights are managed according to defined processes. The established emergency access procedures also ensure that only authorized persons receive the necessary extended access rights in an emergency.

Measures to protect data during transmission

The existing policy on encryption as part of the ISMS specifies the use of strong encryption algorithms in accordance with current standards and regulates secure key and certificate management. Based on the algorithms and protocols permitted by the policy, data transmission via networks is always TLS-encrypted. Remote access takes place via VPN or SSH (see also measures for pseudonymization and encryption of personal data). The communication security policy regulates for all employees which communication channels may be used to transmit information. The rules of behavior for the transmission of information depend on the communication channel used and on the classification of the information in terms of

confidentiality, integrity and availability and are defined by the communication security policy and the information classification policy.

Measures to protect data during storage

The existing policy on encryption as part of the ISMS specifies the use of strong encryption algorithms in accordance with current standards and regulates secure key management. Based on the algorithms and protocols permitted by the policy, hard disk encryption is ensured via FileVault or Bitlocker (see also measures for pseudonymization and encryption of personal data). The existing access policy defines user profiles according to the principle of least privilege (see also Measures for identifying and authorizing users). These user profiles and separate administrator accounts ensure that only authorized persons can access stored data. Events such as successful and failed login attempts or changes to user rights are recorded in accordance with the existing logging policy (see also Measures to ensure the logging of events). The measures to ensure the physical security of locations where personal data is processed are described in the next section and, in addition to physically separate backup copies, also contribute to the protection of data during storage. In addition, there are measures and rules of behavior that are based on the classification of data in accordance with the existing information classification policy. Examples of this are the additional password protection of individual documents, storage only on internal servers or the immediate deletion of local copies after use. Operating system firewalls and defense systems such as Windows Defender or Apple Gatekeeper are used to protect against malware. In addition, regular training courses are held for employees to sensitize them to the dangers of phishing practices, for example. The existing policy on the acceptable use of information assets also regulates the basic handling of client computers and server systems. In particular, this includes a ban on the installation and use of certain software. Stored data that is no longer required is securely deleted in accordance with the existing policy on disposal and destruction.

Measures to ensure the physical security of places where personal data processed

As Bee360 Services Limited does not operate a physical office in the United Kingdom, the following measures apply only to locations where physical offices are operated (e.g. the headquarters in Germany). For the UK, equivalent controls are implemented through remote work policies and data center-level protections.

Employees have access to the office locations via key cards or physical keys. The issue and return of these is documented and receipted in a key list. Visitors may only enter the office locations when accompanied by an employee. Security personnel monitor the premises, particularly at night.

In accordance with the clean desk and clear screen policy and the mobile working policy, every employee protects their workplace by, for example, locking the screen and removing paper documents and data carriers when they are absent or by using privacy screens and laptop locks. This is ensured in particular through regular training and by sensitizing employees to the need for increased vigilance when working from home and in public spaces. In addition, the guidelines on clean desks and clear screens access to and use of the central multifunction printer in shared office spaces.

The data center is operated by a service provider and is certified in accordance with ISO 27001, which includes the following measures to protect against unauthorized access:

- Detailed management of access authorizations
- Organizational instructions for reporting departures, leaves of absence, etc. to the access management system
- Special locking procedures, electronic access control
- Access control at reception
- Video surveillance
- Security personal
- No windows/windowless
- Burglar-proof doors

- Motion detectors

Access is only granted to certain Bee360 employees who are registered with the service provider as authorized users. Access by Bee360 employees is always accompanied by an employee of the service provider. All access to the data center is logged by the service provider.

The data center and the data carriers in it are protected against environmental threats as follows:

- Smoke and fire alarms
- Fire alarm systems with direct connection to the fire brigade
- Fire doors
- Water protection facilities
- Shielding attenuation
- Emergency power supply
- Standardized procedure for regularly reviewing the appropriateness of the protective measures taken
- House rules that only allow access after training/instruction or under escort

INTEGRITY

Measures to ensure the logging of events

The logging policy in place as part of the ISMS specifies the type and form of events to be logged and the corresponding retention periods. The specific specifications depend on the classification of the respective system and include successful and failed login attempts, changes to user rights and the starting and ending of processes. The logs are recorded in standardized formats and contain detailed, uniform time stamps that are synchronized across the systems as well as unique user IDs and log source IDs. This enables centralized evaluation of the log data.

Measures to ensure data quality

To ensure data quality, corresponding validation rules have been implemented for the Bee360 application at various levels. Correct relationships between database elements are ensured, for example, through the use of relational databases, the definition of foreign keys and standardized data formats. Automatically imported data is linked to existing data in Bee360 using unique identifiers. Violations of uniqueness or completeness criteria are automatically intercepted and logged so that the underlying inconsistencies can be corrected. Relevant data is also regularly updated via interfaces. Corresponding consistency criteria are also checked when users enter data. The user is supported by a user-friendly graphical interface when entering data. The fields of the associated forms have format and type definitions. Certain fields are mandatory or require the entry of unique values. Visual information informs the user if the data entered does not fulfil these requirements. Drop-down lists and the automatic filling of certain fields also help to ensure that the data is complete and correct. The initial entry and subsequent changes to the information in the forms are automatically logged and displayed on the form in the form of a change history. Bee360 offers special reports to check for duplicate content.

Measures to ensure data separation

The contractor's and client's systems are separated physically and/or logically in separate virtual environments as well as through appropriate network segmentation and dedicated firewall rules. Separation of the applications of different clients is achieved through separate databases and service installations for each application. Data access is only permitted in accordance with defined roles and authorizations via separate user accounts. In addition, there is a general separation of productive and non-productive systems in correspondingly separate environments. Backup copies are created separately for each customer application and stored separately from the active applications.

AVAILABILITY

Measures to ensure availability at all times

The Bee360 Cloud utilizes a hyperconverged infrastructure (HCI) that is designed for the continuous provision of services even in the event of failures and enables flexible scaling of resources as required. The underlying hardware is redundant in terms of cluster nodes, switches, border firewall and power supply. Corresponding failover mechanisms enable compensation in the event of hardware faults.
The hardware is housed in an ISO-certified data center and protected against hazards such as overheating, sabotage and environmental threats (see also Measures to ensure the physical security of locations where personal data is processed). Responsible persons have physical or administrative access in an emergency in accordance with their roles and authorizations.

Hardware, HCI and virtualized servers are regularly maintained. Availability is monitored in real time using appropriate monitoring systems. Automatic alerts are sent in the event of failures. Subsequent troubleshooting is carried out in accordance with defined processes in line with the existing incident management policy. In addition, there are scenario-based instructions for action for DDoS attacks, for example, as well as preventive protective measures against DDoS attacks. Regular backup routines in accordance with the data backup concept anchored in the existing business continuity policy enable the restoration of operational capability in the event of data loss.

Measures to ensure the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident

The recovery preferences for personal data depend on their respective assessment according to the existing information classification policy. The data backup concept anchored in the business continuity policy prescribes recovery plans and regular backups that enable recovery to a defined point (RPO). The storage of full backups and incremental backups in a data storage system with Raid Level 5 ensures the availability of the backups. Sensitization of employees, emergency contact lists and strictly protected emergency access for the relevant systems ensure the ability to act quickly in an emergency.

ANNEX IV

List of sub-processors

The controller has authorized the use of the following sub-processors:

Strategic partner - supporter in hosting and the provision of other services

Bee360 GmbH

Victor-Gollancz-Str. 3, 76137 Karlsruhe, Germany

security_and_compliance@bee360.com