Data Processing Agreement for TimeSpot Clock

Brightec Time AB, Reg. No. 556594-0375 · Version 1.0 · Effective from 25 November 2026

> The latest version is always at **https://brightectime.com/en/dpa/**. Printed and downloaded copies may be out of date.

This data processing agreement (the "DPA") applies between Brightec Time AB, reg. no. 556594-0375 (hereinafter "Brightec Time" or the "Processor"), and the customer (hereinafter the "Customer" or the "Controller") that has entered into a licence agreement for TimeSpot Clock.

The DPA forms an integral part of the licence agreement for the time and attendance system TimeSpot Clock (the "Licence Agreement") and, if the Customer has chosen to enter into one, the Support Agreement (together the "Service Agreement").

---

1. Background and purpose

1.1 Under the Licence Agreement, the Customer pays a recurring licence fee for the time and attendance system TimeSpot Clock. The Customer may also have entered into the optional Support Agreement, which covers both the time clock (the hardware) and the TimeSpot Clock software. The services under the Service Agreement together constitute the "Service".

1.2 To provide the Service, Brightec Time will process personal data on behalf of the Customer.

1.3 This DPA has been drawn up to ensure that personal data is processed in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council (the "GDPR") and applicable national data protection legislation.

---

2. Instructions and scope of the processing

2.1 Brightec Time shall process personal data only on the Customer's documented instructions, which consist of this DPA.

2.2 The processing is specified in **Annex 1** to this DPA.

2.3 If Brightec Time considers that an instruction infringes the GDPR or other applicable data protection legislation, Brightec Time shall inform the Customer immediately.

2.4 The Customer, as controller, decides how long the personal data is to be stored during the term of the agreement and is responsible for ensuring that the retention period complies with Article 5(1)(e) of the GDPR and with applicable working time legislation, employment law, collective agreements and accounting legislation. Brightec Time does not determine any retention period on behalf of the Customer and stores the personal data in TimeSpot Clock for as long as the Licence Agreement is in force, unless the Customer instructs otherwise.

2.5 The Customer, as controller, is responsible for the purposes of and the legal basis for the processing, for informing the employees, for user permissions in TimeSpot Clock and, where applicable, for carrying out a data protection impact assessment (DPIA) before the Service is put into use.

3. Obligations of the Processor

3.1 Security and protection: Brightec Time shall take appropriate technical and organisational measures to protect the personal data against unauthorised access, loss or destruction. Appropriate security measures are described in **Annex 2**.

3.2 Confidentiality: Brightec Time shall ensure that all persons in its own organisation or at engaged sub-processors who are authorised to process the personal data are bound by a confidentiality undertaking or a statutory duty of confidentiality.

3.3 Assistance: Brightec Time shall, to the extent reasonable, technically possible and at the Customer's request, assist the Customer with:

- Responding to requests from data subjects (employees) exercising their rights under the GDPR.
- Providing documentation where the Customer carries out data protection impact assessments (DPIAs).

3.4 Biometric data: The fingerprint identification function is optional and is used only if the Customer actively enables it. The fingerprint template is stored only on the time clock where it was registered, as a one-way encrypted template and not as an image, and is never shared with or sent to TimeSpot Clock or any other system. The Customer is responsible for the legal basis under Article 9 of the GDPR, for offering equivalent non-biometric alternatives and for deleting a user's fingerprint data on the time clock when the employee leaves or withdraws their consent, and before the user is deactivated in the TimeSpot Clock Admin Portal.

3.5 Support: The Support Agreement is optional and covers both the time clock and TimeSpot Clock. When providing support, Brightec Time processes personal data only to the extent necessary for the support. No punch data is retained on the time clock, but fingerprint templates are. If a time clock is returned for repair or recycling, Brightec Time shall not access, copy or use fingerprint templates on it, and shall delete them when the work is completed or the device is destroyed.

---

4. Sub-processors

4.1 The Customer hereby gives Brightec Time a general authorisation to engage sub-processors to provide the Service. Current sub-processors are listed in Annex 1.

4.2 Brightec Time shall inform the Customer of plans to change or replace sub-processors no later than 15 days before the change takes effect, so that the Customer has the opportunity to object.

4.3 Brightec Time shall enter into written agreements with all sub-processors imposing on them at least the same data protection obligations as those set out in this DPA.

---

5. Transfers to third countries (outside the EU/EEA)

5.1 The personal data is stored and processed within the EU/EEA on servers located in Sweden.

5.2 If personal data is transferred to, or processed in, a country outside the EU/EEA, Brightec Time shall ensure that there is a legal basis for the transfer under Chapter V of the GDPR (e.g. the EU-U.S. Data Privacy Framework or the EU Standard Contractual Clauses (SCCs)).

6. Personal data breaches

6.1 Brightec Time shall notify the Customer of a personal data breach without undue delay and no later than 72 hours after the breach has been discovered.

6.2 The notification shall describe the nature of the breach, the categories of data subjects concerned, the likely consequences and the measures taken or planned to address the breach.

7. Audits and inspections

7.1 Brightec Time shall make available to the Customer the information necessary to demonstrate compliance with the obligations under this DPA.

7.2 The Customer has the right, itself or through an independent third party, to audit Brightec Time's processing of personal data. Reasonable advance notice of such an audit shall be given, and the audit shall be carried out in a way that does not disrupt Brightec Time's normal operations.

8. Term, termination and deletion

8.1 This DPA applies for as long as Brightec Time processes personal data on behalf of the Customer.

8.2 When the Licence Agreement ends, Brightec Time shall, at the Customer's choice, delete or return all personal data relating to the Customer, unless applicable law requires continued storage.

8.3 Deletion shall take place no later than 60 days after the Licence Agreement has ended.

8.4 During the term of the agreement, Brightec Time shall, on the Customer's written instruction and within 30 days, delete or anonymise personal data that the Customer's retention policies no longer allow the Customer to keep.

Annex 1 – Specification of the processing

1. Purpose and nature of the processing

The processing is carried out to provide the time and attendance system **TimeSpot Clock**, which is licensed to the Customer for a recurring fee, for time recording, punch management and payroll data export and, if the Customer has a Support Agreement, to provide support for the time clock and TimeSpot Clock.

2. Categories of personal data

The following personal data is processed in TimeSpot Clock. User data is managed by the Customer in the TimeSpot Clock Admin Portal:

- **Identification data:** first and last name, employee number, username, employment date
- **Organisational data:** work group / company
- **Identification and authorisation codes:** ID code, PIN code, RFID card number.
- **Time and punch data:** punch times (in/out), absence reasons, overtime, project or deviation codes.
- **IP addresses** linked to punches.
- **Device information:** customer-specific company ID and terminal ID, used to authenticate the time clock with the TimeSpot Clock cloud server and for troubleshooting and security.
- **Stored only on the time clock, not in TimeSpot Clock: fingerprint template (special category of personal data).** One-way encrypted template (biometric data under Article 9 of the GDPR), only if the Customer chooses to use fingerprints. It is never sent to the cloud server or any other system.

3. Categories of data subjects

- Employees, consultants, subcontractors and other staff of the Customer who punch in and out on the time clock.

4. Data storage location and servers

- **Primary server/data centre (TimeSpot Clock cloud server):** Inleed / Yelles AB in Stockholm, Sweden
- **Backup:** Brightec Group AB in Mullhyttan, Sweden
- **Data flow:** Punch data is transferred immediately from the time clock to the TimeSpot Clock cloud server and is not retained on the time clock. Fingerprint templates remain on the time clock where they were registered.

5. Approved sub-processors

Company name	Reg. no. / Country	Service / Function	Place of processing
Inleed / Yelles AB	Sweden	Cloud infrastructure and database	Sweden
Brightec Group AB	Sweden	Server backup	Sweden

6. Retention period

The Customer decides the retention period for time and punch data in TimeSpot Clock. The Customer's retention period is set out in the Licence Agreement or in the Customer's written instruction to Brightec Time. The EU Working Time Directive does not set a specific retention period; it follows from national law, collective agreements and the GDPR.

Annex 2 – Technical and organisational security measures

The security measures applied by Brightec Time for TimeSpot Clock include the following:

1. Encryption in transit

All communication with the web interface, API and terminals is encrypted. The application requires an encrypted connection (HTTPS), and the minimum permitted TLS version is 1.2. The time clock connects via HTTPS to the TimeSpot Clock cloud server, which hosts the web application that runs on the time clock.

2. Access control

The Customer's users access recorded data through personal accounts in the TimeSpot Clock Admin Portal. The Customer is responsible for assigning and removing accounts. Within Brightec, only a limited number of named employees (the installation team) have direct access to customer data and servers, and only to the extent required for operations, support and troubleshooting.

3. Authentication

The system supports two-factor authentication for user accounts. The Customer can enable two-factor authentication per account. Session cookies are protected with the Secure and HttpOnly attributes. Access from a time clock to the TimeSpot Clock cloud server is controlled by a customer-specific company ID and a terminal ID.

4. Logging and traceability

The system logs logins, changes and other critical events. Access to the servers is also logged. Logs are kept for 90 days.

5. Backup

Data is backed up automatically every day and the backups are kept for 7 days. Restoration from backups is tested.

6. Operating environment and sub-processor

The servers are located in Stockholm, Sweden, and are operated by Inleed (hosting provider). Personal data is not stored or processed outside the EU/EEA. Punch data is transferred immediately to the server and is not retained on the time clock.

7. Personal data breaches

Brightec notifies the Customer without undue delay after becoming aware of a personal data breach, so that the Customer can fulfil its notification obligation under Article 33 of the GDPR.

Change history

The versions of the agreement and what changed. The latest version is always at brightectime.com/en/dpa.

Version	Effective from	Change
1.0	25 November 2026	First published version.