Schedule 1

Data Protocol

Types of personal data to be processed and categories of data subject

The provision of the Services will involve the Supplier processing Personal Data during the Term as described in more detail below:

List of Parties	**Data Controller: Client** **Data Processor:** Timetastic Limited. **Address**: Kings Court, Water Lane, Wilmslow, Cheshire, SK9 5AR. **Contact:** hello@timetastic.co.uk
The subject matter of the processing	The personal data of the Data Controller's employees will be processed by the Data Processor in the delivery of the services
The duration of the processing	We keep most of your data for as long as you're using Timetastic - when you cancel your account, your data is deleted. If there's no payment or activity on a Timetastic account for 18 months, we consider that dormant and will delete the account and all its data, just as if you'd cancelled. After your account is closed the only personal data we retain is for accounting and legal purposes, which we're required to keep for 6 years. In some circumstances, like complaints and litigation, we're allowed to retain your personal data for longer. When you contact us for support, that conversation is retained for 12 months. We have a background process that automatically deletes conversations when they hit 12 months old.
The nature and purpose of the processing	Timetastic will process personal data for the following purposes: • To provide clients with a software as a service solution for employee records and absence management.
The type of personal data being processed	Personal Data including but not limited to identity data, contact data, financial data, technical data, profile data, usage data, location data, aggregated data and any additional fields relating to an employee in the context of employment as specified by the data controller in the Timetastic software for employee records management purposes. This could extend to 'Special Categories of Data' for absence management purposes. Special Categories of Data would only be input at the discretion of the controller and is not a requirement for the provision of Timetastic services.
The categories of data subjects	Employees (including, but not limited to, contractors, consultants etc.) of the data controller using Timestastic products and services for their ancillary purposes.

Technical and Organisational Security Measures

The following sections define our current technical and organisational measures. We may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1. **Information Security Program and Organisation**
    1. We maintain and will continue to maintain a written Information Security Program that includes policies, procedures, and controls, including the Information Security Policy.
    2. We are Cyber Essentials certified Cyber essentials is a set of baseline technical controls laid out by the UK government. The requirements are specified under five technical control themes:

    - Firewalls
    - Secure configuration
    - User access control
    - Malware protection
    - Security update management
    - We are, and always will maintain this certification as a baseline for our IT controls.

    3. We have an appointed Data Protection Officer (DPO) as a resource to help with any data management processes, complaints and queries.

2. **Human Resources and Security**
    1. We will conduct reasonable and appropriate background/verification checks on all staff prior to employment, including checks of identification, right to work and verification of previous employment.
    2. Our staff access to client data is bound by confidentiality clauses within their employment contract and non-disclosure agreements.
    3. We will conduct security awareness/cyber security training once per month and data protection training annually for all staff.
    4. We have formal disciplinary processes in place to take action against staff who breach internal Policies.

3. **Physical Security Controls**
    1. Timetastic is hosted on Microsoft's Azure Cloud Platform. This places your data in their European data centres. At the time of writing, we use both their UK South and UK West. Timetastic is hosted within data centres provided by Microsoft Azure. As such, we take advantage of their physical, environmental and infrastructure controls.
    2. Azure is accredited to ISO 27001 which covers and accredits their physical security controls.
    3. Data locations have a protected physical perimeter, strong physical controls including, but not limited to, access control mechanisms, tightly controlled outer and inner perimeters with increased security at each level, including perimeter fencing, security officer, locked server racks, integrated alarm systems, around the clock video surveillance, and multi-factor access controls. For further details please refer to AWS - https://timetastic.co.uk/legal/timetastic-data-security

4. **Access Controls**

1. We regularly review the access rights to ensure that all user accounts and user account privileges are allocated on a need-to-know basis. Upon a change in scope of employment or termination of employment, access rights are removed or modified as appropriate. Least privileged Role Based Access Controls (RBAC) are in place across our network.
2. Our team doesn't have a reason to access or process customer data on a day-to-day basis. Processing is fully automated. It's only if there's a problem with an account or to help resolve a customer support question that we might need to access personal data. All our team members have signed confidentiality undertakings and undergo GDPR training in respect of their roles. We use role-based access controls for staff and use two-factor auth on both internal apps and external services.
3. Access to highly sensitive systems and cloud infrastructure is controlled by secure log-on procedures including Multi-Factor Authentication or Virtual Private Networks.
4. Timetastic is geographically spread and load balanced across multiple Azure data centres. It comes with extensive application and infrastructure monitoring. We maintain redundancy throughout our infrastructure in order to minimise the risk of low or slow availability or loss of data.
5. We use web application firewalls, rate limiting & DDOS protection to provide resilience and ongoing availability.

5. **Operational System Security and Encryption**
    1. We maintain a formal Software Development Lifecycle Framework that includes secure coding practices based on Open Web Application Security Project (OWASP) recommendations and related standards and will perform both manual and automated code reviews before the code is released into a production environment.
    2. We perform an external penetration test of our client facing applications on an annual basis to assess the security of the service. All tests are undertaken by a CREST certified third-party.
    3. We maintain an isolated production environment that includes commercial-grade network management controls such as a load balancer, firewall, and intrusion detection system.
    4. We encrypt and protect all data in transit using TSL 1.2 or above for any communication between services or from client to server.
    5. We encrypt and protect all data at rest using Transparent Data Encryption (TDE) for SQL Databases. Storage data is encrypted by default using 256-bit AES encryption (FIPS 140-2 compliant).
    6. We run regular internal vulnerability scans utilising best in class third party applications. CVE scores are used when conducting vulnerability scans and known vulnerabilities are categorised and remediated.
    7. We have in place password requirements for internal users with a minimum 16-character passphrase consisting of 3 unconnected random words. For the client facing application the password requirements are 8-20 characters, at least one lowercase letter, one uppercase letter, one number and at least one special character (?!*@).
    8. Passwords for signing in are hashed and salted using an PBKDF2-based function in line with the recommendations of the UK's National Cyber Security Centre .
    9. We suggest all users set up two-factor authentication in Timetastic to protect their account and data.
    10. We also offer Single Sign-On (SSO) to access Timetastic with any of the main identity providers, including Microsoft 365 Active Directory or Google Workspace.
    11. Only you, the client, can invite and remove users and apply permission levels in your account.

12. We automate a lot of tests that monitor our infrastructure to make sure it's up and running 24/7. We also use an external service to monitor availability, you can see our current and historical availability on our status page .
13. We complete the Cyber Essentials accreditation each year as well as periodic penetration tests and are happy to work with security researchers .

6. **Incident Response and Breach Notification**
    1. We maintain procedures that ensure an appropriate response to security incidents addressing monitoring, investigation, response, and notification.
    2. All events are recorded in log files, therefore it's possible to review when and by who personal data was entered, altered, or deleted. We provide access to this information in the form of downloadable CSV files in Timetastic.

7. **Business Continuity and Disaster Recovery**
    1. We store client data redundantly at multiple locations in our hosting provider's data centres to ensure availability. We maintain backup and restoration procedures, which will allow recovery from a major disaster.
    2. We maintain a business continuity/disaster recovery plan. The plan provides for the restoration of access to client data, a continuation of operations and Services during a range of short-term and long-term disaster events. The plan covers re-establishment of information technology environment(s) following an unplanned event impacting the data centre, infrastructure, data, or systems.
    3. The Business continuity/disaster recovery plan and related procedures are tested at least annually.

Approved Third Party Processors

Peaberry Software Inc.

Service We use Customer.io for sending emails. To do this Customer.io stores user names, email addresses and analytical data on their usage of Timetastic. We use this data to make sure we only send emails that are relevant to your use of Timetastic.
The types of data shared are: Identity, Contact, Technical, Profile, Usage.
Location of Processing (Country) All the data is stored in the EU.
Cross-border Documentation in place Basis of transfer is the UK-EU adequacy agreement.

Zendesk Inc.

Service Our customer support system is provided by Zendesk. When send in a support request your email addresses will appear in Zendesk along with the discussion between us.
Data Types The types of data shared are Identity, Contact, Technical, Profile, Usage.
Location of Processing (Country) Data is stored in the USA.
Cross-border Documentation in place Basis of transfer is a Data Processing Agreement that includes the EU Standard Contractual Clauses as well as being a member of the Data Privacy Framework offering adequate level of protection.

Sendgrid Inc.

Service All the transactional emails from Timetastic are sent out through Sendgrid Inc. That means sharing email addresses and email content.
Data Types The types of data shared are Identity & Contact.
Location of Processing (Country) Data is stored in the USA.
Cross-border Documentation in place Basis of transfer is a Data Processing Agreement that includes the International Data Transfer Addendum to the EU Standard Contractual Clauses.

Cloudflare Inc.

Service We use Cloudflare to deliver content globally, manage web traffic and as part of our web security setup. All information contained in web traffic to and from Timetastic goes through Cloudflare's systems, but they don't have access to this information.
Data Types The types of data shared are Technical - IP address and device information.

Location of Processing (Country) Data is stored worldwide.
Cross-border Documentation in place Basis of transfer is the EU Commission Standard Contractual Clauses and UK transfer addendum.

Microsoft Inc.

Service We use Microsoft Azure to host and provide you with Timetastic (they are our cloud hosting provider). Cloud Infrastructure Provider – Where the application code and database reside. We also use Microsoft to store daily, weekly, and monthly backups of the database. Office 365 – personal data included in emails, documents and other data transferred in electronic form in the context of using MS services.
Data Types The types of data shared are Identity, Contact, Technical, Profile, Usage, Location.
Location of Processing (Country) Data is stored in the UK.
Cross-border Documentation in place N/A