Guidelines for Using TimeTap Services in a GDPR-Compliant Manner

Last Updated: 9th January 2020

1 Introduction

The TimeTap Services ("Services") provide appointment capabilities over the internet. This document describes how to use these Services in a manner compliant with the EU General Data Protection Regulation (GDPR).

When used as directed:

- no Client Personal Data leaves the European Economic Area (EEA) and
- data is Processed with security and privacy measures compliant with the GDPR

To help customers meet their compliance obligations, TimeTap provides a Data Processing Addendum (DPA) to the standard License Agreement. To request a copy of the DPA, please email privacy@TimeTap.com.

2 Sending Personal Data to the Services

We take every precaution to ensure that personal data is secure; however we also rely on you to keep your information secured as well.

Due to the nature of our Services, we have no way of knowing the types of Personal Data you send to us or the categories of Data Subject to whom any Personal Data relates. It is your responsibility to only store the minimum amount of Personal Data required for Processing.

Rule 1 - Personal Data should be sent ONLY to the Services as follows:

1. The HTTPS protocol must be used to ensure the transmitted data is encrypted

Any Data sent according to the above rules (and any document created) reside only on the computer servicing the request, and only for the duration of the request. As such, no Personal Data is stored by TimeTap. The computers servicing these requests reside within the EEA.

3 Custom Fields and Images should not contain Personal Data.

Appointment provisioning includes the use of custom fields provisioned by the customer:

- Custom Fields
- Images

The geographic region used to store the resources is determined by:

- The region selected when using TimeTap Services.
- The endpoint URL when using the API.

These resources should only be stored in the European region. This is necessary for processing to occur in the EEA.

These resources should not contain Personal Data.

Rule 2 - Only store Personal Data or Images in the Europe region.

1. When configuring custom fields or images via the Console, ensure the Europe region is selected in the top left corner.
2. When updating fields or images via the API the endpoint URL used must be:
   https://www.TimeTapeu.com/api/*.
3. Instead of using Personal Data in resources, use TimeTap "placeholders" in the template.
4. Send the personal Data to the Services as per Rule 1 above.
5. The "placeholders" allow both text and image data of a sensitive nature to be provided only in accordance with Rule 1 above.

4 Do not send Personal Data to TimeTap in any other manner.

The TimeTap Support Team and other team members are based outside the EEA.
When communicating with TimeTap, do not send Personal Data other than as described in Rule 1 above.

Rule 3 - Do not sent Personal Data to TimeTap Support or other team members.

1. If you require support from TimeTap – do not include Personal Data in any documents / data / documents / screenshots that you send.
2. Instead, consider sending a cut-down version that highlights the problem you have using non sensitive data.
3. This applies to any information you send, whether via our website or via email.

5 Specific GDPR Compliance Notes

Article 28 (3)

Documented Instructions	Your calls to the TimeTap Cloud Web Services API specify your documented instructions to TimeTap on how to process your data
After the provision of services	TimeTap returns data to you according to your instructions in the API call and automatically deletes personal data
Records of processing	We maintain aggregate records of your individual processing requests such as the number of times an email/text is used or the number of appointments generated, but we do not store a record of each processing activity. This is your responsibility.

Article 32 (1)

Encryption	Personal Data is encrypted in transport and NOT stored. Other data (templates/images) are encrypted in transport and encrypted at rest where stored.
Confidentiality, integrity, availability and resilience of processing systems and services	Please refer to our description of TimeTap Cloud Security Measures on the TimeTap website.
Restore access to personal data	When the Services are used according to these guidelines, we do not store Personal Data