Version:	CYBSAFE-Personal Data outside EEA-180518 JW
Author:	Jonathan Webster, CTO
Last updated/reviewed:	18/05/18

PERSONAL DATA PROCESSED BY OUR PLATFORM OUTSIDE THE EEA

1. Intercom - help / lead tool

Data - IP Address / Browser details, will track return visits. If provided: Email, name, customer conversations, company of employment.

Mechanism - Browser based js tool, using cookies.

Retention - Anonymous interactions are held for 90 days only. Conversations / Identified leads or customers are kept indefinitely. CybSafe keep the 400-500 most recent.

Jurisdiction - US with AWS. AWS

https://www.intercom.com/security

If US, do they subscribe to Privacy Shield? Yes

https://www.intercom.com/terms-and-policies#eu-us

Terms

https://www.intercom.com/terms-and-policies#terms

2. Google Analytics

Data - IP Address / Browser details / Internet usage monitoring. Not personally identifiable but Google can provide profiling if they have enough data. Profiling meaning (estimated age, gender, industry of employment)

Mechanism - Browser based js tool, using cookies

Retention - 26 months. After contract cease, client/user PII is removed/pseudo anonymised, but with test scores and usage stats retained.

Jurisdiction - EEA & US (we cannot guarantee which data centre this information might go to).

If US, do they subscribe to Privacy Shield? Yes

https://support.google.com/analytics/answer/7105316?hl=en

Terms

https://privacy.google.com/businesses/processorterms/

https://www.google.com/analytics/terms/dpa/dataprocessingamendment_20160909.html

3. SendGrid - email sending

Data - Sendgrid are CybSafe's SMTP relay, Email address, names and account information can be placed in emails. To customer administrators, they can be sent information relating to and identifying their employee users. Sendgrid record mailbox delivery records, clicked links, metadata etc.

Mechanism - Email Relay (SMTP)

Retention - (sendgrid site) We retain email message activity/metadata (such as opens and clicks) for 365 days. We store bounce messages and spam reports (which may contain content) indefinitely, and we store minimal random content samples for 61 days.

Jurisdiction - US

If US, do they subscribe to Privacy Shield? Yes
https://sendgrid.com/wp-content/uploads/2018/03/2-18_SendGrid_FAQ.pdf

Terms

https://sendgrid.com/policies/tos/

4. ## Twilio - SMS sending

Potentially voice calling in future (Vishing product)

Data - Telephone number, name

Mechanism - HTTPS API

Retention - Twilio SMS message and traffic storage

The traffic data, or CDRs, for SMS messages is stored for 10 years. We store this information for tax compliance purposes.

The SMS content, or messages sent and received, is stored as specified by the project owner or Twilio customer. Customers can choose to delete message bodies any time via an HTTP DELETE request. Once the request is received, it is removed from the customer facing repository that holds messages. Message bodies may persist up to 30 days in database backups. Twilio backs up its data bases in order to be able to recover from service failure. These backups are deleted every thirty days.

Jurisdiction - EEA & US (we cannot guarantee which data centre this information might go to).

If US, do they subscribe to Privacy Shield? Yes

https://www.twilio.com/legal/privacy/shield

Terms

https://www.twilio.com/legal/tos

5. ## Sentry.io

Error Reporting platform

Data: Email address, client id (unique client identifier: eg 135), language, country, IP address. Error debugging information. Other personal data is not routinely captured but this is a crash report, so potentially information is contained amongst the technical information (passwords are intentionally & automatically filtered out).

Mechanism - HTTPS API

Retention - 90 days.

Jurisdiction - US

If US, do they subscribe to Privacy Shield? Yes

https://sentry.io/security/

Terms

https://sentry.io/terms/

Personal Data processed outside the EEA is communicated to our partners and customers as follows in a schedule attached to our customer and reseller agreements.

Schedule looks like this:

Subject matter of processing

Cybsafe is providing the Services to the Customer through a unified cyber awareness platform which educates Authorised Users via a range of modules designed to optimise behavioural change.

Duration of Processing

Personal Data will be processed for the duration of this Agreement

Nature and Purpose of Processing

Cybsafe will process the Personal Data in order to identify and authenticate Authorised Users, give the Customer and Authorised Users access to the learning modules, analyse the levels of understanding and improvements in behaviour of Authorised Users in relation to cyber security and provide analyses to the Customer.

Cybsafe will anonymise the Personal Data for use as comparative and statistical information.

Types of Personal Data to be Processed

Data of Authorised Users to be processed will be:

- Name
- Business email address
- Personal email address (if shared),
- Gender
- Age

Categories of Data Subjects

The Data Subjects will be employees, agents and independent contractors of the Customer authorised to use the Services.

Transfers of Personal Data to a country outside EU/international organisation

Some third party tools - such as Google Analytics - used by Cybsafe to deliver the Services involve personal data being processed in the USA. This is only done under the legally binding personal data protection terms of EU-US Privacy Shield Agreement.

END OF DOCUMENT