A Q&A TO HELP OUR CUSTOMERS UNDERSTAND HOW WE ARE REVISING OUR BUSINESS TERMS TO BE GDPR-COMPLIANT

Cybsafe (we or us) is committed to complying with the General Data Protection Regulation (GDPR).

In our arrangements with our customers (you):

- we are a **data processor** and.
- you are a **data controller**.

Under the GDPR, arrangements between a data controller and a data processor must be documented in a contract which now has to contain certain provisions. We have incorporated provisions into our documents with you to reflect the obligations on data processors under the GDPR. Those obligations also have to be contained in any agreement which we have with a sub processor.

You'll need to know the following terms:

- **personal data** means any information relating to a living individual who can be identified, directly or indirectly, from that information, whether or not in association with other information
- **data subject** means any living individual who can be identified from personal data
- **controller** means any person or organisation which directs how and why personal data is processed
- **processor** means any person or organisation which processes personal data on behalf of a controller
- **processing** means any operation performed on personal data, including: collecting, organising, storing, altering, retrieving, consulting, using, sharing, updating and deleting.

The clauses in our revised terms address the following points:

1. What personal data from your employees do we use?

You provide us with certain information about your employees who are to have access to our training modules. This includes:

- each employee's name, and
- their email address (which may be a business address if the employee has one or their personal email address if they don't).

This is personal data which you have in your capacity as their employer.

We may also ask each employee to give us information about:

- their gender and
- the age bracket which applies to them.

We do not need or ask for any "sensitive personal data".

2. What purposes do we use the personal data for?

We use the personal data in order to identify and authenticate each employee, matching the data they input to the information which you have supplied to us. This enables us to give the employees access to the learning modules. We also analyse the level of understanding and improvements in the employees' behaviours towards cyber security and provide analyses to you of the performance of your employees.

3. Do we use your employees' personal data for our own purposes?

No we don't. Where we are acting as a data processor, we can only use the personal data in accordance with your instructions. That is reflected in the data protection clauses in the agreement and a Schedule to the agreements called "Data Processing Details".

It's important for you and for us that those details are included in the agreement. If there are laws which require us to use the data in some other way, then we must tell you.

4. What security do we have in place to protect personal data?

We assess the types of security systems and processes we need, taking into account a number of factors including:

- the state of the art,
- the costs of implementing the measures,
- the nature, scope and purposes of the processing, and
- the risks to the employees.

Our Platform Security Policy explains the key security measures that are in place on the website and server infrastructure.

The GDPR also requires us, as a data processor, to assist you, as a data controller, with any of the requests which an employee can make about their personal data under the GDPR (e.g. if an employee makes a subject access request). We have to take that into account in devising our systems and processes.

5. Will CybSafe staff keep your personal data confidential?

The GDPR requires that all of our staff who deal with the personal data are subject to obligations of confidentiality. Our staff have confidentiality provisions in their employment contracts.

6. Can CybSafe pass your employees' personal data to another organisation?

We can only do this if you agree.

Where we have been introduced to you by a member of our Partner Programme, and you want that partner (usually only Resellers as you are their customers rather than ours) to have an ongoing role in monitoring and reporting on your employees' use of our training, we will need your agreement to pass the personal data to the partner for that purpose.

Remember that it is your responsibility to ensure that you can give us that authority.

7. Can you ask us to help if an employee of yours exercises one of their rights under the GDPR?

The GDPR provides new rights for data subjects. Your employees can not only ask to see the personal data which is held about them but ask for it to be corrected if it is wrong, and, in certain circumstances, object to the use of their personal data or ask for it to be erased. We will refer any request from an employee to you, (and not respond to the request) and provide reasonable assistance to you in dealing with the request.

We have to keep certain records of the processing of the personal data which we carry out and will make those records available to you if you request them.

8. Do we transfer the personal data abroad?

All of the personal data on platform is held in the EEA. Our storage and backup policies are explained in our Platform Security Policy. 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.

9. What happens if there is a breach of security or a complaint?

If a breach of security leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any personal data we must tell you and provide certain information about the breach and its likely consequences.

If there is a complaint against either us or you relating to our or your obligations under the GDPR then you and we must promptly tell the other.

10. What happens to the personal data at the end of the contract between you and CybSafe?

We will delete or return the personal data to you at the end of the agreement unless we are required, by law, to store the data or we require to store the data in the event of any legal claim.

11. Who is responsible for making sure that we have the right to use the personal data?

It is your responsibility, as the data controller, to ensure that you can make your employees' personal data available to us so that we can provide the services. As you are collecting and using your employees' personal data in your capacity as an employer you should not rely on the consent of the employees to those uses unless no other lawful basis of processing exists. The lawful bases of processing under the GDPR are:

- the employee has given consent
- processing is necessary for the performance of a contract made with the employee (e.g. the employment contract)
- processing is necessary for compliance with a legal obligation to which the customer is subject;
- processing is necessary in order to protect the employees' vital interests (or those of another individual);
- processing is necessary in the public interest or under official authority;
- processing is necessary in the customer's legitimate interests (or those of a third party), subject to the employees' interests or fundamental rights and freedoms.
- Who is responsible for making sure that we have the right to use the personal data?

12. Do you have a Data Protection Officer?

Yes, please email dpo@cybsafe.com.

13. When will our GDPR-related updates be live?

In advance of the GDPR coming into force on 25th May 2018.

14. Some helpful links

- Letter from the CEO to Customers and Partners.
- Here are our GDPR-compliant:
    - Terms & Conditions (CybSafe Pro)
    - Terms & Conditions (CybSafe Lite)
    - End User Licence Agreement (Mobile App)
    - Privacy Policy.
- Here is the Information Commissioner's Office Guide to the General Data Protection Regulation (GDPR)

END OF DOCUMENT