A Q&A TO HELP OUR PARTNERS 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 each of your customers:

- we are a **data processor** and.
- the Customer is a **data controller**.

Under the GDPR, arrangements between a data controller and a data processor must be contained in a contract which now has to contain certain provisions. We have incorporated those provisions into our documents with our Customers to reflect the obligations on data processors under the GDPR.

As one of our Partners, you are also a data processor and a sub processor of ours. **Note: this does NOT apply to Affiliate partners.**

We have incorporated provisions into your contract with us to reflect that relationship and the obligations which therefore apply to you under the GDPR.

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 agreement with you address the following points:

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

Each of your customers provide us with certain information about their 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 the Customer has in their capacity as the employer of those individuals.

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. For what purposes do we use the employees' personal data?

We use the personal data in order to identify and authenticate each employee, matching the data they input to the information which the Customer has 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 the Customer of the performance of their employees.

3. For what purposes do you use the employees' data?

The Customer may request that you are provided with access to all or some of the personal data which we use so that you:

- can oversee the Customer's use of our services, and
- review the analyses of their employees' use of the services, their levels of understanding and progress.

You can only use the personal data for those purposes.

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

No. You are acting as a data processor, so you can only use the personal data in accordance with our instructions (which reflect the instructions of our Customer). That is reflected in the data protection clauses in our agreement with you and a Schedule to the agreement called "Data Processing Details" It is important for you and for us that those details are included in the agreement. If there are laws which require you to use the data in some other way then you must tell us - promptly.

5. What security must you have in place to protect personal data?

You must have systems and processes in place, 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.

This is to:

- to make sure that you have an appropriate level of security to prevent unlawful destruction, loss, alteration, unauthorised disclosure of or access to the personal data; and
- to assist us and our Customers 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).

6. How can our Customer be comfortable that your staff will keep their employees' personal data confidential?

The GDPR requires that all of your staff who deal with the personal data are subject to obligations of confidentiality. Your staff must therefore have confidentiality provisions in their employment contracts and must have been trained in compliance with the GDPR.

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

You can only do this if we (and the Customer) agree.

8. Can we ask you to help if an employee exercises one of its rights under the GDPR?

The GDPR provides new rights for data subjects. Our Customer's 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. You must refer any request from an employee to us (and not respond to the request) so that we can refer it to the Customer. You may need to provide reasonable assistance to us or the Customer in dealing with the request.

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

9. Do you transfer the personal data abroad?

Only if we specifically agree that you may do so. This is likely to mean that additional provisions will need to be added to your agreement with us. It is important that you check where any personal data which you process is stored.

You must tell us if it is stored on servers which are outside the EU.

10. 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 you must tell us and provide certain information about the breach and its likely consequences.

If there is a complaint against you relating to your obligations under the GDPR then you must promptly tell us.

11. What happens to the personal data at the end of the contract between you and us?

You must delete or return the personal data to us at the end of the agreement unless you are required, by law, to store the data.

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

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

13. Some helpful links

- Letter from the CEO to Customers and Partners.
- Here are our GDPR-compliant. End User Licence Agreement (Mobile App)
- Here is the Information Commissioner's Office Guide to the General Data Protection Regulation (GDPR)

END OF DOCUMENT