



The Health and Safety Consultancy
The Annex
8 Astridge Road
Witcombe
Gloucestershire
GL3 4SY
01452 864213

VAT Registration Number: 229 9431 80

Data Processing Agreement

This Data Processing Agreement is incorporated into the standard terms of engagement for the provision of health and safety services between THE HEALTH AND SAFETY CONSULTANCY LIMITED and its Clients with effect from May 25, 2018.

1. Background:
 - 1.1. On May 25, 2018, the General Data Protection Regulation (GDPR) comes into effect replacing prior data protection laws and imposing obligations on the Controllers and Processors of Personal Data
 - 1.2. The Client is the Controller of Personal Data collected and processed in connection with its business activities
 - 1.3. The Consultant may have access to the said Personal Data in order to process it on behalf of the Client and, in addition, where the Services provided by the Consultant include access to the training portal created by the Consultant for the delivery and processing of training data, may collect Personal Data and process it on behalf of the Client
 - 1.4. These written terms and conditions are intended to ensure that there are proper arrangements in place relating to Personal Data passed from the Client to the Consultant or processed by the Consultant on its behalf as required by the GDPR and, in particular, Article 28.
2. Definitions:
 - 2.1. Capitalised expressions shall have the same meaning as set out in the GDPR.
 - 2.2. "Services" means the services provided by the Consultant to the Client as set out in the engagement for services between the parties hereto, including training services.
 - 2.3. "Data" means the data collected or processed by the Consultant on behalf of the Client.
 - 2.4. "Training Portal" means the website sub domain operated by the Consultant to deliver training.

Registered Number: 9939204
Registered Office: Unit 17, Foxes Bridge Road, Forest Vale Industrial Estate,
Cinderford, Glos, GL14 2PQ
Email: elizabeth.matthews@thehealthandsafetyconsultancy.co.uk
Web: www.thehealthandsafetyconsultancy.co.uk

3. Data Processing:
 - 3.1. The Client is the data controller for the Data and the Consultant is the data processor for the Data.
 - 3.2. The Consultant agrees to process the Data only in accordance with GDPR and in particular on the following conditions.
 - 3.3. The Consultant shall only process the Data:
 - 3.3.1. on the written instructions from the Client, including in accordance with this agreement
 - 3.3.2. only process the Data for completing the Services and
 - 3.3.3. only process the Data in the UK with no transfer of the Data outside of the UK (Article 28, para 3(a) GDPR);
 - 3.4. The Consultant will ensure that all employees and other representatives accessing the Data are:
 - 3.4.1. aware of the terms of this Agreement;
 - 3.4.2. have received comprehensive training on data protection and related good practice;
 - 3.4.3. are bound by a commitment of confidentiality (Article 28, para 3(b) GDPR)
4. Rights of Data Subjects
 - 4.1. The Consultant will immediately notify the Client in the event of any request received from individuals exercising their rights laid down in Chapter III of GDPR and will give notice to the individual making the request that it has done so, providing the name and contract details of the Client (Article 28, para 3(e) GDPR).
 - 4.2. The Consultant will at the Client's direction as soon as reasonably practicable:
 - 4.2.1. correct, update and amend Data
 - 4.2.2. safely delete or return the Data at any time, keeping only such information as may be required to demonstrate compliance
 - 4.2.3. provide a copy of the Data
 - 4.2.4. maintain the integrity of the Data, without undocumented alteration, ensuring that the Data can be separated from any other information created
5. Cooperation
 - 5.1. The Consultant will make available as soon as reasonably practicable all information necessary to demonstrate compliance with the obligations laid down under this Agreement and allow for and contribute to any audits, inspections or other verification exercises required by the Client from time to time (Article 28, para 3(h) GDPR)
 - 5.2. The Consultant will immediately contact the Client if there is any personal data breach or incident where the Data may have been compromised and will assist the Client in ensuring compliance with the obligations pursuant to Articles 32 to 36 of GDPR – security, notification of data breaches, communication of data breaches to individuals, data protection impact assessments and when necessary consultation with the ICO etc, taking into account the nature of processing and the information available to the Processor (Article 28, para 3(f) GDPR).
6. Subcontracting

The Consultant shall not subcontract the processing of the Data without the consent of the Client. Such consent shall not be unreasonably withheld and the Client understands and agrees that Data processed on the Training Portal is stored externally on servers owned and operated by third parties. If consent is given a further processing agreement will be required (Article 28, para 3(d) GDPR).

7. Termination

- 7.1. The Client and the Company may each terminate its agreement for the provision of Services as set out in the engagement agreement for services. Upon termination of that agreement this agreement will automatically come to an end unless otherwise agreed in writing.
- 7.2. Upon termination and payment of all outstanding consultancy fees and expenses, the Consultant will provide a complete copy of all Data held on behalf of the Client in a pdf, excel or csv format.
- 7.3. The Consultant will continue to store the Data, but not otherwise process it, for a period of three years following the date of termination (but so that additional copies can be provided to the Client at the Client's request) and shall thereafter delete the Data.

8. Deletion

Where the Consultant is to delete the Data, deletion shall include destruction of all existing copies unless the Consultant shall otherwise have a legal obligation to retain the Data. Where there is a legal obligation to retain data, the Processor will confirm such an obligation in writing to the Client. Upon request by the Client the Processor shall provide certification of destruction of all Data (Article 28, para 3(g) GDPR).

9. Preservation of Rights

Nothing in this agreement shall restrict the right of the Consultant to provide Data to third parties where legally obliged to do so, or as necessary in the defense or pursuance of legal claims.

10. Security of Processing

- 10.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Consultant shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as the Consultant shall deem appropriate:
 - 10.1.1. the pseudonymisation and encryption of personal data;
 - 10.1.2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - 10.1.3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - 10.1.4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- 10.2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
- 10.3. The Consultant shall take steps to ensure that any natural person acting under the authority of the Consultant who has access to Personal Data does not process them except on instructions from the Controller, unless he or she is required to do so by Union or Member State law.
- 10.4. The Consultant will not transfer Personal Data to a third country outside of the European Union unless required to do so by Union or Member State law but so that in such a case, the Consultant shall inform the Client of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest
- 10.5. Data on the Training Portal may be copied periodically to the Client in a pdf, excel or csv format sent, including transmittal by email, to any Director or Partner or to any person authorised by the Client to receive such Data.
- 10.6. Data will be made available for transfer to the Client by viewing online or printing or downloading directly from the database maintained by the Consultant. It shall be the

responsibility of the Client to ensure that confidentiality is maintained when viewing the Data and that only authorised individuals have access to the Training Portal to view.

10.7. Once printed or downloaded or copied to the Client it shall be the responsibility of the Client to maintain the integrity and confidentiality of the Data.

11. General

11.1. This Agreement may only be varied with the written consent of both parties.

11.2. This Agreement represents the entire understanding of the parties relating to necessary legal protections arising out of their data controller/processor relationship under GDPR and related Data Protection Laws.

11.3. This Agreement is subject to English law and the exclusive jurisdiction of the English Courts.