

DATA PROCESSING AGREEMENT

This Agreement is between Contracting Party (hereinafter „Controller“) and LLP SPECTRALSOFT Palliser House, Palliser Rd, London W14 9EB, UK (hereinafter „Processor“) for the processing of personal data acting on behalf of a third party including ("Agreement").

1. Subject and Duration of the Agreements.

1.1. Subject of the Agreement.

The subject of the Agreement is the execution of the following tasks by the Processor in accordance with the service description in [PULSEDESK TERMS OF USE](#) of the Processor agreed between the Parties (Main Agreement): collection, management, documentation and transfer of the consent of the Controller's users or personal data collected on the basis of legitimate interests via the technology provided by the Controller and, if applicable, other services agreed with the Controller in accordance with the Main Agreement. In doing so, the Processor processes personal data for the Controller within the meaning of Art. 4 no. 2 and Art. 28 GDPR on the basis of the Main Agreement. Definitions in the Main Agreement shall also apply in this Agreement. Definitions in this Agreement shall only apply to this Agreement.

1.2 Duration of the Agreement.

The duration of this Agreement (term) shall correspond to the duration of the Main Agreement.

2. Specification of the Agreement content.

2.1. Scope, Nature and Purpose

Scope, nature and purpose of the collection, processing and / or use of personal data by the Processor for the Controller result from the Main agreement.

2.2. Type of Data.

Subject of the collection, processing and / or use of personal data are the following data:

User data:

- Consent Data (Consent ID, Consent date and time, User Agent of the browser and Consent State.)
- Device data (HTTP Agent, HTTP Referrer)
- URL visited
- User language
- IP address
- Geolocation
- Name, email addresses, and telephone numbers
- Company data such as the name, size and location of the company you work for and your role - within the company as well as publicly available company information and activity associated with company data;
- chat transcript data from Client's support chat sessions
- information about a device you use, such as browser, device type, operating system, the presence or use of "apps", screen resolution, and the preferred language;
- behavioral data of the internet connected computer or device you use when interacting with the sites, such as advertisements clicked or viewed, sites and content areas, date and time of activities or the web search used to locate and navigate to a site.

2.3. Categories of Data Subjects.

The categories of data subjects affected by the processing of their personal data within the scope of this Agreement include:

- Website visitors, Affiliates, Clients and or users as it defined in the Main Agreement.

3. Controller's Authority to Issue Instructions / Location of the Data Processing.

3.1. The data is handled exclusively within the framework of the agreements made and in accordance with documented instructions from the Controller (cf. Art. 28 Para. 3 lit. a GDPR). The Main Agreement, this Agreement

and, if applicable, the settings made by the Client for the use of the Services shall constitute the Controller's instructions. Within the scope of the description of the data processing mandate in this Agreement, the client reserves the right to issue comprehensive instructions on the type, scope and procedure of data processing, which he can specify in more detail by means of individual instructions. Changes to the object of processing and procedural changes are to be jointly agreed and documented. Any additional expenses incurred are to be remunerated by the Controller on a time and material basis. The Processor may only provide information to third parties or the person concerned with the prior written consent of the Controller.

3.2 The Processor shall not use the data for any other purposes and shall in particular not be entitled to pass them on to third parties. Excluded from this are back-up copies, insofar as they are necessary to ensure proper data processing, as well as data which is necessary in order to comply with legal obligations under Union law or the law of UK, and to comply with retention obligations.

3.3. The Processor must inform the Controller without delay in accordance with Art. 28 para. 3 subpara. 2 GDPR if it believes that an instruction violates data protection regulations. The Processor is entitled to suspend the execution of the corresponding instruction until it is confirmed or amended by the person responsible at the Controller.

3.4. The processing of the Controller data by the Processor takes place within the EU / UK. The Processor shall be obliged to inform the Controller prior to the commencement of the processing of the Controller's data of a legal obligation of the Processor to carry out the processing of the Controller's data at another location, unless such notification is prohibited by law. The processing and / or transfer to a third country outside the territory of the EU / UK or to an international organization requires the prior written consent of the Controller. In this case, the Processor shall also be required to ensure an adequate level of data protection at the place of data processing in accordance with the applicable statutory provisions and the interpretations thereof by courts and authorities or - at the Controller's option - to give the Controller the opportunity to ensure an adequate level of data protection, including by concluding or acceding to standard EU contractual clauses, published by the EU Commission on 4.6.2021, available https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en, as well as additional measures where necessary.

4. Confidentiality.

4.1. The Processor shall ensure that employees involved in the processing of personal data and other persons working for the Processor are prohibited from processing the personal data outside the scope of the instruction. Furthermore, the Processor shall ensure that the persons authorized to process the personal data have committed themselves to confidentiality or are subject to an appropriate legal obligation of secrecy. The confidentiality / secrecy obligation shall continue to exist after the termination of the Agreement.

5. Technical-organisational Measures.

5.1. Within his area of responsibility, the Processor shall design the internal organisation in such a way that it meets the special requirements of data protection. He will take appropriate technical and organisational measures to protect the personal data of the Controller which meet the requirements of Art. 32 GDPR. In particular, the technical and organisational measures are to be taken in such a way that the confidentiality, integrity, availability and resilience of the systems and services in connection with data processing are permanently guaranteed. The Controller is aware of these technical and organisational measures and is responsible for ensuring that they provide an adequate level of protection for the risks of the data to be processed.

5.2. The technical and organisational measures are subject to technical progress and further development.

6. Subprocessors.

6.1. The engagement and/or change of Subprocessors by the Processor is only allowed with the consent of the Controller. The Controller agrees to the engagement of Subprocessors as follows:

6.1.1. The Controller agrees to the use or modification of Subprocessors if the Processor notifies the Controller of the use or change in writing (email sufficient) thirty (30) days before the start of the data processing. The Controller may object to the use of Subprocessor or the change. If no objection is made within the aforementioned period, the approval of the use or change shall be assumed to have been given. The Controller acknowledges that in certain cases the service can no longer be provided without the use of a specific Subprocessor. In these cases, each party is

entitled to terminate the contract without notice. If there is an important data protection reason for the objection and if an acceptable solution between the parties is not possible, the Controller is granted a special right of termination. The Controller shall declare its intention to terminate the contract in writing to the Processor within one week after the failure to reach an agreeable solution. The Processor may remedy the objection within two weeks of receipt of the declaration of intent. If the objection is not remedied, the Controller can declare the special termination, which becomes effective upon receipt.

6.2. The Processor shall design the contractual arrangements with the Subprocessor(s) in such a way that they contain the same data protection obligations as defined in this Agreement, taking into account the nature and extent of data processing within the scope of the Subcontract. The Subprocessor's commitment must be made in writing or in electronic format.

6.3. Subcontracting relationships within the meaning of this provision do not include services which the Processor uses with third parties as ancillary services to support the execution of the Agreement. These include, for example, telecommunications services, maintenance, and user service, cleaning staff, inspectors, or the disposal of data media. However, the Processor is obliged to make appropriate and legally compliant contractual agreements and to take control measures to ensure the protection and security of the Controller's data, even in the case of ancillary services contracted out to third parties.

7. Data Subject Rights.

7.1. The Processor shall support the Controller within the scope of its possibilities in meeting the requests and claims of affected persons in accordance with Chapter III of the GDPR.

7.2. The Processor shall only provide information on the data processed on behalf of the Controller, correct or delete such data or restrict the data processing accordingly upon instruction of the Controller. Insofar as a data subject should contact the Processor directly for the purpose of information, correction, or deletion of his/her data as well as with regard to the restriction of data processing, the Processor shall forward this request to the Controller without undue delay.

8. Processor's Obligations to Cooperate.

8.1. The Processor shall assist the Controller in complying with the obligations regarding the security of personal data, reporting obligations in the event of data breaches, data protection impact assessments, and prior consultations as set out in Articles 32 to 36 GDPR.

8.2. With regard to possible notification and reporting obligations of the Controller according to Art. 33 and Art. 34 GDPR the following applies: The Processor is obliged (i) to inform the Controller without undue delay of any violation of the protection of personal data and (ii) in the event of such a violation, to provide the Controller with appropriate support, if necessary, in its obligations under Art. 33 and 34 GDPR (Art. 28 para. 3 sentence 2 lit. f GDPR). Notifications pursuant to Art. 33 or 34 GDPR (notifications and reports of violations of personal data protection) for the Controller may only be carried out by the Processor following prior instructions pursuant to Section 3 of this Agreement.

8.3. If the Controller has an obligation to notify or report in the event of a security incident, the Processor is obliged to support the Controller at the Controller's expense. In the case the security incident results from the risk sphere of the Processor, the Controller is not obliged to reimburse costs.

9. Other obligations of the Processor.

9.1. The Processor shall inform the Controller immediately of control actions and measures taken by the supervisory authority pursuant to Art. 58 GDPR. This shall also apply if a supervisory authority is investigating the Processor in accordance with Art. 83 GDPR.

9.2. The Processor shall ensure to execute the control of the proper contract performance and fulfillment by means of regular self-inspections, in particular the adherence to and, if required, the necessary adjustment of regulations and measures for the execution of the contract.

10. Controller's right to information and inspection.

10.1. The Controller has the right to request the information required under Art. 28 Para. 3 h) GDPR to prove that the Processor has complied with the agreed obligations and to carry out inspections in agreement with the Processor or to have them carried out by auditors to be appointed in individual cases.

10.2. The parties agree that the Processor is entitled to submit convincing documentation to the Controller in order to prove adherence to his obligations and implementation of the technical and organizational measures. Convincing documentation can be provided by presenting a written report displaying the compliance covering the security by the Processor.

10.3. This shall not affect the right of the Controller to conduct on-site visits. However, the Controller shall consider whether an on-site inspection is still necessary after submission of meaningful documentation, in particular taking into account the maintenance of the Processor's regular business operations.

10.4. The Controller has the right to assure himself of the Processor's compliance with this Agreement in his business operations by means of spot checks, which as a rule must be announced in good time. The Processor is committed to provide the Controller, upon request, with the information required to comply with his obligation to carry out inspections and to make the relevant documentation available.

11. Deletion of Data and Return of Data Carriers.

11.1. In the event of termination of the Agreement, the Processor shall, at the Controller's option and request, hand over to the Controller without undue delay, at the latest within 30 days, all documents, processing and utilization results produced and data files connected with the contractual relationship which have come into the Processor's possession within the scope of the implementation of the Agreement or destroy them in accordance with data protection law after prior consent. The same shall apply to test and reject material. The protocol of the deletion shall be submitted upon request. By way of derogation, a deletion or surrender period of no longer than 6 months shall apply to back-ups made by the Processor.

11.2. Documentation that serves as proof of the orderly and appropriate data processing shall be kept by the Processor in accordance with the respective retention periods beyond the end of the contract. He can hand them over to the Controller at the end of the contract to exonerate him.

12. Liability.

12.1. The parties' liability under this Agreement shall be governed internally by the liability provisions in the Processor's General Terms and Conditions unless otherwise stated in the service description or in a separate agreement between the parties. For the external legal liability, the regulations according to Art. 82 GDPR apply.

13. Miscellaneous.

13.1. Changes and additions to this Agreement and all of its components, must be made in a written agreement, which may also be made in an electronic format (text form), and the express statement that it constitutes a change or addition to the present terms and conditions. This also applies to any waiver of this written-form requirement.

13.2. The provisions of this Agreement shall survive the termination of the Main Agreement and remain in force until such time as all personal data of Controller have been destroyed in full or returned to Controller.

13.3. In other respects, the provisions of the Main Agreement / the contract shall apply in like manner.

13.4. If any individual part of this Agreement is invalid, this shall not affect the validity of the remainder of the Agreement.