



Information on the processing of Suppliers' personal data pursuant to Article 13 of the UK GDPR

Pursuant to the current legislation on the protection of personal data (the “**Privacy Legislation**”) including EU Regulation 2016/679 (the “**GDPR**”) as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (“**UK GDPR**”), together with the Data Protection Act 2018, **Deep Sea Electronics Limited**, in its capacity as data controller (“**DSE**” or the “**Company**” or the “**Data Controller**”), informs the physical persons who represent and/or operate on behalf of companies that provide services to the Company (hereinafter generally understood as the “**Data Subjects**” or “**Suppliers**”, or in the singular the “**Data Subject**” or the “**Supplier**”) that within the framework of the supply contract in place between them and the Company (hereinafter, the “**Contract**”), the personal data related to the Data Subjects will be processed in compliance with the Privacy Legislation, for the purposes and in the manner described in this policy (the “**Policy**”).

1 Data Controller



The Data Controller is **Deep Sea Electronics Limited**, with registered office in Highfield House, Hunmanby Industrial Estate, Hunmanby, North Yorkshire, YO14 0PH, UK - 53031, VAT no. 3169 234 57, which can be contacted at +44 (0) 1723 89009 or at the following e-mail address sales@deepseaelectronics.com.

2 Personal Data subject to processing



Common Data:

- **identification data** obtained during contractual or pre-contractual relationships with the Company, such as: name, address or other personal identification elements; company name where containing personal data; common data of the Supplier's employees and/or collaborators and/or consultants;
- **contact details**, such as: company e-mail, certified e-mail address, mobile phone number;
- **professional data**, such as: job title; role
- **financial and tax data (if referring to suppliers who are individuals/sole proprietorships)**, such as: IBAN; current account number and, in general, the information necessary to make payments and invoicing.

3 Purpose and legal basis of the processing and nature of the provision of Personal Data

 Purpose of the processing	 Legal basis for the processing	 Period of storage of personal data	 Nature of the provision of Personal Data
a) Performance of the Contract and/or pre-contractual measures such as the selection of Suppliers, the negotiation of contractual relationships, the formalization, stipulation and execution of the Contract, as well as the performance of activities related to the management of accounting and related obligations, contractual obligations, services, invoicing/ payments,	Art. 6 (1)(b): Performance of the Contract to which the Data Subject is a party and performance of pre-contractual measures adopted at the request of the Data Subject.	The personal data of the Data Subjects necessary for the stipulation and performance of the Contract will be stored and processed for the entire duration of the Contract itself and, after its termination, for any reason whatsoever, for a period not exceeding 10 (ten) years (i.e. the ordinary limitation period), with reference to the data necessary for the issuance of certificates or documentation that may be required for any obligations legal,	The provision of personal data is necessary for the establishment and proper performance of the Contract, as well as to correctly comply with current legislation and the obligations arising from the Contract. Therefore, any refusal by the Data Subject to provide personal data, in whole or in part, for the pursuit of the indicated Purposes, will mean it is impossible to establish or perform the Contract or carry out the obligations provided for by the regulations in force.



<p>auditing and mandatory/optional certification of the financial statements, of the assignment or advance of receivables, as well as to fulfill specific requests and comply with other obligations arising from the Contract.</p>		<p>tax and accounting obligations related to or arising from the conclusion of the Contract, as well as for the legal protection of the Company. At the end of the identified retention period, the personal data of the Data Subjects will be deleted, unless there are further legitimate interests of the Data Controller and/or legal obligations that make it necessary, subject to minimization, to retain them.</p>	
<p>b) Fulfilment of obligations provided for by law, regulations, EU or UK legislation or by an order of the Authority (e.g. accounting and budgetary obligations, anti-money laundering, <i>antitrust</i>, as well as tax, health, labour and safety obligations, etc.).</p>	<p>Art. 6(1)(c): Legal obligation to which the Data Controller is subject.</p>		
<p>c) Management of obligations related to the intra-corporate and financial organization (e.g. company secretary, communications, deposits, reporting, solvency checks, etc.), as well as <i>internal reporting & controlling</i>.</p>	<p>Art. 6(1)(f): Legitimate interest of the Data Controller in the proper management of the company in relation to logistical, accounting and financial organization.</p>		
<p>d) Greater control in the context of the qualification processes of its Suppliers and to verify their compliance with the Code of Ethics and the Organization, Management and Control Model adopted by the Company ("OMC"), as well as any other company policies relating to Suppliers.</p>	<p>Art. 6(1)(b): Performance of a contractual obligation, where the Supplier has contractually undertaken to provide the requested information and to comply with the Code of Ethics and the OMC, as well as any additional policies/procedures adopted by the Company.</p> <p>Art. 6(1)(f): Even in the absence of a contractual commitment on the part of the Supplier to comply with the Code of Ethics, the OMC or other company policies/procedures of the Company, the latter may still process some of the Supplier's personal data that it deems necessary to verify that the activities/conduct carried out by the Supplier are not in contrast with its own company principles/rules. In this case, the processing will be based on the legitimate interest of the Data Controller to prevent and counter the notion that the Data Controller was involved in the commission, by the Supplier, of offences provided for under applicable law or of any other conduct deemed to be in contrast with its Code of Ethics and/or with its predecessors/company policies.</p>		



e) Establishing, exercising or defending legal claims.	Art. 6 (1)(f): Legitimate interest of the Data Controller relating to the right of defence and exercise of its rights or of a third party.		
f) Transmit personal data (e.g. data collected as part of audit activities) within the business group to verify compliance with conflict minerals legislation , for internal administrative purposes.	Art. 6(1)(f): Legitimate interest of the Data Controller in proper internal administrative management.		
g) Transmit personal data within the business group for the performance – for internal administrative purposes – of screening activities on Suppliers who are natural persons and on legal representatives of Suppliers who are legal entities to identify persons and/or companies with whom it is prohibited to establish business relationships pursuant to applicable regulations, through the use of software and/or applications implemented at group level (e.g. Amber Road).	Art. 6(1)(f): For details on the adequate safeguards adopted for the transfer of the personal data of the Data Subjects, please refer to point 6 of this Policy below.	[•]	

If the legal basis of the processing is the legitimate interest of the Data Controller, the Data Controller has carried out, or will carry out, a *balancing test* aimed at assessing the proportionality of the processing so that the rights and freedoms of the Data Subjects are not affected, taking into account their reasonable expectations in relation to the specific processing activity carried out.

Data Subjects may request **further information on the above assessment** by sending an e-mail to the following e-mail address sales@deepseaelectronics.com

The Data Controller also informs the Data Subject that he/she has the possibility to **object**, at any time, to the processing of his/her personal data based on the legitimate interest of the Company.

In the event that the Company intends to use the personal data for any other purpose that is incompatible with the Purposes for which the data was originally collected or authorised, the Company will inform the Data Subject in advance and, where required, request his/her consent for such processing activity.

4 Recipients of Personal Data



The personal data of the Data Subjects will be processed by the Company’s employees and collaborators.

Data Subjects’ personal data may be disclosed for the Purposes listed above to additional **recipients or categories of recipients**, as independent data controllers or, where necessary, data processors specifically selected and appointed pursuant to Article 28 of the UK GDPR, including, by way of example but not limited to:

- Third-party companies in charge of carrying out audits for the issue of certifications of compliance with specific European regulations;
- managers of the software and technological infrastructures used by the Data Controller, as well as providers of IT support services;
- consultants and freelancers in individual or associated form (accountants and accounting experts, statutory auditors, lawyers);
- public or private bodies and/or organizations.



Furthermore, the personal data of the Data Subjects may also be disclosed to third parties in the following cases: (i) when the communication is required by applicable laws and regulations with respect to legitimate third party recipients of communications, such as authorities and public economic and non-economic bodies that process your data as independent data controllers for their respective institutional purposes, Etc.; (ii) in the event of extraordinary transactions (e.g. mergers, acquisitions, sale of companies, etc.).

The complete list of recipients of the personal data of the Data Subjects, including further details on the location of the recipients themselves, is kept at the headquarters of the Data Controller and can be requested at any time.

5 Transfer of Personal Data Abroad



The management and storage of personal data will take place on servers located within the UK or European Union, except as described herein.

DSE informs Data Subjects that, being part of an **international group**, some data may be transferred – for the Purposes referred to in point 3 of this Policy above – as well as processors, which are based in the EU, UK, or **United States of America**.

The EU benefits from an adequacy decision of the UK government. Considering that the United States does not guarantee an adequate level of protection of personal data compared to that provided for in the European Union, the Data Controller has taken steps to ensure that the transfer of the personal data of the Data Subjects to this country takes place only in compliance with the conditions set out in art. 45/49 of the UK GDPR and, in particular:

- USA (entities certified under the Data Privacy Framework): Data protection adequacy for non-EU countries (europa.eu); and/or
- possible contractual agreements based Standard Contractual Clauses (“**SCCs**”) as developed by the European Commission pursuant to Article 46 of the EU GDPR as modified by the UK International Data Transfer Addendum (and you are entitled to obtain a copy of these upon request);
- Binding Corporate Rules approved by the UK data protection supervisory authority.

Should the Company intend to transfer the personal data of the Data Subjects to non-UK countries other than those mentioned above, such transfer will take place only in compliance with the conditions set out in art. 45/49 of the UK GDPR.

6 Your rights



The Data Controller informs the Data Subject that, in accordance with the law, he/she will always have the right to revoke his/her consent at any time, where given (without affecting processing occurring prior to revocation), as well as to exercise, at any time, the following rights, subject to any conditions or limitations in applicable law (collectively, the “**Rights**”):

- a) the “**right of access**” and specifically to obtain confirmation of the existence or otherwise of personal data concerning him/her and their communication in an intelligible form;
- b) the “**right to rectification**”, i.e. the right to request the rectification or, if interested, the completion of personal data;
- c) the “**right to erasure**”, i.e. the right to request the erasure, transformation into anonymous form of data processed in violation of the law, including those whose retention is not necessary in relation to the Purposes for which the personal data were collected or subsequently processed;
- d) the “**right to restriction of processing**”, i.e. the right to obtain from the Data Controller the restriction of processing in certain cases provided for pursuant to the Privacy Legislation;
- e) the right to request from the Data Controller the indication of the recipients to whom it has notified any rectification or erasure or limitation of processing (carried out pursuant to Articles 16, 17 and 18 of the UK GDPR, in compliance with the notification obligation except in the event that this proves impossible or involves a disproportionate effort);
- f) the “**right to data portability**”, i.e. the right to receive (or to transmit directly to another data controller) personal data in a structured, commonly used and machine-readable format;

g) the “right to object”, i.e. the right to object, in whole or in part:

- **the processing of personal data carried out by the Data Controller for its own legitimate interest;**
- **to the processing of personal data carried out by the Data Controller for marketing or profiling purposes.**



In the above cases, where necessary, the Data Controller will inform the third parties to whom the personal data of the Data Subject are communicated of the possible exercise of the rights, except in specific cases in which this is not possible or is too onerous and, in any case, in accordance with the provisions of the Privacy Legislation.

It is expressly understood, as provided for in Article 21 of the UK GDPR, that in the event of the exercise of the right to object by the Data Subject, the Data Controller will refrain from further processing the personal data unless the Data Controller demonstrates the existence of compelling legitimate reasons to proceed with the processing that prevail over the interests, rights and freedoms of the Data Subject or for the establishment, the exercise or defence of a right in court.

The exercise of the above Rights is not subject to any formal constraint and is free of charge. The Data Controller may eventually require the Data Subject to verify his/her identity before taking further action following the request to exercise the aforementioned Rights.

The Data Subject may at any time exercise his/her Rights in the following ways:

- by e-mail to: sales@deepseaelectronics.com
- by ordinary mail, to the address of the registered office of Deep Sea Electronics Limited - Highfield House, Hunmanby Industrial Estate, Hunmanby, North Yorkshire, YO14 0PH, UK.

7 Complaint to the Supervisory Authority pursuant to Article 77 of the UK GDPR



You have the right to lodge a complaint with the competent supervisory authority (in particular in the Member State of your habitual residence, place of work or place of the alleged infringement), if you are of the opinion that your personal data is being processed in a way that leads to violations of the UK GDPR.

A complaint can be filed with the UK supervisory authority, the ICO, at <https://ico.org.uk/make-a-complaint/> Make a complaint | ICO.

CHANGES TO THIS POLICY

This Policy may be amended and supplemented from time to time. We invite Data Subjects to periodically check their contents. In any case, it will be the responsibility of the Data Controller to appropriately report any significant changes made to this Policy.

Document updated: 13 June 2024