

Privacy Statement

We take the protection of your personal data very seriously. In this Privacy Statement we, Electro Optical Systems Nordic AB (“We” or “EOS”) will inform you about how we process and use your personal data and on the specific rights you have in connection with your personal data.

One of the main purposes of this Privacy Statement is to fulfil transparency obligations under Regulation (EU) 2016/679 (General Data Protection Regulation, “GDPR”). For this reason we use certain technical terms also used in the GDPR in the context of this Privacy Statement. These and other terms repeatedly used in this Privacy Statement will be explained to you below in Section 2.

Many of our customers are organisations and companies (so-called legal entities). If you contact us as an employee of an organization or a company, we will store and process the categories of data described hereinbelow generally in relation to this organization or company, but may link it to the information that you are employed by such organization or company and are our contact person.

1. Name and Address of the Data Controller, Contact Details for the Data Protection Officer, and Supervisory Authority

1.1. This Privacy Statement describes the data processing for which we, EOS, are the controller within the meaning of the GDPR. You will find our contact details below:

Electro Optical Systems Nordic AB
Stena Center 1 C
41292 Gothenburg
Sweden
Tel. +46 31 760 46 41 Fax +46 70 511 43 26
E-Mail info@eos.info Website: www.eos.info

1.2. You can contact our data protection officer at any time with any questions about data protection. The name and contact details of our group data protection officer who also serves as data protection officer of our company are as follows:

Sabina Hrnjica-Ceman
EOS GmbH Electro Optical Systems
Robert-Stirling-Ring 1, 82152 Krailling
E-Mail: datenschutz@eos.info

1.3. The data protection supervisory authority responsible for us is:

Datainspektionen
Director General Mrs Eva Håkansson
Box 8114 / Drottninggatan 29 5th floor
SE-Schweden - 104 20 Stockholm

Telefon: + 46 8 657 6100

Telefax: + 46 8 652 8652

E-Mail: datainspektionen@datainspektionen.se

2. Definitions

For ease of reading, we use various technical terms in this Privacy Statement which have the following meaning throughout this Privacy Statement:

<i>anonymisation</i>	means rendering personal data anonymous in such a manner that the data subject is not or no longer identifiable taking into account all means reasonably likely to be used, such as singling out, either by the controller or by another person, to identify the natural person directly or indirectly.
<i>consent</i>	is your clear affirmative act establishing a freely given, specific, informed and unambiguous indication of your agreement to the processing of your personal data. For clarification: If processing requires consent, we will obtain this separately. Taking note of this Privacy Statement does not replace consent.
<i>controller</i>	Refers to us, as the entity which, alone or jointly with others, determines the purposes and means of the processing of personal data.
<i>data subject</i>	is you, i.e. the natural person to whom the personal data refers.
<i>direct marketing</i>	is any marketing by which we approach you directly, for example by post or (if permissible) by telephone, e-mail or fax;
<i>GDPR</i>	is Regulation (EU) 2016/679, also known as the General Data Protection Regulation. You can find the full text here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
<i>group of undertakings</i>	comprises EOS Holding AG, Robert-Stirling-Ring 1, 82152 Krailling and all of its subsidiaries (as we are one).
<i>guarantee(s)</i>	includes standard data protection clauses adopted by the Commission, codes of conduct approved by the supervisory authority, and, in relation to the USA, the Privacy Shield Program, and all other measures intended to ensure an adequate level of protection with respect to data protection.
<i>information society service</i>	is any service normally provided for remuneration, at a distance (i.e. without the parties being simultaneously present), by electronic means (i.e. by means of electronic equipment for the processing (including digital compression) and storage of data) and at the individual request of a recipient of services.
also referred to as a " <i>web service</i> " in this Privacy Statement.	
<i>personal data</i>	is any information relating to an identified or identifiable data subject. The term "identifiable" refers to those who can be identified directly or indirectly, especially by assignment to an

identifier or to one or more special characteristics.

processing

means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

processors

are other entities which process personal data on our behalf.

profiling

is any form of automated processing of your personal data evaluating personal aspects, in particular to analyse or predict aspects concerning your personal preferences or interests, reliability or behaviour, location or movements.

pseudonymisation

means the processing of personal data in such a manner that it can no longer be attributed to a specific data subject without the use of additional information, whereby this additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

recipients

are other entities to which we may disclose personal data, irrespective of whether they are third parties.

restriction of processing

is the restriction of processing of stored personal data such that they are only processed with your consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest and that you are informed before this restriction is lifted.

special categories of personal data

include, in accordance with Article 9 of the GDPR, data revealing racial and ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

third party

is anyone who is not a data subject, a controller or a processor;

unsafe third country

is any country outside the European Economic Area for which the Commission has not decided that it offers an adequate level of data protection.

3. General Information on the Legal Basis for Processing

Unless you have expressly consented to any processing (Art. 6 no. 1 lit. a) of the GDPR), we will only process your personal data if this is necessary for the performance of a contract with you or in order to take steps prior to entering into a contract at your request (Art. 6 no. 1 lit. b) of the GDPR) or for the fulfilment of a legal obligation (Art. 6 no. 1 lit. c) of the GDPR) or where this is necessary for the purposes of our legitimate interests (except where such interests are overridden by

your interests or fundamental rights and freedoms which require protection of personal data) (Art. 6 no. 1 lit. f) of the GDPR) or if any other legal basis or authorisation under Art. 6 of the GDPR exists. We will provide further details to you below on the specific legal basis for processing in each individual case and, where we pursue legitimate interests, also on those interests.

4. Processing in the Context of our Telephone Hotline

4.1. In this Section we will inform you about how we process and use personal data in relation to you that we collect in connection with calls to our telephone hotline and on the specific rights you have in this respect.

4.2. When you call our hotline, our representative will record your name, the date and time of your call and the content of your request in a call log. If you are registered with us in the customer database, this information will be stored in your customer account and the information in Section 6 will then apply. If you express interest in a product or service and there is no customer relationship, this information will be stored in our database of prospective customers and the information in Section 5 will then apply. In all other cases we will record your details in a separate database with call logs.

We will store and process the above information to perform the contractual relationship with you with respect to the delivery or service to which the call relates on the one hand (legal basis for processing: Art. 6 no. 1 lit. b) of the GDPR), and on the other hand, to protect our legitimate interest in improving our deliveries and services to meet your individual requirements and thus promoting the sale of our products and services, possibly offering you additional products or services in line with your interests, documenting the content of your request for the establishment, exercise or defence of legal claims and, where relevant, fulfilling our product monitoring obligations with respect to our products and services (legal basis for processing: Art. 6 no. 1 lit. f) of the GDPR).

Unless one of the longer retention periods specified further below applies, call logs will be retained for six months after the call.

4.3. We record individual calls to ensure service quality. We will obtain your consent for this in advance. We will use these records on the one hand on the basis of your consent, and, on the other hand, to protect our legitimate interest in improving our services (legal basis for processing: Art. 6 no. 1 lit. f) of the GDPR). The records will be evaluated within one month after the call by managers or trainers, and discussed with the hotline employee in order to continuously improve their customer friendliness and performance. The recordings will be deleted at the end of this period.

4.4. We share data with other companies of our group of undertakings. For further information on this and on the safeguards we have put in place in this respect, please refer to Sec. 10 below.

5. Processing in the Context of our Database of Prospective Customers

5.1. In this Section we will inform you about how we process and use the personal data

in relation to you that we collect when you express an interest in our products or services and on the specific rights you have in this respect.

- 5.2. If you express your interest in our products or services by making an enquiry (e.g. at a trade fair or conference, by e-mail, or via the contact form), we will store your contact data and the subject of your interest in a separate database for prospective customers.
- 5.3. We will store and process this data in order to process your inquiry and also to protect our legitimate interest in improving our deliveries and services to meet your individual requirements, promoting the sale of our products and services and possibly offering you additional products or services in line with your interests (legal basis for processing: Art. 6 no. 1 lit. f) of the GDPR).
- 5.4. We may process data on prospective customers in the context of "know your customer", anti-corruption, anti-money laundering, anti-terror and export control or similar screenings or audits in order to perform our compliance obligations and give effect to our compliance policies. The legal basis for such audits and screenings is the fulfilment of a legal obligation, where they are legally required (legal basis for processing: Art. 6 no. 1 lit. c) of the GDPR), and otherwise our legitimate interest in avoiding business relationships which we consider to violate our ethical standards (legal basis for processing: Art. 6 no. 1 lit. f) of the GDPR).
- 5.5. If a customer relationship is established, the data will be transferred to our customer database (cf. Section 6). If no customer relationship is established, the data will be deleted 2 years after the last correspondence with you.
- 5.6. We share data with other companies of our group of undertakings. For further information on this and on the safeguards we have put in place in this respect, please refer to Sec. 10 below.
- 5.7. You can object to the use of your data for direct marketing purposes at any time (cf. Section 13.7).

6. Processing in the Context of our Customer Database

- 6.1. In this Section we will inform you about how we process and use personal data in relation to you that we store in our customer database and on the specific rights you have in this respect.
- 6.2. We will set up a customer account in our customer database if a customer relationship exists or is established with you. The customer account contains your master data (name, address, account etc.). All correspondence and documents (correspondence, orders, contracts, complaints, etc.) within the scope of the customer relationship will then be stored in, or linked to, this customer account.
- 6.3. We will store and process the above information on the one hand to perform the respective contractual relationship with respect to the products and services we deliver to you (legal basis for processing: Art. 6 no. 1 lit. b) of the GDPR), and on the one hand, and, on the other hand, to protect our legitimate interest in improving our deliveries and services according to your individual requirements and thus promoting the sale of our products and services, and possibly offering you additional products or services in accordance with your interests, documenting contractual

agreements and correspondence for establishing, exercising or defending related legal claims, and, where relevant, fulfilling our product monitoring obligation with respect to our products and services (legal basis for processing: Art. 6 no. 1 lit. f) of the GDPR) as well as fulfilling statutory documentation and document retention obligations (legal basis for processing: Art. 6 no. 1 lit. c) of the GDPR).

- 6.4. When establishing the customer relationship, or at any time during the customer relationship, we may process customer data in the context of “know your customer”, anti-corruption, anti-money laundering, anti-terror and export control or similar screenings or audits in order to perform our compliance obligations and give effect to our compliance policies. The legal basis for such audits and screenings is the fulfilment of a legal obligation, where they are legally required (legal basis for processing: Art. 6 no. 1 lit. c) of the GDPR), and otherwise our legitimate interest in avoiding business relationships which we consider to violate our ethical standards (legal basis for processing: Art. 6 no. 1 lit. f) of the GDPR).
- 6.5. We share data with other companies of our group of undertakings. For further information on this and on the safeguards we have put in place in this respect, please refer to Sec. 10 below.
- 6.6. We also refer to Sections 11 et seq. for further information regarding the possible recipients and retention periods of the above information.

7. Processing of Prospective Supplier Data and Supplier Data

- 7.1. In this Section we will inform you about how we process and use personal data in relation to prospective and actual suppliers. In this context we use the term “supplier” cover not only the suppliers of products but any business partner who is not a customer or employee, including also service providers, consultants and freelancers.
- 7.2. We generally store and process data in relation to prospective and actual suppliers in the same manner and in the same databases as data on prospective and actual suppliers. Therefore all information on prospective customer data and customer data in this Privacy Statement also apply to data in relation to prospective and actual suppliers.
- 7.3. We will store and process data in relation to prospective and actual suppliers and all correspondence and documents (correspondence, orders, contracts, complaints, etc.) within the scope of the business relationship to perform the respective contractual relationship with you with respect to your products and services on the one hand (legal basis for processing: Art. 6 no. 1 lit. b) of the GDPR), and, on the other hand, to protect our legitimate interest in documenting contractual agreements and correspondence for establishing, exercising or defending related legal claims, and, where relevant, fulfilling our product monitoring obligation with respect to your products and services (legal basis for processing: Art. 6 no. 1 lit. f) of the GDPR) as well as fulfilling statutory documentation and document retention obligations (legal basis for processing: Art. 6 no. 1 lit. c) of the GDPR).
- 7.4. When establishing the business relationship or at any time during the business relationship, we may process data in relation to prospective and actual suppliers in the context of “know your customer”, anti-corruption, anti-money laundering, anti-

terror and export control or similar screenings or audits in order to perform our compliance obligations and give effect to our compliance policies. The legal basis for such audits and screenings is the fulfilment of a legal obligation, where they are legally required (legal basis for processing: Art. 6 no. 1 lit. c) of the GDPR), and otherwise our legitimate interest in avoiding business relationships which we consider to violate our ethical standards (legal basis for processing: Art. 6 no. 1 lit. f) of the GDPR).

7.5. We share data with other companies of our group of undertakings. For further information on this and on the safeguards we have put in place in this respect, please refer to Sec. 10 below.

7.6. We also refer to Sections 11 et seq. for further information regarding the possible recipients and retention periods of the above information.

8. Processing in the Context of Visits to our Facilities, CCTV Surveillance

8.1. In this Section we will inform you about how we process and use personal data in relation to you that we collect in connection with your visits to our facilities and on the specific rights you have in this respect.

8.2. When you visit our facility, we ask you to register. Typically your name and company and the date and time of visit will be recorded and you may be asked to sign a confidentiality undertaking.

8.3. We will store and process the above information to protect our legitimate interest in preventing abusive behaviour during visits and in establishing, exercising or defending possible legal claims (legal basis for processing: Art. 6 no. 1 lit. f) of the GDPR). Unless one of the longer retention periods set forth below applies, the information will be retained for one year after the visit. If you are a customer, they may be stored in your customer account and retained for the longer periods described in Sec. 12.

8.4. Sensitive areas of our facilities may be subject to closed circuit TV (CCTV) surveillance. CCTV cameras will be placed visibly and clearly marked. CCTV Cameras may be linked to live monitors without further recording but may also involve recording of videos. Recordings may be reviewed by security staff either on a random sample basis or where there is an indication of unauthorized access or abusive behaviour. After 72 hours recordings will be deleted unless required for investigation of a specific incident. We will store and process information collected through CCTV surveillance to protect our legitimate interest in preventing unauthorized access and abusive behaviour during visits and in establishing, exercising or defending possible legal claims (legal basis for processing: Art. 6 no. 1 lit. f) of the GDPR). Information collected through CCTV surveillance will not be used for any other purpose.

9. Processing of Applicant Data

9.1. In this Section we will inform you how we process and use personal data in relation to you that we collect in connection with applications for employment with our company or other entities within our group of undertakings and on the specific rights

you have in this respect.

9.2. Data Collection, Legal Basis and Purposes

- 9.2.1. If you send us your application documents via the general contact form or by e-mail, you should be aware that such transmission is not effectively protected against unauthorised access. We will therefore never ask you to send us your application documents exclusively in this way. We recommend that you submit your application documents only by post or via the secure connection we have provided for this purpose.
- 9.2.2. If you register with us as an applicant and send us application documents in printed or electronic form, we will store and process your contact data, your application documents (in printed or electronic form) and all documents and records concerning you which are created in the course of the application process (all these data and documents will be collectively referred to subsequently as "**applicant data**") for the duration of the application procedure, and for the purpose of performing the application procedure (legal basis for processing: Art. 6 no. 1 lit. b) of the GDPR).
- 9.2.3. We do not normally require special categories of personal data for the application process. We kindly ask you not to include such data in your application documents. Where such data are relevant in exceptional circumstances, we will process them together with other applicant data. This may include information on job restrictions based on pregnancy or health issues or information on disabilities in view of our special legal obligations vis-à-vis the disabled. In these cases we process your data for carrying out obligations and exercising specific rights in the field of employment and social security and social protection law (legal basis for processing: Art. 9(2)(b) of the GDPR) and/or for the assessment of your working capacity (legal basis for processing: Art. 9(2)(h) of the GDPR).
- 9.2.4. We may also process applicant data in the context of anti-corruption, anti-money laundering, anti-terror and export control or similar screenings or audits in order to perform our compliance obligations and give effect to our compliance policies. The legal basis for such audits and screenings is the fulfilment of a legal obligation, where they are legally required (legal basis for processing: Art. 6 no. 1 lit. c) of the GDPR), and otherwise our legitimate interest in avoiding employment of persons we consider to violate our ethical standards (legal basis for processing: Art. 6 no. 1 lit. f) of the GDPR).
- 9.2.5. Where during the application process you provide information or documents which are not strictly necessary for the application process, we process such information or documents within the scope of your consent (legal basis for processing: Art. 6 no. 1 lit. a) of the GDPR).
- 9.2.6. You can find out how we also store and use your applicant data, e.g. book keeping information where you are indemnified for out-of-pocket expenses, in Section 9.6.

9.3. Recipients and Categories of Recipients

9.3.1. If the advertised position is with another entity in our group of undertakings or otherwise is group-related, e.g. if the position reports to an employee of another entity within the group of undertakings (so-called matrix structure), we may also make the applicant data accessible to those employees of other companies in the group of undertakings who participate in the recruitment process. This serves the purposes specified in Section 9.2 and also to protect our legitimate interest in an exchange of information within the group of undertakings as required for the execution of the application procedure (legal basis for processing: Art. 6 no. 1 lit. f) of the GDPR).

9.4. EOS Talent Pool

9.4.1. Even if your particular profile does not fit a position we are looking to fill, we value your talent and interest in our business. We have therefore created a “talent pool” in which we continue to store application data of applicants whose application was not successful after the conclusion of the application process. When we seek to fill vacant positions in future, we access and use the application data stored in the talent pool in order to determine whether a past applicant’s profile would fit the position, and, if so, contact the applicant to inquire whether it would be interested in applying for the position.

9.4.2. Applicant data in the talent pool is accessible to all companies in our group of undertakings in order to identify applicants which may fit for a position they are seeking to fill. Such companies may be located in an unsafe third country. For further information on the safeguards we have put in place in this respect, please refer to Sec. 10 below.

9.4.3. Applicant data is entered into the talent pool only with the express consent of the applicant which we will seek during the application process. The legal basis for all processing and use is Art. 6 no. 1 lit. a) of the GDPR.

9.4.4. We delete applicant data in the talent pool after expiry of 24 months from the last communication with the applicant.

9.5. Transfers to Unsafe Third Countries and Guarantees

9.5.1. Normally, the recipients of applicant data in accordance with Section 9.3 will not be located in an unsafe third country. If, exceptionally, this is the case, we will agree appropriate guarantees with the recipient to ensure an adequate level of data protection for the application procedure.

9.5.2. For further information on the safeguards we have put in place in the event that information must be shared with another company of our group of undertakings located in an unsafe third country, please refer to Sec. 10 below.

9.6. Retention Periods and Deletion

- 9.6.1. If the application is successful, the applicant data will continue to be stored and used as part of your personnel file in order to perform the employment contract (legal basis for processing: Art. 6 no. 1 lit. b) of the GDPR).
- 9.6.2. If the application process is not successful, we will return printed application documents to you and will retain copies of them and all other applicant data for another three months after completion of the application process and will then delete or anonymise them. The storage of these data and documents serves to protect our legitimate interest in establishing, exercising or defending legal claims in connection with the application procedure, particularly if we need them as evidence in our defence against the assertion of discrimination in the selection process (legal basis for processing: Art. 6 no. 1 lit. f) of the GDPR).

10. Data Transfers within the EOS Group of Undertakings

In this Section we will provide further details how we may share personal data about you with other companies within our group of undertakings, and how such other companies may process and use such data.

10.1. Data Transfers, Legal Basis and Purposes

Personal data controlled by one company within our group of undertakings (herein also referred to as “EOS Affiliate”) may be disclosed to other EOS Affiliates where such data is uploaded to a joint database.

Joint databases are centrally hosted by one EOS Affiliate for access by all EOS Affiliates for the purposes identified below. However, access to data in joint databases is always restricted by multiple levels of access rights granted on a need-to-know basis ensuring that the EOS Affiliates, and within each EOS Affiliate the respective employees, access only the data they require for their business functions.

Within our group of undertakings we currently have the following joint databases:

Database	Data	Purposes
Central ERP database	Customer Database (See Sec. 6 above)	Enterprise resource planning and financial management, purposes identified in Sec. 6 above.
Central file server	meeting protocols, correspondence, any other documents or files	document and file depository and management
Central Exchange server and database	mail addresses, communications	contacts. Mail service for business correspondence to all business contacts, global address book and calendar function
Central CRM system and Database	Database of Prospective Customers (See Sec. 5 above)	Purposes identified in Sec. 5 above, resource planning and financial management
Sharepoint	address list and photos of all employees event photos and announcements of personal anniversaries	sharing of document templates, organizational structure information, technical documentation, business related issues like news, announcements, shared workspace and information platform

My site - personal job, related data

Central HR database Applicant data (See Sec. 9 Purposes identified in Sec. 9 above above) including Talent Pool

All databases and systems are located in Krailling, Germany and operated by EOS GmbH Electro Optical Systems.

Personal data controlled by one EOS Affiliate may in addition also be disclosed to other EOS Affiliates where one EOS Affiliate provides intragroup services to the other EOS Affiliate. Currently EOS GmbH Electro Optical Systems, Krailling, Germany provides central IT services to all other EOS Affiliates and in the context of such services may have access to all data stored on the respective EOS Affiliate's systems. EOS GmbH Electro Optical Systems, Krailling, Germany, has, however, undertaken to access such data as a processor and only for the purposes and subject to the instructions of the respective EOS Affiliate.

We share data in the contexts specified hereinabove in order to protect our legitimate interests in coordinating sales processes and business and IT administrative processes on the level of the group of companies and planning and providing our deliveries and services as close to our customers as possible (legal basis for processing: Art. 6 no. 1 lit. f) of the GDPR).

We will assume that your interests do not conflict with this, because the safeguards described below are taken in order to provide a uniform level of data protection.

10.2. *Recipients and Categories of Recipients, Transfers to Unsafe Third Countries and Guarantees*

The disclosures set forth above may be made EOS Affiliates within and outside of the European Economic Area. In order to provide for a uniform level of data protection throughout our group of companies and also to provide sufficient guarantees in this case, all EOS Affiliates have agreed on the application of uniform data protection provisions for all data transfers within our group of companies which, with respect to data exports outside of the European Economic Area, incorporate the standard data protection clauses adopted by the Commission for this purpose.

11. *General Information on Recipients, Categories of Recipients and Transfers*

- 11.1. Our data protection officer will have access to your data as necessary for the consummation of its data protection tasks. The data protection officer is under a statutory obligation of confidentiality.
- 11.2. All of our servers and databases may be operated, maintained or further developed by additional processors or other contractors. They may have access to your data.
- 11.3. We may use third party service providers for the archiving and/or destruction of documents. They will have access to your data.
- 11.4. Where we store and process data for the consummation of contracts, we may pass these data on to agents and contractors we employ for such consummation (e.g. to carriers for transportation purposes).

- 11.5. Where we store and process data for communication with you, we may use additional processors or contractors in order to process or transmit correspondence with you (e.g. letter shops), who will then have access to your data.
- 11.6. We may also retain consultants or advisors such as legal, tax or business consultants. They may have access to your data.
- 11.7. Where we use contractors of the categories listed hereinabove to handle your data on our behalf, we have concluded, or will conclude prior to such processing, a contract processing agreement with the contractor to ensure that personal data is processed only on our behalf and in accordance with our instructions. Where the data are not processed on our behalf, we will enter into appropriate confidentiality agreements with the contractors.
- 11.8. We will transfer your personal data to competent law enforcement, regulatory or other authorities, institutions or bodies if we are legally obligated to do so (legal basis for processing: Art. 6 no. 1 lit. c) of the GDPR) or if we have a legitimate interest in averting coercive measures of such authorities, institutions or bodies within the scope of their legal authority (legal basis for processing: Art. 6 no. 1 lit. f) of the GDPR). Such legally required or necessary transmissions are not the subject of this Privacy Statement.

12. General Information on Retention Periods and Anonymisation

- 12.1. We have enacted a data retention and deletion policy in order to ensure that personal data are only stored for as long as necessary for their purpose.
- 12.2. Our data retention and deletion policy takes account of the principle that personal data should be retained for limited periods even after the original purpose has become obsolete, in order to preserve our legitimate interest in preventing unintentional deletions, in enabling the establishment, exercise or defence of legal claims and in rendering the administration of retention and deletion periods practicable (legal basis for processing: Art. 6 no. 1 lit. f) of the GDPR). We assume that your interests do not conflict with this, because these additional retention periods are appropriate with respect to the interests to be protected.
- 12.3. Unless detailed information on deletion periods has already been provided above, the following general deletion periods will apply in accordance with our data retention and deletion policy. Where data fall under several different deletion periods, the longest will always apply:
 - 12.3.1. We will retain customer data for the duration of the customer relationship. After the end of the customer relationship such data will continue to be retained for as long as these data are necessary for the maintenance of the customer account and for the administration of documents or data relating to the customer which fall into any of the categories identified hereinbelow. Otherwise customer data will be deleted after expiry of one year.
 - 12.3.2. For compliance with the statutory retention period for commercial letters and tax documents we will retain correspondence for seven years and invoices and other booking documentation for 11 years.
 - 12.3.3. We will retain contract-related data and documents for 11 years after the

end of the contractual relationship in view of the statutory limitation period for claims and statutory document retention obligations for booking receipts.

- 12.3.4. We will retain all product safety documents and product data including information on safety-relevant incidents and accidents or customer complaints to comply with our statutory product monitoring obligation and to assert, exercise or defend legal claims within the statutory limitation periods for 31 years after the end of product sales.
- 12.4. If the term "deletion" is mentioned in this Privacy Statement, we reserve the right to anonymise the relevant data record, such that it can no longer be assigned to you, instead of complete deletion
- 12.5. Anonymised data may be processed and used by us and our processors for an unlimited period. The processing and use of anonymised data is not subject to the GDPR and is not the subject of this Privacy Statement.

13. Your Rights

You as the data subject have certain rights with regard to your personal data, which we will explain to you below:

- 13.1. **Right of Access and Information (Art. 15 of the GDPR)** - You have the right, where the statutory requirements are met, to request from us at any time, at no cost, confirmation as to whether personal data relating to you is being processed, a copy of this data and comprehensive information on this personal data. This right extends in particular, without limitation, to the purposes of processing, the categories of personal data being processed, the recipients, the storage period and the origin of the data.
- 13.2. **Right to Rectification (Art. 16 of the GDPR)** - You have the right to request us to rectify incorrect and incomplete personal data concerning you without delay, where the statutory requirements are met.
- 13.3. **Right to be Forgotten (Art. 17 of the GDPR)** - You have the right to demand from us the immediate deletion of personal data concerning you, where the statutory requirements are met, if, among other reasons, their storage is no longer necessary or unlawful, if you revoke your consent on which their storage was based, if you have validly objected to their storage in accordance with Sections 13.6 et seq., if we are obligated to delete them for any other reason or if the data were collected as part of a web service. If we have made the data public, in addition to deletion of the data, we must also inform other controllers in such cases that you have requested the deletion of this data and all references thereto, insofar as this is reasonable in view of the available technology and the implementation costs. The above obligation does not apply in certain exceptional cases, in particular storage for the purpose of establishing, exercising or defending legal claims.
- 13.4. **Right to Restriction of Processing (Art. 18 of the GDPR)** - You have the right to request us, where the statutory requirements are met, to restrict the processing of personal data relating to you, for example if you dispute their accuracy, the storage

is no longer necessary or is unlawful and you still do not wish to have it deleted or if you have filed an objection to the processing (Sections 13.6 et seq.) as long as it has not yet been established whether our legitimate reasons outweigh yours.

- 13.5. **Right to Data Portability (Art. 20 of the GDPR)** - If automated processing of personal data occurs solely on the basis of your consent or to fulfil a contract with you or to implement pre-contractual measures, you have the right to require us, subject to statutory requirements, to make available the personal data in relation to yourself that you have provided to you or to a third party you designate, if this is technically feasible, in a structured, current and machine-readable format and not to impede its transfer to a third party.
- 13.6. **Right of Objection (Art. 21(1) of the GDPR)** - You have the right to require us, where the statutory requirements are met, to no longer process personal data relating to you which we process for the performance of a task which is in the public interest or for the protection of our legitimate interests or those of a third party, if you object to such processing for reasons which arise from your particular situation. In this case we must desist from further processing unless there are compelling grounds for processing which outweigh your interests or the processing is carried out for the establishment, exercise or defence of legal claims.
- 13.7. **Right of Objection to Direct Marketing (Art. 21(2) of the GDPR)** - You can object to the further processing of your personal data for direct marketing purposes at any time, and we will consequently refrain from processing them for this purpose. This also applies to profiling insofar as it is associated with such direct marketing.
- 13.8. **Automated Decisions (Art. 22 of the GDPR)** - We will not make any decisions without your consent which produce legal effects concerning you or similarly significantly affect you and that are based exclusively on automated processing (including profiling).
- 13.9. **Guarantees** - To the extent that we indicate in this Privacy Policy that guarantees have been agreed to provide an adequate level of protection, you may request copies of the relevant documents from our Data Protection Officer. If a guarantee exists in the form of participation in the Privacy Shield Program, you will find information and documentation here: [http://europa.eu/rapid/press-release MEMO-16-434 en.htm](http://europa.eu/rapid/press-release_MEMO-16-434_en.htm)..
- 13.10. **Consents** - If you consent to processing, this is voluntary, unless we inform you otherwise in advance, and the refusal of consent will not be sanctioned. You can withdraw your consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Processing on a legal basis other than your consent will also be unaffected by such withdrawal. However, you may also exercise the above statutory rights in this respect (e.g. the right of objection pursuant to Sections 13.6 et seq.). In particular, you may withdraw any consent to the use of your e-mail address or telephone number for direct marketing at any time and may object to any further use of your e-mail address or telephone number for this purpose at any time, free of charge (other than communication costs payable to your provider).
- 13.11. **Right to Lodge a Complaint** - You have the right to lodge a complaint with a supervisory authority. This may include, among others, the supervisory authority responsible for your place of residence or the supervisory authority generally responsible for us (Section 1.3).

13.12. **Contact** - You can contact us in any form to exercise your rights, in particular to withdraw any consent you may have given, and especially our data protection officer also. You may be required to identify yourself to us as a data subject to exercise your rights.

14. Security

We have implemented extensive, industry standard technical and organisational measures to protect your personal data from unauthorised access and misuse.

15. Changes to this Privacy Statement

In the event of future changes to this Privacy Statement, you can retrieve old versions and information on the periods for which they were valid [here](#).

Electro Optical Systems Nordic AB

Rev. May 2018