



Boatlabs AS

## DATA RETENTION POLICY



---

**BOATLABS AS**

Sjøgata 55, N-6065 Ulsteinvik, Norway  
Notenesgata 12, N-6002 Ålesund, Norway  
Phone +47 483 20 888 – Email: [post@boatlabs.no](mailto:post@boatlabs.no)  
Enterprise no. NO 991 807 950 VAT – [www.boatlabs.no](http://www.boatlabs.no)

## Table of contents

<b>1.</b>	<b>PURPOSE, SCOPE AND USERS</b> .....	<b>3</b>
<b>2.</b>	<b>REFERENCE DOCUMENTS</b> .....	<b>3</b>
<b>3.</b>	<b>RETENTION RULES</b> .....	<b>3</b>
3.1.	RETENTION GENERAL PRINCIPLE .....	3
3.2.	RETENTION GENERAL SCHEDULE .....	4
3.3.	SAFEGUARDING OF DATA DURING RETENTION PERIOD .....	4
3.4.	DESTRUCTION OF DATA.....	4
3.5.	ROUTINE DISPOSAL SCHEDULE.....	5
<b>4.</b>	<b>VALIDITY AND DOCUMENT MANAGEMENT</b> .....	<b>5</b>
<b>5.</b>	<b>APPENDICES</b> .....	<b>5</b>



## 1. Purpose, Scope and Users

This policy sets the required retention periods for specified categories of personal data and sets out the minimum standards to be applied when destroying certain information within Boatlabs AS (further: the “Company”).

This Policy applies to all business units, processes and systems in all countries in which the Company conducts business and has dealings or other business relationships with third parties.

This Policy applies to all Company officers, directors, employees, agents, affiliates, contractors, consultants, advisors or service providers that may collect, process, or have access to data (including personal data and / or sensitive personal data). It is the responsibility of all of the above to familiarise themselves with this Policy and ensure adequate compliance with it.

This policy applies to all information used at the Company but not limited to. Examples of documents include:

- Emails
- Hard copy documents
- Soft copy documents
- Video and audio
- Data generated by physical access control systems

## 2. Reference Documents

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- The Norwegian law; Lov om behandling av personopplysninger (personopplysningsloven)
- Personal Data Protection Policy
- Disposal and Destruction Policy

## 3. Retention Rules

### 3.1. Retention General Principle

In the event, for any category of documents not specifically defined elsewhere in this Policy and unless otherwise mandated differently by applicable law, the required retention period for such document will be deemed to be 3 years from the date of creation of the document.

***General rule for Boatlabs AS is that data to a customer might be deleted once the product is delivered and verification of work task is completed and accepted by the customer.***



### 3.2. Retention General Schedule

Data Protection Officer defines the time period for which the documents and electronic records should to be retained through the Data Retention Schedule.

As an exemption, retention periods within Data Retention Schedule can be prolonged in cases such as:

- Ongoing investigations from Member States authorities, if there is a chance records of personal data are needed by the Company to prove compliance with any legal requirements; or
- When exercising legal rights in cases of law suits or similar court proceeding recognized under local law.

### 3.3. Safeguarding of Data during Retention Period

The possibility that data media used for archiving will wear out shall be considered. If electronic storage media are chosen, any procedures and systems ensuring that the information can be accessed during the retention period (both with respect to the information carrier and the readability of formats) shall also be stored in order to safeguard the information against loss as a result of future technological changes. The responsibility for the storage falls to IT Manager.

### 3.4. Destruction of Data

The data will be destroyed according to the Disposal and Destruction Policy. Breach, Enforcement and Compliance

The person appointed with responsibility for Data Protection ([Job title]) has the responsibility to ensure that each of the Company's offices complies with this Policy. It is also the responsibility of the IT Manager to assist any local office with enquiries from any local data protection or governmental authority.

Any suspicion of a breach of this Policy must be reported immediately to IT Manager. All instances of suspected breaches of the Policy shall be investigated and action taken as appropriate.

Failure to comply with this Policy may result in adverse consequences, including, but not limited to, loss of customer confidence, litigation and loss of competitive advantage, financial loss and damage to the Company's reputation, personal injury, harm or loss. Non-compliance with this Policy by permanent, temporary or contract employees, or any third parties, who have been granted access to Company premises or information, may therefore result in disciplinary proceedings or termination of their employment or contract. Such non-compliance may also lead to legal action against the parties involved in such activities.



### 3.5. Routine Disposal Schedule

Records which may be routinely destroyed unless subject to an on-going legal or regulatory inquiry are as follows:

- Announcements and notices of day-to-day meetings and other events including acceptances and apologies;
- Requests for ordinary information such as travel directions;
- Reservations for internal meetings without charges / external costs;
- Transmission documents such as letters, fax cover sheets, e-mail messages, routing slips, compliments slips and similar items that accompany documents but do not add any value;
- Message slips;
- Superseded address list, distribution lists etc.;
- Duplicate documents such as CC and FYI copies, unaltered drafts, snapshot printouts or extracts from databases and day files;
- Stock in-house publications which are obsolete or superseded; and
- Trade magazines, vendor catalogues, flyers and newsletters from vendors or other external organizations.

In all cases, disposal is subject to any disclosure requirements which may exist in the context of litigation.

## 4. Validity and document management

This document is valid as of 2018-06-25.

The owner of this document is IT Manager who must check and, if necessary, update the document at least once a year.

## 5. Appendices

- Appendix - Data Retention Schedule

