Stonewall

ABOUT THIS RESOURCE

This resource is produced by Stonewall, a UK-based charity that stands for the freedom, equity and potential of all lesbian, gay, bi, trans, queer, questioning and ace (LGBTQ+) people.

At Stonewall, we imagine a world where LGBTQ+ people everywhere can live our lives to the full.

Founded in London in 1989, we now work in each nation of the UK and have established partnerships across the globe. Over the last three decades, we have created transformative change in the lives of LGBTQ+ people in the UK, helping win equal rights around marriage, having children and inclusive education.

Our campaigns drive positive change for our communities, and our sustained change and empowerment programmes ensure that LGBTQ+ people can thrive throughout our lives. We make sure that the world hears and learns from our communities, and our work is grounded in evidence and expertise.

To find out more about our work, visit us at www.stonewall.org.uk

Registered Charity No 1101255 (England and Wales) and SC039681 (Scotland)

DATA RETENTION POLICY

JULY 2020

Contents

Stonewall
192 St John Street,
London, EC1V 4JY

Switchboard: 020 7593 1850
Info Line: 0800 050 2020
Email: info@stonewall.org.uk

Website: stonewall.org.uk
Facebook: stonewalluk
Twitter: @stonewalluk

1 Purpose, Scope and Users

In order to ensure that personal data held by Stonewall is not kept for longer than necessary, the below Data Retention Policy outlines how Stonewall will meet the requirements of the current legislation and follow best practice in this area.

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 Stonewall.

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

This Policy applies to all Stonewall's trustees, 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 organisation. 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).
- Personal Data Protection 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 in particular within the Data Retention Schedule) 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.

Stonewall
192 St John Street,
London, EC1V 4JY

Switchboard: 020 7593 1850
Info Line: 0800 050 2020
Email: info@stonewall.org.uk

Website: stonewall.org.uk
Facebook: stonewalluk
Twitter: @stonewalluk

3.2 Retention General Schedule

The Data Protection Officer defines the time period for which the documents and electronic records should 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 legal cases 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 Data Protection Officer will be responsible for storage.

3.4 Destruction of Data

Stonewall and its employees should on a regular basis, review all data, whether held electronically on their device or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant. See Appendix for the retention schedule. Overall responsibility for the destruction of data falls to the Data Protection Officer.

Once the decision is made to dispose according to the Retention Schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality. The method of disposal varies and is dependent upon the nature of the document. For example, any documents that contain sensitive or confidential information (and particularly sensitive personal data) must be disposed of as confidential waste and be subject to secure electronic deletion; some expired or superseded contracts may only warrant in-house shredding. The Document Disposal Schedule section below defines the mode of disposal.

In this context, the employee shall perform the tasks and assume the responsibilities relevant for the information destruction in an appropriate way. The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the Data Protection Officer subcontracts for this purpose. Any applicable general provisions under relevant data protection laws and the organisation's Personal Data Protection Policy shall be complied with.

Appropriate controls shall be in place that prevent the permanent loss of essential information of the company as a result of malicious or unintentional destruction of information – these controls are described in the company's IT Security Policy.

Stonewall
192 St John Street,
London, EC1V 4JY

Switchboard: 020 7593 1850
Info Line: 0800 050 2020
Email: info@stonewall.org.uk

Website: stonewall.org.uk
Facebook: stonewalluk
Twitter: @stonewalluk

The Data Protection Officer shall fully document and approve the destruction process. The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed.

3.5 Breach, Enforcement and Compliance

The person appointed with responsibility for Data Protection, the Data Protection Officer has the responsibility to ensure that each of the Company's offices complies with this Policy. It is also the responsibility of the Data Protection Officer 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 Data Protection Officer. 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 Stonewall'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 Stonewall 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.

4 Document Disposal

4.1 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.

Stonewall
192 St John Street,
London, EC1V 4JY

Switchboard: 020 7593 1850
Info Line: 0800 050 2020
Email: info@stonewall.org.uk

Website: stonewall.org.uk
Facebook: stonewalluk
Twitter: @stonewalluk

4.2 Destruction Method

Level I documents are those that contain information that is of the highest security and confidentiality and those that include any personal data. These documents shall be disposed of as confidential waste (cross-cut shredded and incinerated) and shall be subject to secure electronic deletion. Disposal of the documents should include proof of destruction.

Level II documents are proprietary documents that contain confidential information such as parties' names, signatures and addresses, or which could be used by third parties to commit fraud, but which do not contain any personal data. The documents should be cross-cut shredded and then placed into locked rubbish bins for collection by an approved disposal firm, and electronic documents will be subject to secure electronic deletion.

Level III documents are those that do not contain any confidential information or personal data and are published Company documents. These should be strip-shredded or disposed of through a recycling company and include, among other things, advertisements, catalogues, flyers, and newsletters. These may be disposed of without an audit trail.

5 Managing Records Kept on the Basis of this Document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Data Retention Schedule	Data Protection Officer's One Drive	Data Protection Officer	Only authorised persons may access this document	Permanently

6 Validity and document management

This document is valid as of 13 July 2020.

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

7 Appendix

- Appendix – Data Retention Schedule.

Stonewall
192 St John Street,
London, EC1V 4JY

Switchboard: 020 7593 1850
Info Line: 0800 050 2020
Email: info@stonewall.org.uk

Website: stonewall.org.uk
Facebook: stonewalluk
Twitter: @stonewalluk