Data Retention Policy

Version 2 - Approved by Madhav Bhagat

Contents

1. Objective

Customers and users of SpotDraft may request the deletion of data that belongs to them from our systems. This policy outlines the provisions we provide for such requests and describes how such requests should be handled.

2. Scope

This policy is applicable to data that is in possession of SpotDraft and received from our customers or users. Data collected concerning SpotDraft products or services that are in testing, alpha/beta state, or an early access program are also part of the scope.

3. Policy Statement

Data retention is based on valid reasons, and customers can request the deletion of their information. Requests should be authenticated and evaluated for legitimacy. Deletion may be withheld if it disrupts services. Anonymization of personal data may be considered before deletion, except where prohibited.

4. Data Retention Guidelines

- All data is retained within our systems only when there is a continued and valid reason to store or process the data.
- Customers and users have the right to request the deletion of their information by making a request. This request must be made by the customer or user.
- If a data deletion request is received, please assess the authenticity of the request and decide the legitimacy of the request. For example, after a customer has canceled their contract with SpotDraft and requested to delete their data, we should oblige such a request. However, a data deletion request from a customer with an active contract with SpotDraft is likely invalid. Deletion of their data may lead to disruption of services.
- For deletion pertaining to personal data, do consider anonymization of the data before deleting it as long as it does not conflict with any local laws or customer contracts.
- If you have any questions regarding a data deletion request or any other questions regarding this policy, please contact the Information security officer before taking action.
- Versions of company policy documentation and older versions of company policy are maintained for at least six years.

5. Document Security Classification

Company Internal (please refer to the Data Classification policy for more details).

6. Non-Compliance

Compliance with this policy shall be verified through various methods, including but not limited to automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

7. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

8. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization.

End of Data Retention Policy. For version history, please see the next page.

Version history

Version	Log	Date
2 Current	Policy version approved by Madhav Bhagat	29 Jul, 2024
2	New Policy version Created	29 Jul, 2024
1	Policy version approved by Madhav Bhagat	02 Aug, 2022
1	New Policy version Created	02 Aug, 2022