



LEGAL · VERSION 1

Data Processing Agreement

How Frabs processes personal data on behalf of its customers.

VERSION

FRABS_DPA_V.1
OCTOBER 2026

APPLIES TO

Every customer, as part
of the Terms

GOVERNING LAW

England and Wales

CONTACT

frabs.net
info@frabs.net
support@frabs.net

Contents

1.	THIS DPA AND ITS DEFINITIONS	3
2.	ROLES AND SCOPE	3
3.	INSTRUCTIONS AND CUSTOMER RESPONSIBILITIES	4
4.	PERSONNEL	4
5.	SECURITY	4
6.	SUB-PROCESSORS	4
7.	DATA SUBJECT RIGHTS	5
8.	PERSONAL DATA BREACHES	5
9.	ASSISTANCE	5
10.	INTERNATIONAL TRANSFERS	5
11.	AUDIT AND INFORMATION	6
12.	RETURN AND DELETION	6
13.	LIABILITY	6
14.	TERM, CHANGES AND GOVERNING LAW	6
Annex 1	DETAILS OF THE PROCESSING	7
Annex 2	SECURITY MEASURES	7
Annex 3	SUB-PROCESSORS	8

About this DPA. This Data Processing Agreement forms part of the Agreement made under the Frabs Terms and Conditions. It applies automatically when a customer accepts the Terms. No separate signature is needed.

1. THIS DPA AND ITS DEFINITIONS

- 1.1 This Data Processing Agreement (the "DPA") is between Frabs, the business that operates frabs.net, and the Customer. It forms part of the Agreement made under the Frabs Terms and Conditions (the "Terms") and applies whenever Frabs processes Personal Data on the Customer's behalf in providing the Service.
- 1.2 Words that start with a capital letter and are not defined in this DPA have the meaning they have in the Terms.
- 1.3 In this DPA:
- | | |
|-------------------------------|--|
| Controller, Processor, | have the meanings given in Data Protection Law. |
| Data Subject, | |
| Personal Data, | |
| Personal Data Breach, | |
| Process and Processing | |
| Customer Personal Data | Personal Data that is part of the Customer Data and that Frabs Processes as Processor for the Customer. |
| ICO | the UK Information Commissioner's Office. |
| Restricted Transfer | a transfer of Customer Personal Data to a country or organisation outside the United Kingdom, or outside the European Economic Area where EU law applies, that is not covered by an adequacy decision or adequacy regulations under Data Protection Law. |
| Sub-processor | a third party that Frabs engages to Process Customer Personal Data. |
- 1.4 If this DPA and the Terms conflict about the Processing of Personal Data, this DPA prevails.

2. ROLES AND SCOPE

- 2.1 The Customer is the Controller of the Customer Personal Data. If the Customer is itself acting as a Processor for its End Customers, the Customer confirms that it is authorised to give Frabs the instructions in this DPA and to appoint Frabs as a Sub-processor, and Frabs acts as the Customer's Sub-processor.
- 2.2 Frabs is the Processor of the Customer Personal Data and will Process it only as set out in this DPA.
- 2.3 Annex 1 sets out the subject matter, duration, nature and purpose of the Processing, the types of Personal Data and the categories of Data Subjects.
- 2.4 Frabs is the Controller of the Personal Data that it holds in order to run Accounts, bill the Customer and keep the Service secure. That data is described in the Frabs Privacy Notice and is not covered by this DPA.
- 2.5 Each party must comply with Data Protection Law.

3. INSTRUCTIONS AND CUSTOMER RESPONSIBILITIES

- 3.1 Frabs will Process Customer Personal Data only on the Customer's documented instructions. These are the Terms, this DPA, the Customer's use of the Service and its settings, and the Documentation. Frabs may also Process it where the law requires, in which case Frabs will tell the Customer before it does so, unless the law prevents it.
- 3.2 Frabs will tell the Customer if, in its opinion, an instruction infringes Data Protection Law. Frabs is not required to check the Customer's instructions.
- 3.3 The Customer is responsible for:
- (a) having a lawful basis to give Frabs the Customer Personal Data and to have it Processed as set out in this DPA;
 - (b) giving its End Customers and others any notice that the law requires, including notice that their traffic is monitored;
 - (c) the accuracy of the information it gives to Frabs;
 - (d) not sending the content of its End Customers' communications, or special category data, to Frabs; and
 - (e) its decisions on Approvals, automation rules and Remediation Actions.

4. PERSONNEL

- 4.1 Frabs will make sure that every person who Processes Customer Personal Data on its behalf is bound by a duty of confidentiality and is allowed access only where it is necessary to provide the Service.

5. SECURITY

- 5.1 Frabs will use the technical and organisational measures in Annex 2 to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.
- 5.2 Frabs may update those measures from time to time, as long as the overall level of protection is not reduced.
- 5.3 The Customer is responsible for the security of its own systems, including the Nodes on which the Sensor runs and the sign-in details of its Authorised Users.

6. SUB-PROCESSORS

- 6.1 The Customer gives Frabs general authorisation to use the Sub-processors listed in Annex 3.
- 6.2 Frabs will give the Customer at least 30 days' notice before it adds or replaces a Sub-processor, by email to the owner of the Account and by updating the Frabs Sub-processors page.
- 6.3 The Customer may object on reasonable data protection grounds within those 30 days. Frabs will then work with the Customer to find a solution. If the objection cannot be resolved, the Customer may cancel its subscription under clause 21.2 of the Terms.

- 6.4 Frabs will bind each Sub-processor to terms that give similar protection to this DPA, and remains responsible to the Customer for the Sub-processor's work.
-

7. DATA SUBJECT RIGHTS

- 7.1 If a Data Subject asks Frabs to use a right under Data Protection Law in relation to Customer Personal Data, Frabs will, without undue delay, pass the request to the Customer and will not respond to it except to say that it has been passed on, unless the law requires otherwise.
- 7.2 Taking into account the nature of the Processing, Frabs will give the Customer reasonable help, through the features of the Panel and on request, so that the Customer can answer requests from Data Subjects.
-

8. PERSONAL DATA BREACHES

- 8.1 Frabs will tell the Customer without undue delay, and in any case within 48 hours, after becoming aware of a Personal Data Breach that affects Customer Personal Data.
- 8.2 The notice will say, as far as Frabs knows: what happened; the categories and approximate numbers of Data Subjects and records affected; the likely consequences; and the steps taken or proposed to deal with it and to reduce its effects. Frabs may give the information in stages as it becomes available.
- 8.3 Frabs will take reasonable steps to contain the breach and will help the Customer to meet its duties to tell the ICO and Data Subjects. The Customer decides whether and how to tell them, unless the law requires Frabs to do so.
-

9. ASSISTANCE

- 9.1 Taking into account the nature of the Processing and the information available to it, Frabs will give the Customer reasonable help with data protection impact assessments and with prior consultation of the ICO, where they relate to the Service.
-

10. INTERNATIONAL TRANSFERS

- 10.1 Frabs Processes Customer Personal Data in the United Kingdom and the European Economic Area. The servers are in Amsterdam, the Netherlands.
- 10.2 Under UK adequacy regulations, Personal Data may move from the United Kingdom to the European Economic Area.
- 10.3 Frabs will not make a Restricted Transfer unless an appropriate safeguard under Data Protection Law is in place, such as the UK International Data Transfer Agreement, the UK Addendum to the EU standard contractual clauses or the EU standard contractual clauses, and the Customer has been told through a notice under clause 6.2.

11. AUDIT AND INFORMATION

- 11.1 Frabs will give the Customer the information it reasonably needs to show that Frabs has met the obligations in this DPA. Frabs may do this by sending its Security overview, its Sub-processors page and written answers to the Customer's questions.
- 11.2 If that information is not enough, or if the law or a regulator requires it, the Customer may carry out an audit of Frabs's Processing of Customer Personal Data, as long as it:
- (a) gives Frabs at least 30 days' written notice;
 - (b) carries out the audit during business hours and in a way that does not disrupt the Service more than necessary;
 - (c) audits no more than once in any 12 months, unless there has been a Personal Data Breach or a regulator requires otherwise;
 - (d) keeps what it learns confidential under clause 17 of the Terms; and
 - (e) pays its own costs.

12. RETURN AND DELETION

- 12.1 The Customer can export its Incident records and audit log from the Panel at any time until the Agreement ends, and for 30 days after it, as set out in clause 21.6 of the Terms.
- 12.2 Frabs will delete the Customer Personal Data within 30 days after the end of that export period, as set out in clause 21.7 of the Terms, unless the law requires Frabs to keep some of it. Backup copies are deleted as the backups are replaced.
- 12.3 Frabs will confirm in writing that the Customer Personal Data has been deleted if the Customer asks.

13. LIABILITY

- 13.1 Each party's liability under this DPA is subject to the limits and exclusions in clause 20 of the Terms, and counts towards the limit in clause 20.3 of the Terms.
- 13.2 Nothing in this DPA limits a liability that cannot be limited by law, or the rights that Data Subjects have under Data Protection Law.

14. TERM, CHANGES AND GOVERNING LAW

- 14.1 This DPA starts when the Agreement starts and continues for as long as Frabs Processes Customer Personal Data.
- 14.2 Frabs may update this DPA to reflect a change in Data Protection Law or in the Service, by giving at least 30 days' notice in line with clause 22 of the Terms.
- 14.3 This DPA, and any dispute or claim that arises from it, is governed by the law of England and Wales, and the courts of England and Wales have exclusive jurisdiction, as set out in clause 24.10 of the Terms.

ANNEX 1

DETAILS OF THE PROCESSING

Item	Details
Subject matter	Providing the Service to the Customer
Duration	The Subscription Term and the Trial Period, plus the export and deletion periods in clause 12
Nature of the Processing	Collecting, storing, analysing, attributing, displaying and deleting Detection Data and related Customer Data
Purpose	To detect, attribute, investigate and help to remediate outbound abuse from the Customer's network, and to keep a record of it
Types of Personal Data	Network addresses (such as the IP addresses of virtual servers and of their destinations), ports, protocols, timings and traffic volumes, identifiers for virtual servers and End Customers that the Customer provides, and the contact details of Authorised Users
Categories of Data Subjects	End Customers and their users, people who communicate with End Customers' servers, and the Customer's Authorised Users
Special category data	Not intended. The Customer must not send it to the Service
Content of communications	Not collected. The Sensor analyses flow metadata and abuse indicators, not the content of traffic

ANNEX 2

SECURITY MEASURES

Area	Measures
Access to the Panel	Multi-factor authentication for every user. Roles of owner, admin, analyst and read-only limit what each person can do
Access by Frabs	Operators sign in with passkeys. Administrative access to servers is only through one management server, reached over an encrypted private tunnel. Views of a customer's Account by staff are read-only, need a recorded reason, are limited in time and are shown in the customer's audit log
Separation	Each customer's data is separated from other customers' data, enforced in the database. The database and the operations console are not reachable from the public internet

Area	Measures
Encryption	Data is encrypted in transit between users and Frabs, and between Frabs servers, over private encrypted tunnels. Secrets are stored in protected form
Logging	A tamper-evident audit log records staff actions. Servers are monitored and logs are collected centrally
Backups and recovery	Backups of the database are taken regularly and kept separately from the live system
Email	Frabs emails are signed and authenticated. They do not contain tracking links, and never ask for a password or a sign-in code
Incident response	Security incidents are investigated, contained and recorded. Customers are told about a Personal Data Breach as set out in clause 8
Deletion	Data is deleted as set out in clause 12

ANNEX 3

SUB-PROCESSORS

Sub-processor	Purpose	Location
Leaseweb Netherlands B.V.	Hosting of the servers on which the Service runs	Amsterdam, the Netherlands

- 1.1 The current list is also published on the Frabs Sub-processors page. Other service providers that do not receive Customer Data are listed there separately.