E

Spoofing

We cannot tell which of our admins edited personal data, as admin accounts are shared.

E

Tampering

Data in the database can be "fixed" by the admins, and nobody will ever know.

E

Repudiation

We don't log personal data access, because we do not process any customer data, only employee data.

F

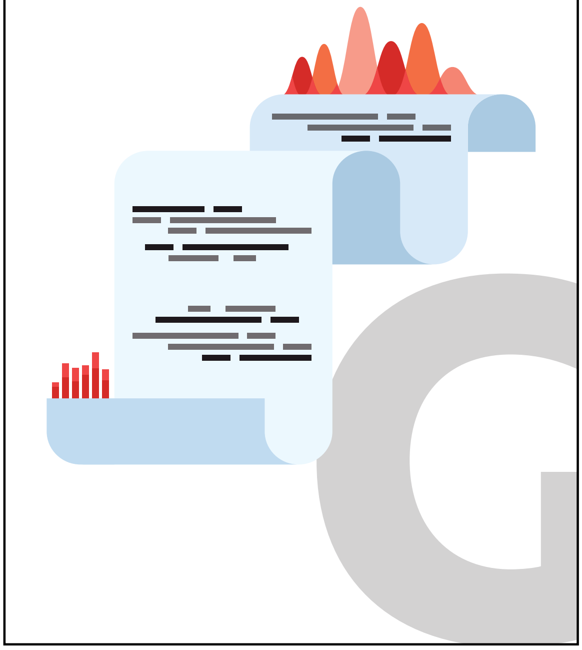
Repudiation

We log changes and deletions of personal data, but viewing is not logged.

G

Repudiation

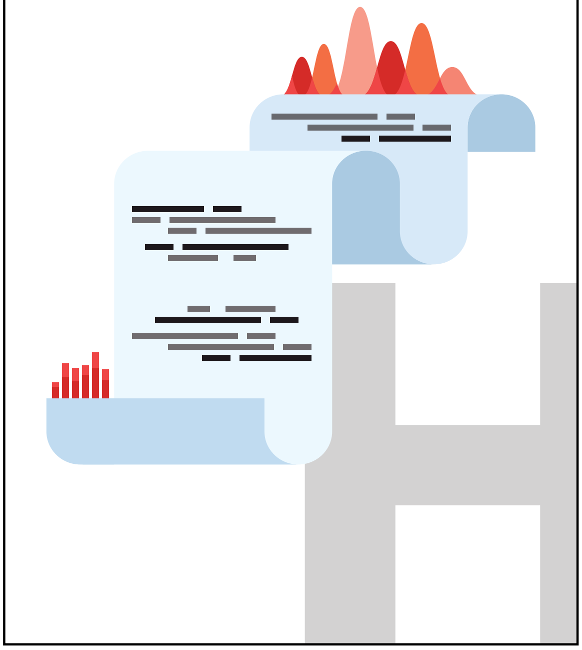
We log personal data access, but there is no ongoing monitoring or alerting.



H

Repudiation

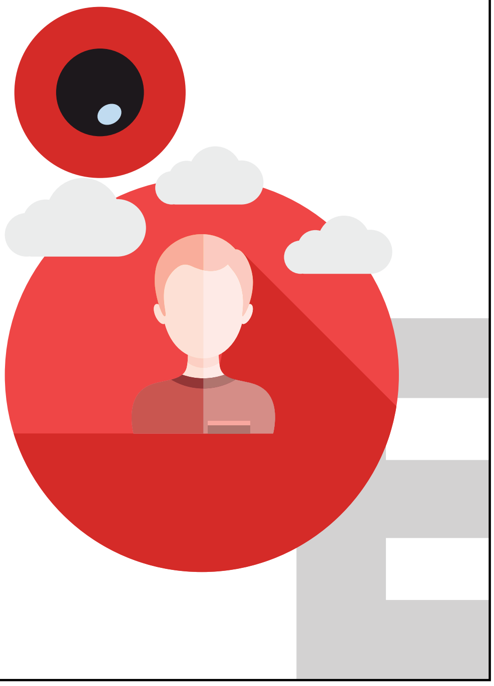
Our audit log contains personal data, and we do not record who looks at our audit logs.



E

Information Disclosure

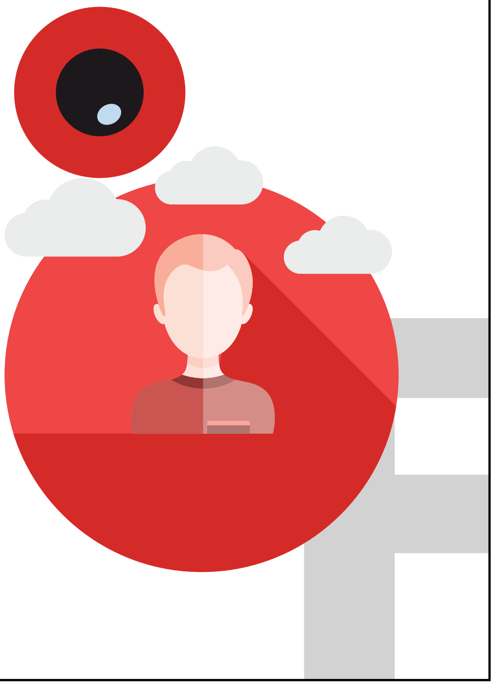
Personal data is being sent over a plaintext connection or email.



F

Information Disclosure

Personal data is being saved on unencrypted media.



E

Denial of Service

Availability of certain personal data is a life-or-death matter, and our system is not as reliable as it should.

2

Transfer

The application uses an API which makes them our data processor, but we don't know whether this is reflected in our API contract.

3

Transfer

We provide an API that ingests personal data, but we do not know whether we are a data processor or a data controller, and it's not defined in our contracts.

4

Transfer

We call an API with personal data, but we do not know where the API is being hosted geographically.

5

Transfer

We export a database dump by writing a CSV file on an FTP site. What happens to the file after it has been downloaded is not our problem.

6

Transfer

Some of our systems are hosted outside the EU, but the service provider says that they take security very seriously, so that's fine.

7

Transfer

Our systems are being administered from outside the EU, but admin access is not personal data access, right? Right?

8

Transfer

We send personal data over email, but only within the company, so that should be fine, right?

9

Transfer

We provide an API to access personal data, and we do not control who can access this API.

A

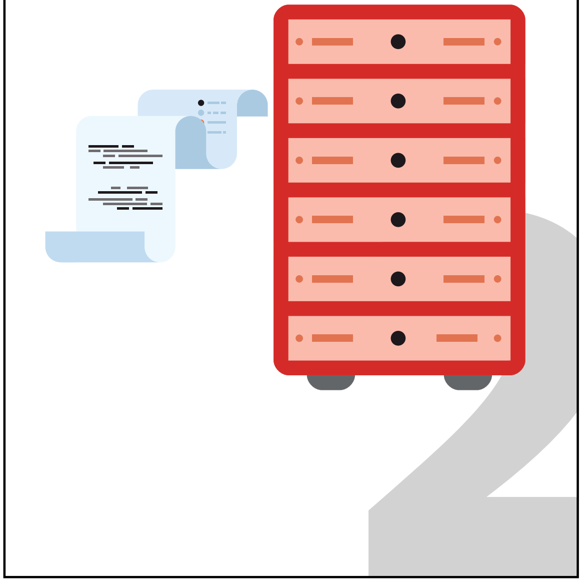
Transfer

You have identified a new personal data flow out from your system.

2

Retention/ Removal

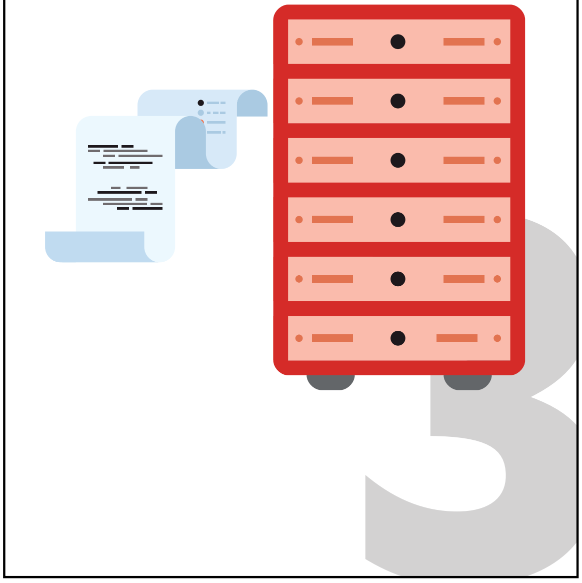
Users' file uploads containing personal data are saved to temp files on the front-end.



3

Retention/ Removal

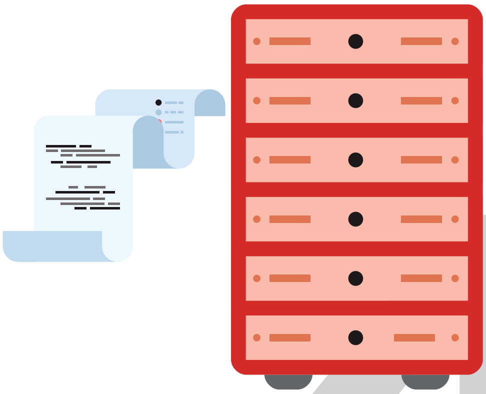
All personal data goes into a large pile in the cloud, and going through it to find individual records would cost a fortune in retrieval and outbound data transfer fees.



4

Retention/ Removal

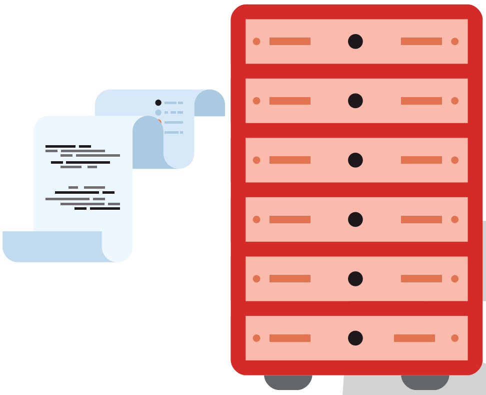
We store personal data on disk, even though we only need it temporarily and could just cache it in memory.



5

Retention/ Removal

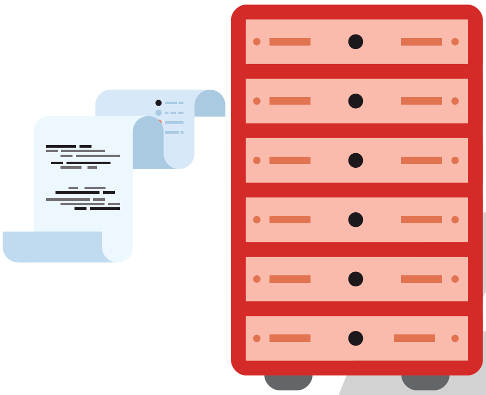
When changing data, we retain all old data in order to be able to show what has been changed.



6

Retention/ Removal

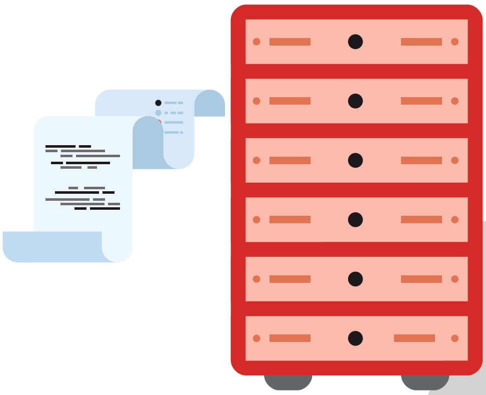
The personal data is stored on a blockchain. We can't delete it at all.



7

Retention/ Removal

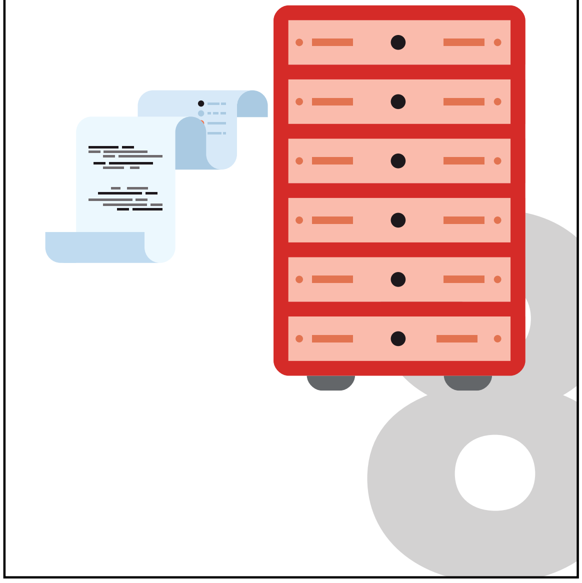
Consent is a checkbox, but to withdraw the consent and remove your data, you need to email us.



8

Retention/ Removal

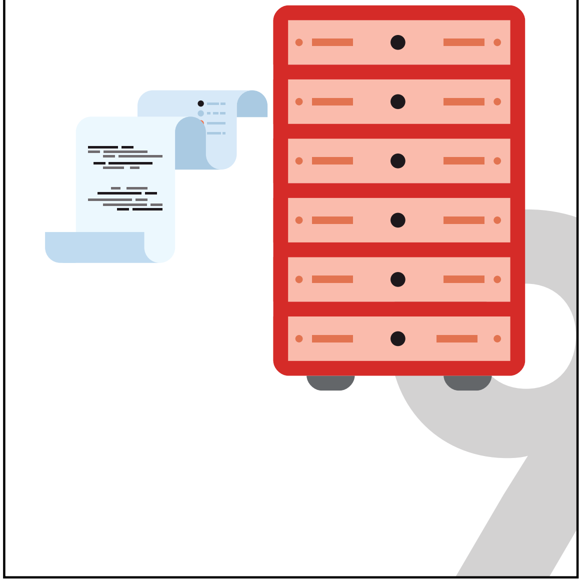
We have not defined a specific retention time for personal data, but we can delete it if someone asks us to.



9

Retention/ Removal

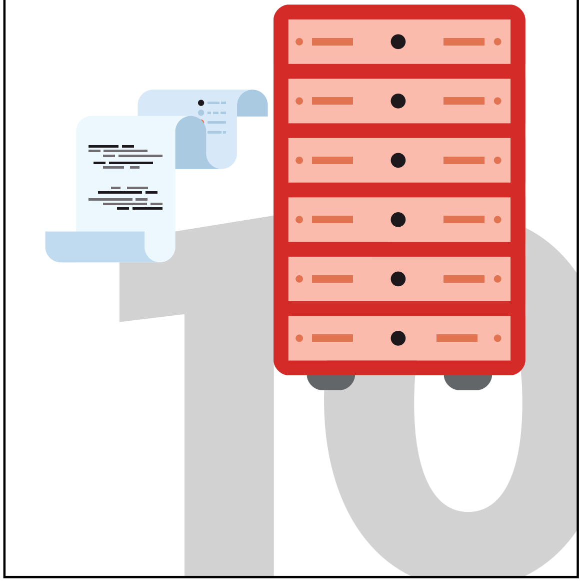
Yes, we have defined a retention time for personal data - it’s defined by the IT department based on disk space usage.



10

Retention/ Removal

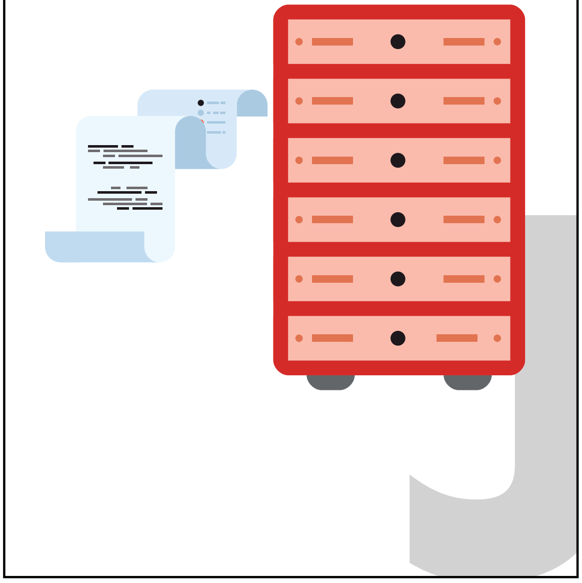
We cannot remove personal data as the database schema requires the data to be there.



J

Retention/ Removal

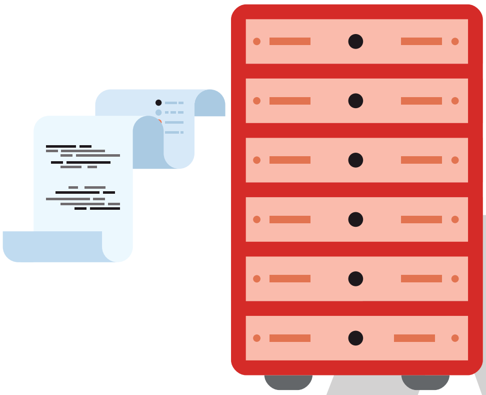
We have defined a retention time for personal data, but that’s only a policy. There is no technical system that enforces it.



A

Retention/ Removal

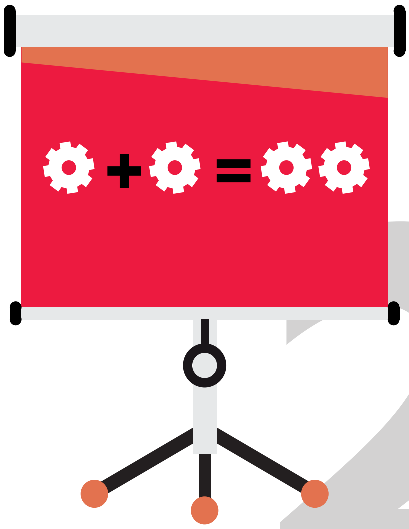
You have found a new personal data storage location that you did not know existed.



2

Inference

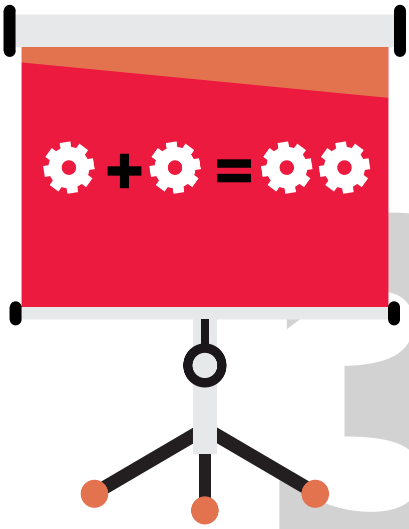
We use a common identifier across all the systems, and also expose this to third parties.



3

Inference

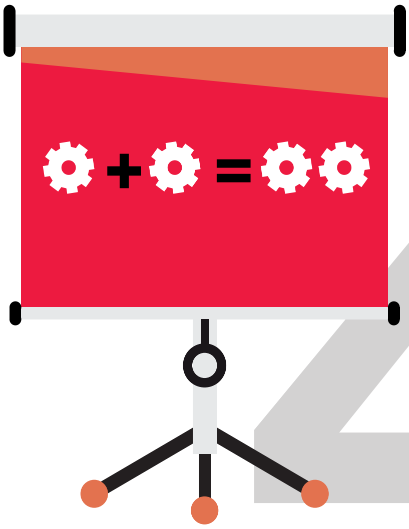
Our geolocation data is as accurate as possible, even if we really only need to know which city the user is from.



4

Inference

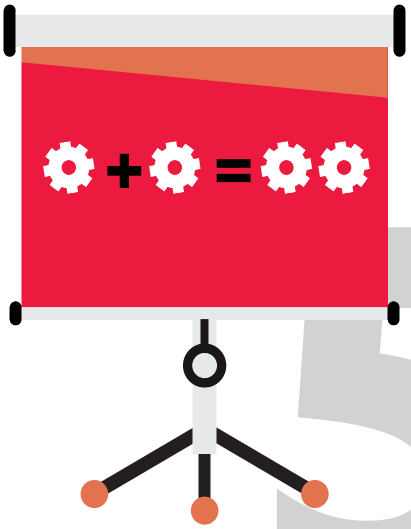
We use our users' names or email addresses as reference keys between systems, even if we could use random identifiers.



5

Inference

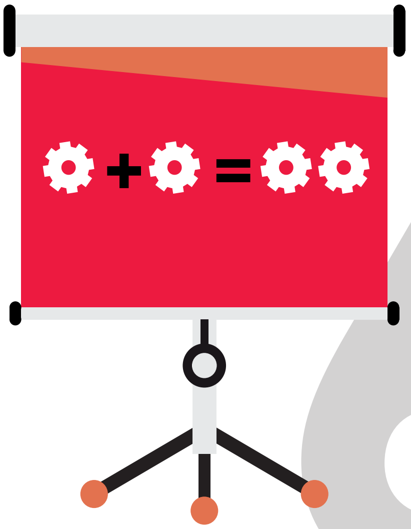
We use national ID numbers or SSNs as identifiers, because they are conveniently unique.



6

Inference

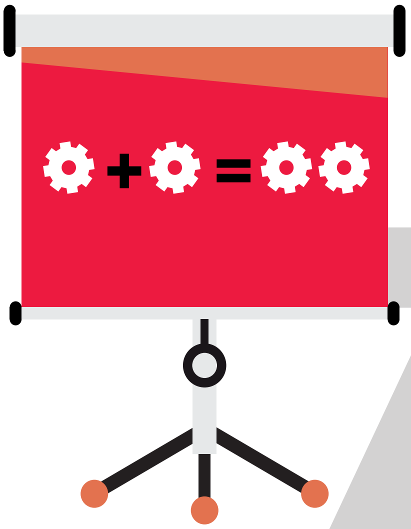
We use identifiers in our web links. These identifiers leak in browsers' referrer headers and get logged by redirectors and URL shorteners.



7

Inference

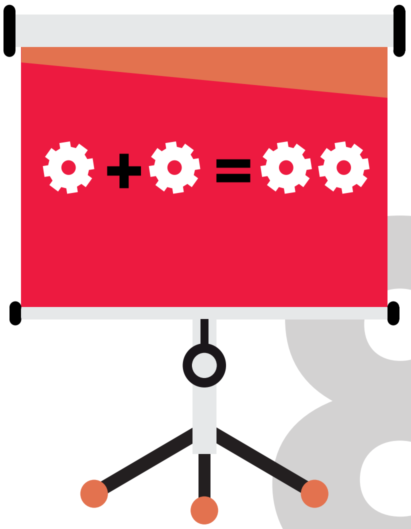
There is no review process for introducing new trackers or advertising providers on the web pages; whatever our designers like, or marketing sells, will be used.



8

Inference

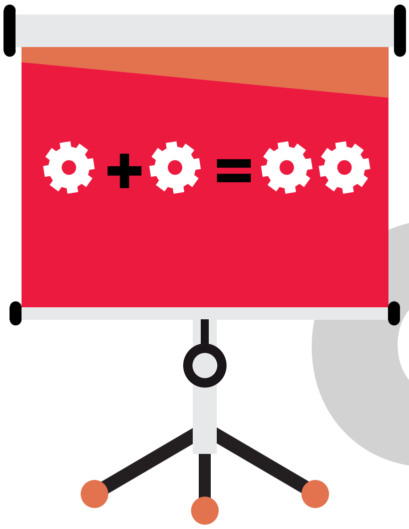
Our telemetry is tied to the users, even though our analytics couldn't care less who the user actually is.



9

Inference

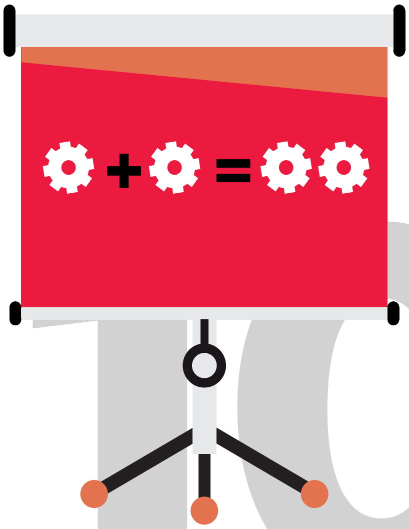
A neural network makes customer-related decisions, but nobody can really explain to the customers what the model is based on.



10

Inference

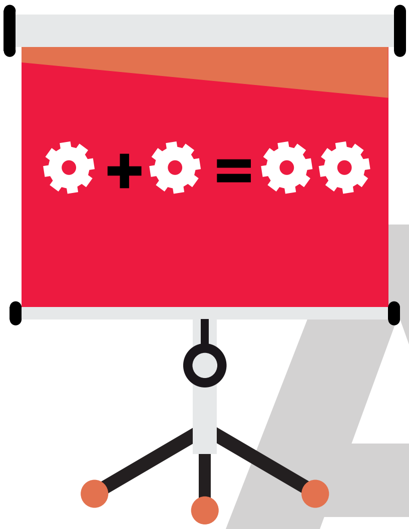
We do not make any checks to personal data before we use it for training machine learning models.



A

Inference

You have found a new place where we can replace personal data with a random identifier.



2

Minimisation

We put absolutely everything in the audit log, so we can positively audit all personal data activities.

3

Minimisation

Our testing data is a month-old copy from production. Fake data just does not have the same feel to it.

4

Minimisation

Our website does not work at all with an ad blocker.

5

Minimisation

We send personal data to an API even though we believe it is really not being used for anything.

6

Minimisation

We'll just block EU and California from our site. We've got enough customers elsewhere.

A Minimisation

You have found a piece of personal data that we can technically do without.