Welcome to Elevation of Privacy, an unofficial extension set to Microsoft's Elevation of Privilege threat modelling card game.

These playing cards portray privacy and data protection compliance risks that have been identified in the real world. The simplest way to use these cards is to draw a Data Flow Diagram or a Message Sequence Chart, and discuss the aspects in the context of each of the data flows and data stores.

You can play this game with or without the original Elevation of Privilege deck. It extends the STRIDE model with TRIM:

- Transport of personal data across geopolitical or contractual boundaries
- Retention and Removal of personal data
- Inference of personal data from other personal data, for example, through correlation
- Minimisation of personal data and its use

Those suites that have been extended beyond the normal A-K cards in the original game have hexadecimal values starting from E.

Instructions

We recommend you use these cards in conjunction with a security threat modelling session. Privacy cannot exist without security. If you use data flow analysis for your threat modelling, it usually provides a very good basis for the analysis of personal data flows as well.

These cards do not fully cover EU General Data Protection Regulation compliance, but are a useful safety net to catch many of the related risks and problematic design decisions and may form a part of a Privacy Impact Assessment (PIA) activity.

For best results, discuss privacy and data protection both during service design and technical design.

Working group: Marko Hämäläinen, Laura Noukka, Hiski Ruhanen, Ilona Varis, Antti Vähä-Sipilä.

Instructions

E

Spoofing

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

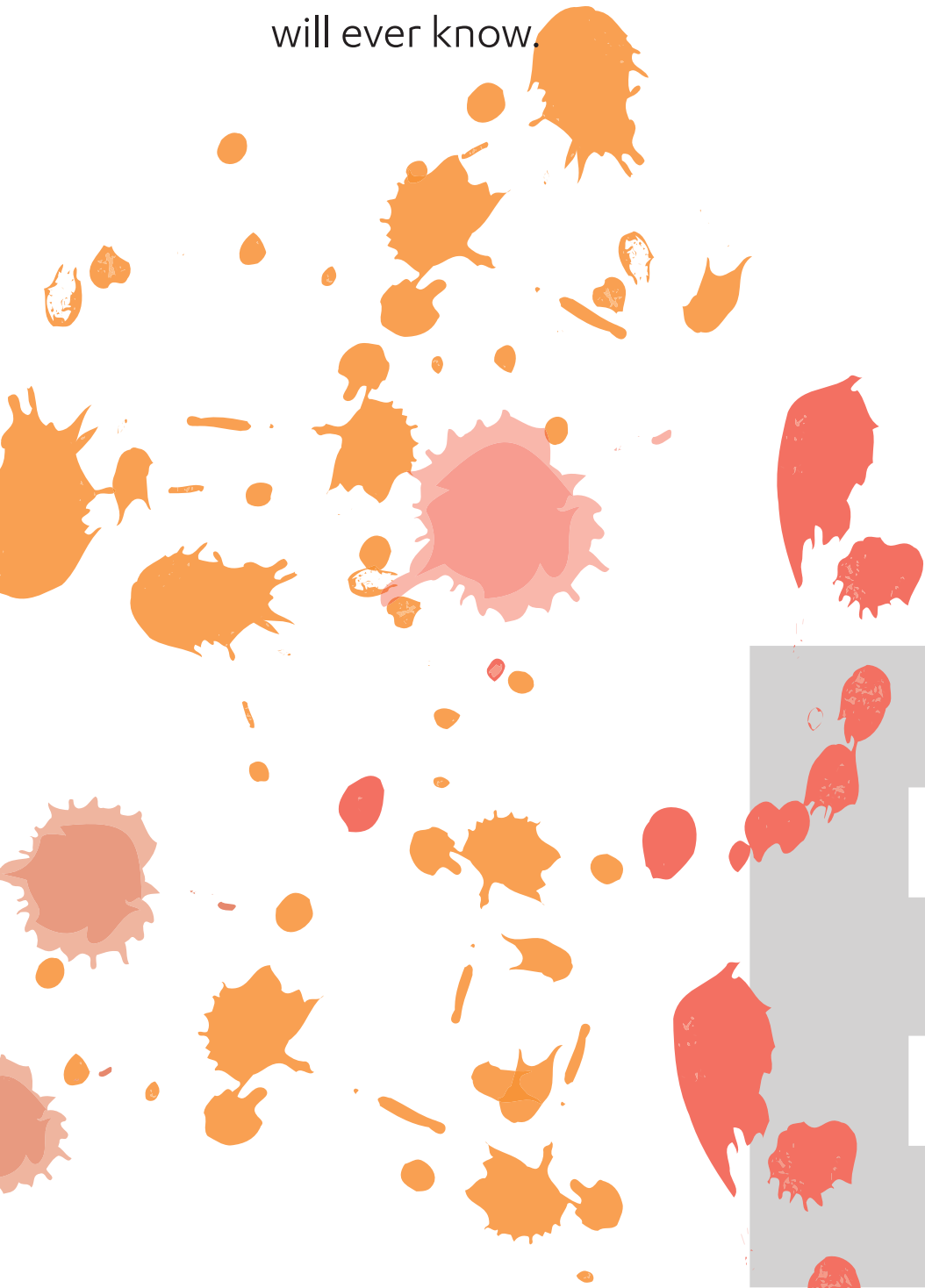
F-Secure

ELEVATION OF PRIVACY

E

Tampering

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



F-Secure

ELEVATION OF PRIVACY

Repudiation

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

F-Secure

ELEVATION OF PRIVACY

F

Repudiation

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

F

F-Secure

ELEVATION OF PRIVACY

G

Repudiation

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

F-Secure

ELEVATION OF PRIVACY

Repudiation

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

F-Secure

ELEVATION OF PRIVACY

E

Information Disclosure

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

F-Secure

ELEVATION OF PRIVACY

F

Information Disclosure

Personal data is being saved on unencrypted media.

F-Secure

ELEVATION OF PRIVACY

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.

F-Secure

ELEVATION OF PRIVACY

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.

F-Secure

ELEVATION OF PRIVACY

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.

F-Secure

ELEVATION OF PRIVACY

4 Transfer

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

F-Secure

ELEVATION OF PRIVACY

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.

F-Secure

ELEVATION OF PRIVACY

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.

F-Secure

ELEVATION OF PRIVACY

7 Transfer

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

F-Secure

ELEVATION OF PRIVACY

8 Transfer

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

F-Secure

ELEVATION OF PRIVACY

9 Transfer

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

F-Secure

ELEVATION OF PRIVACY

A

Transfer

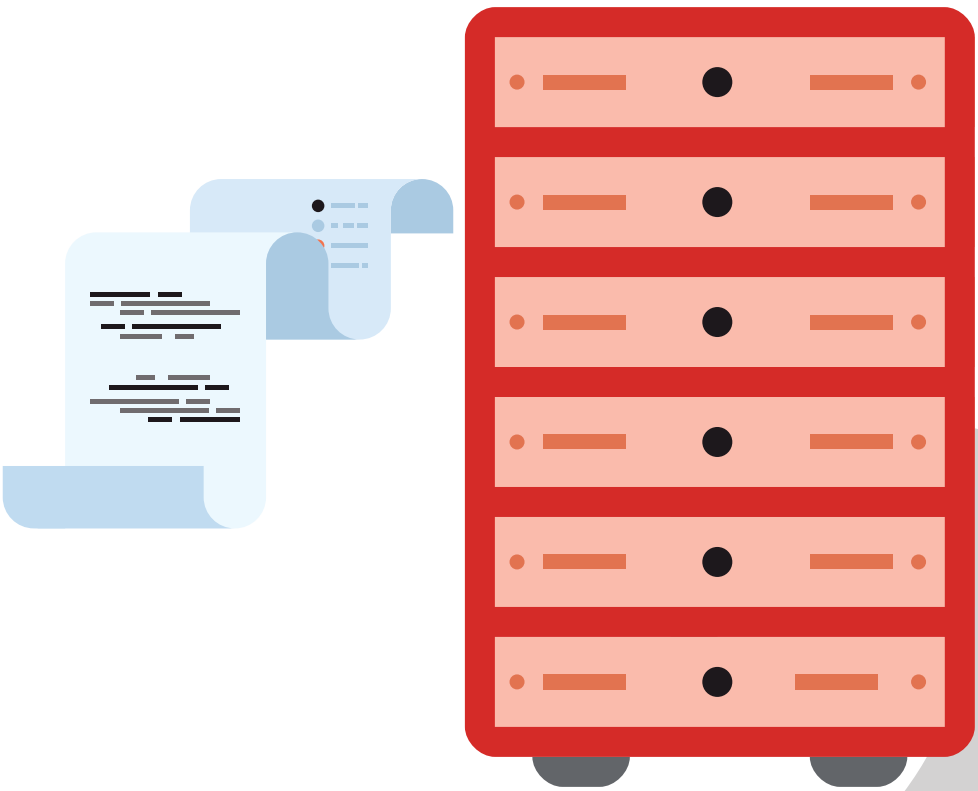
You have identified a new personal data flow out from your system.

F-Secure

ELEVATION OF PRIVACY

2 Retention/ Removal

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

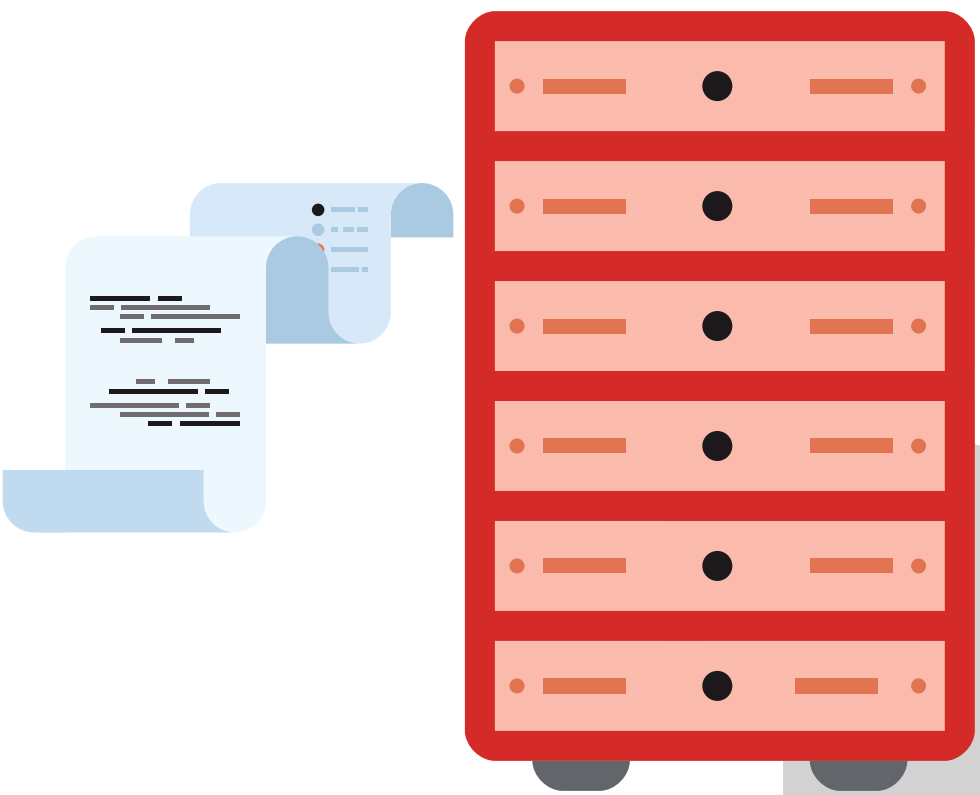


F-Secure

ELEVATION OF PRIVACY

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.

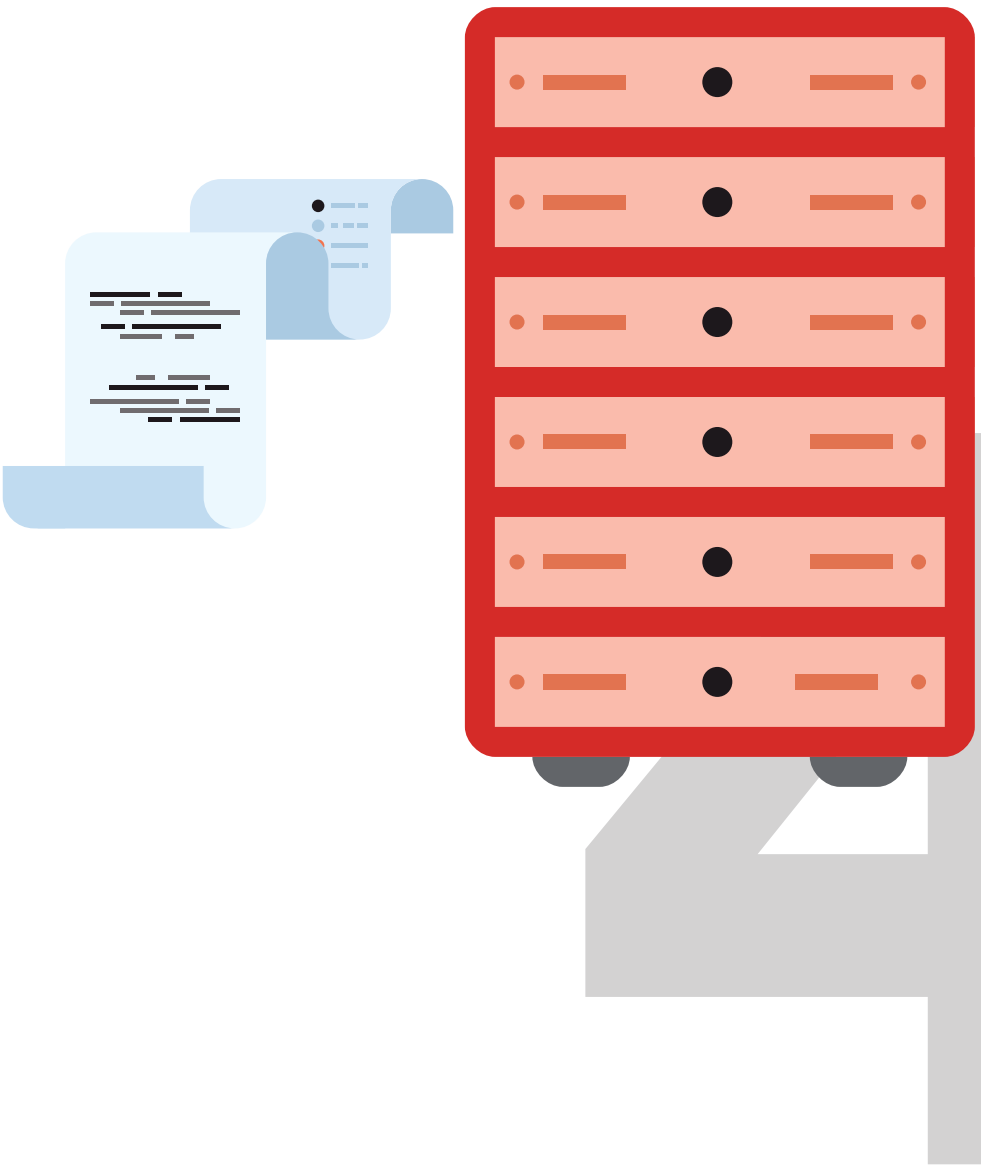


F-Secure

ELEVATION OF PRIVACY

4 Retention/ Removal

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

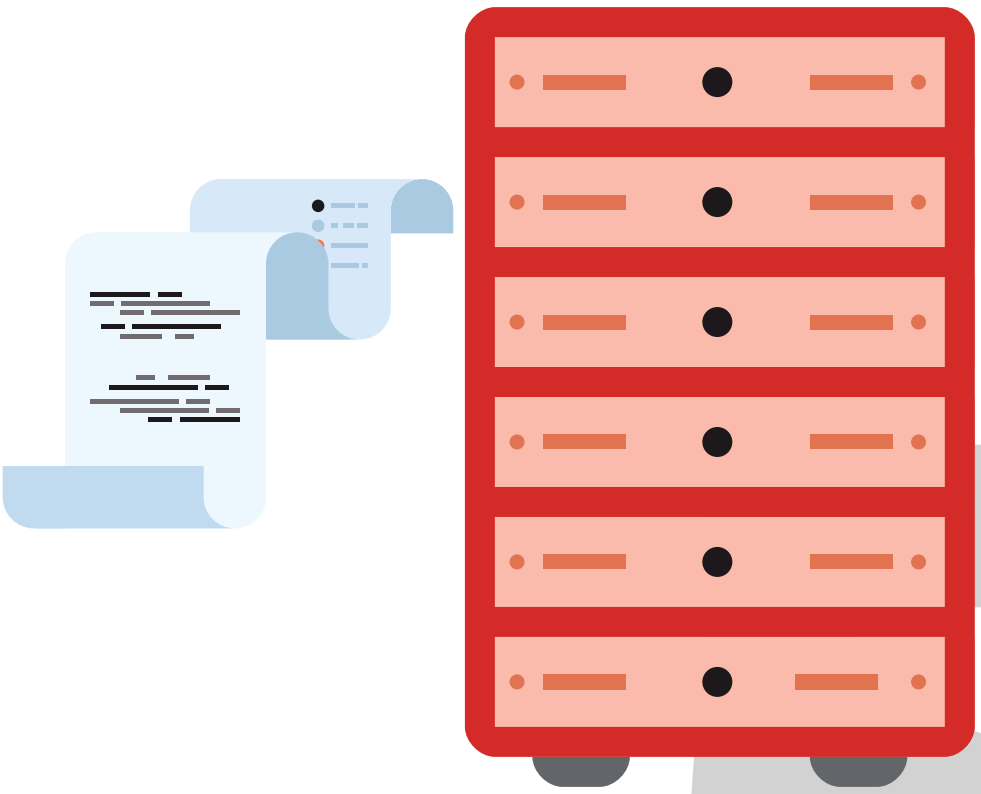


F-Secure

ELEVATION OF PRIVACY

5 Retention/ Removal

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

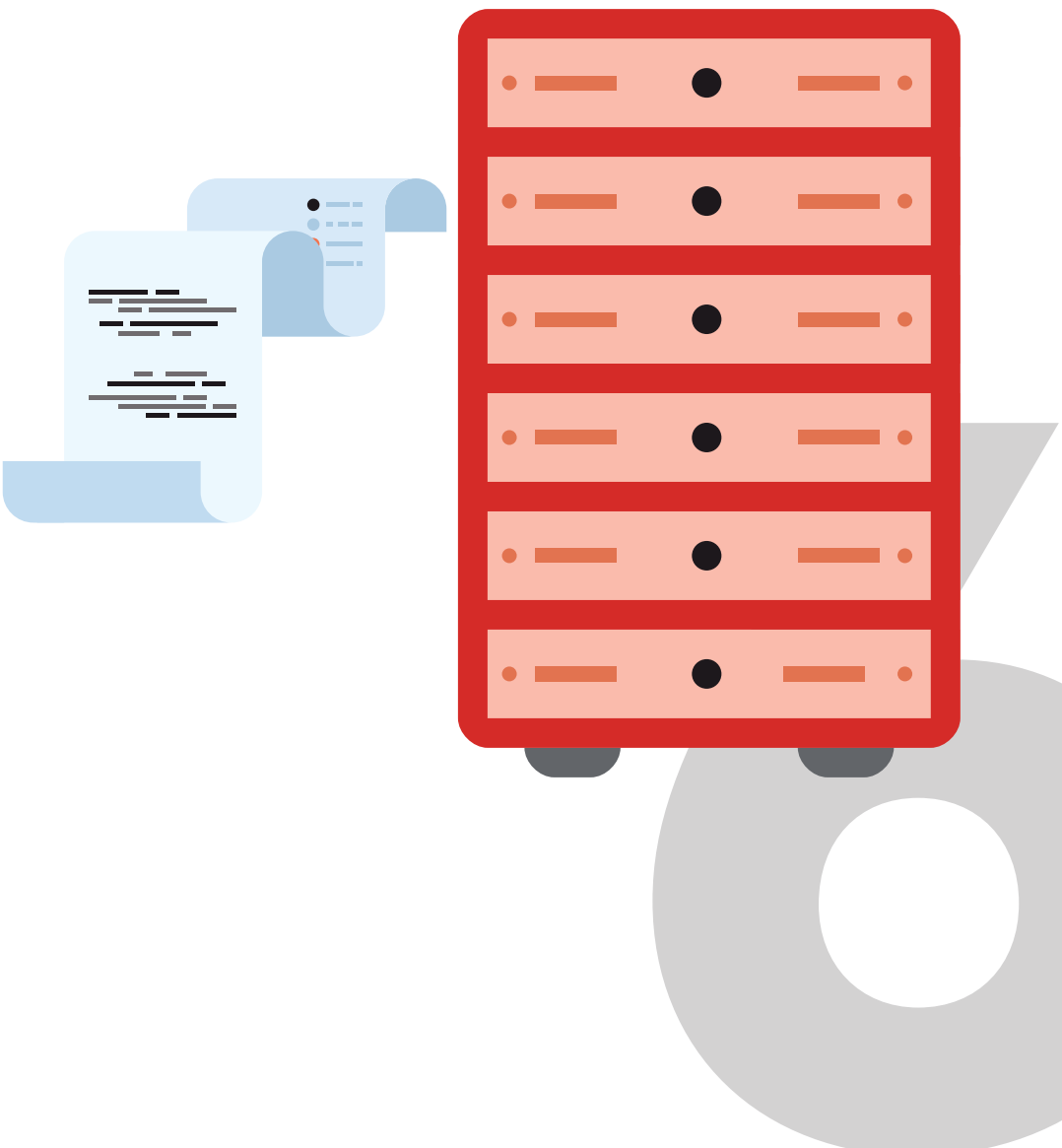


F-Secure

ELEVATION OF PRIVACY

6 Retention/ Removal

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

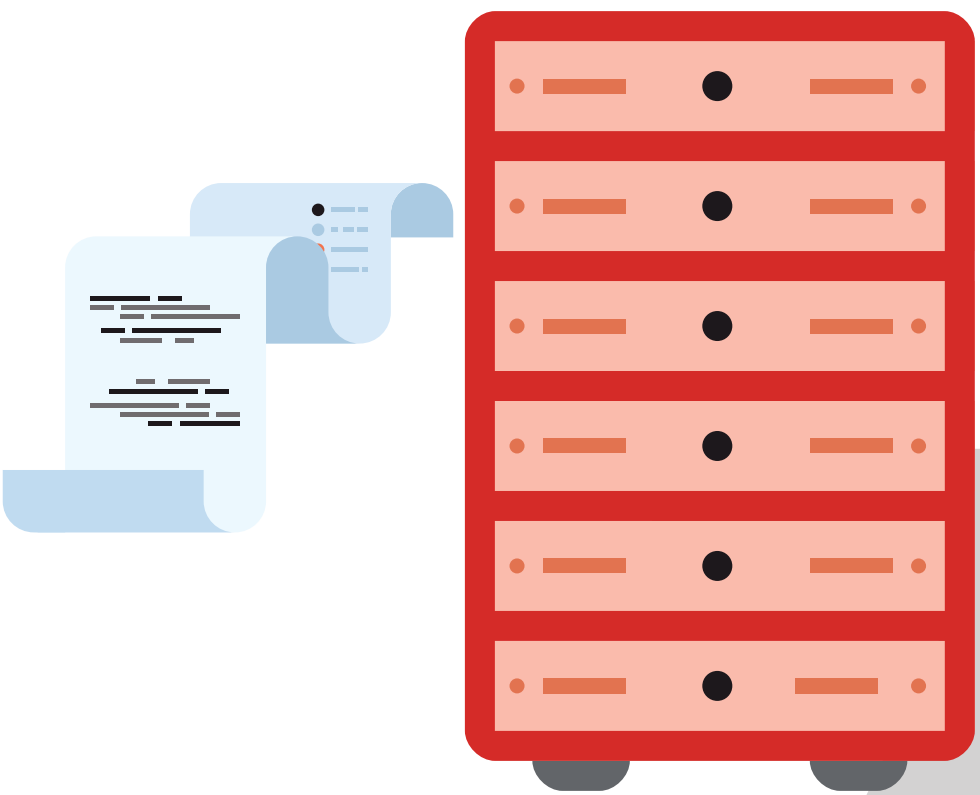


F-Secure

ELEVATION OF PRIVACY

7 Retention/ Removal

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

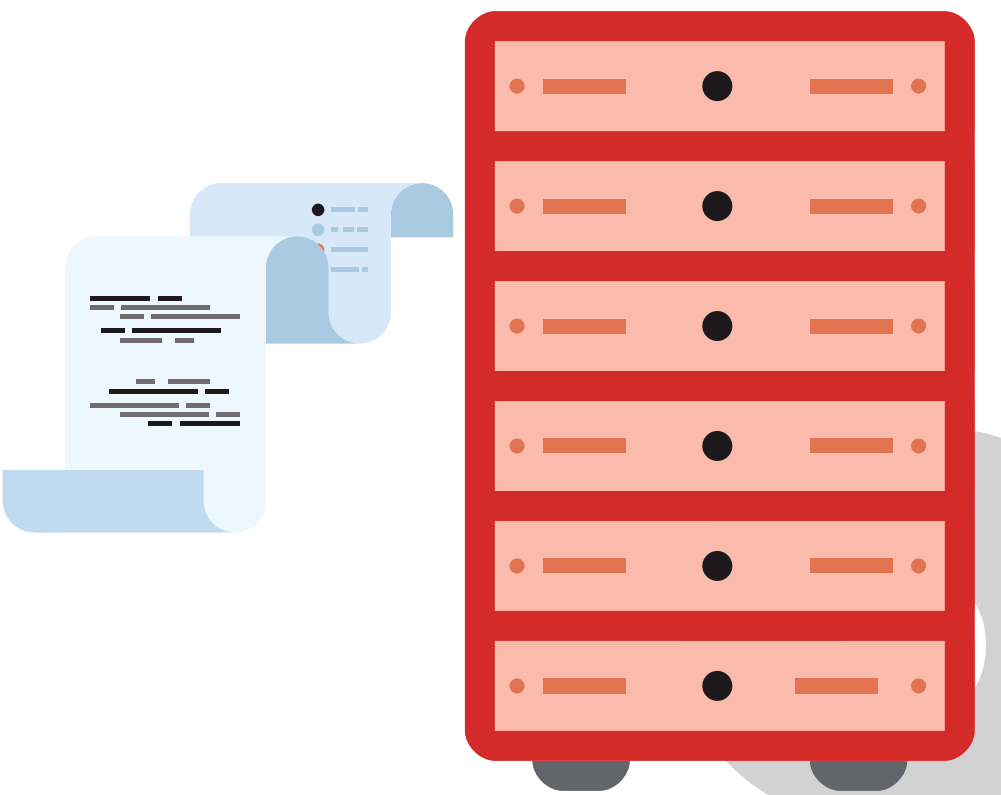


F-Secure

ELEVATION OF PRIVACY

8 Retention/ Removal

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

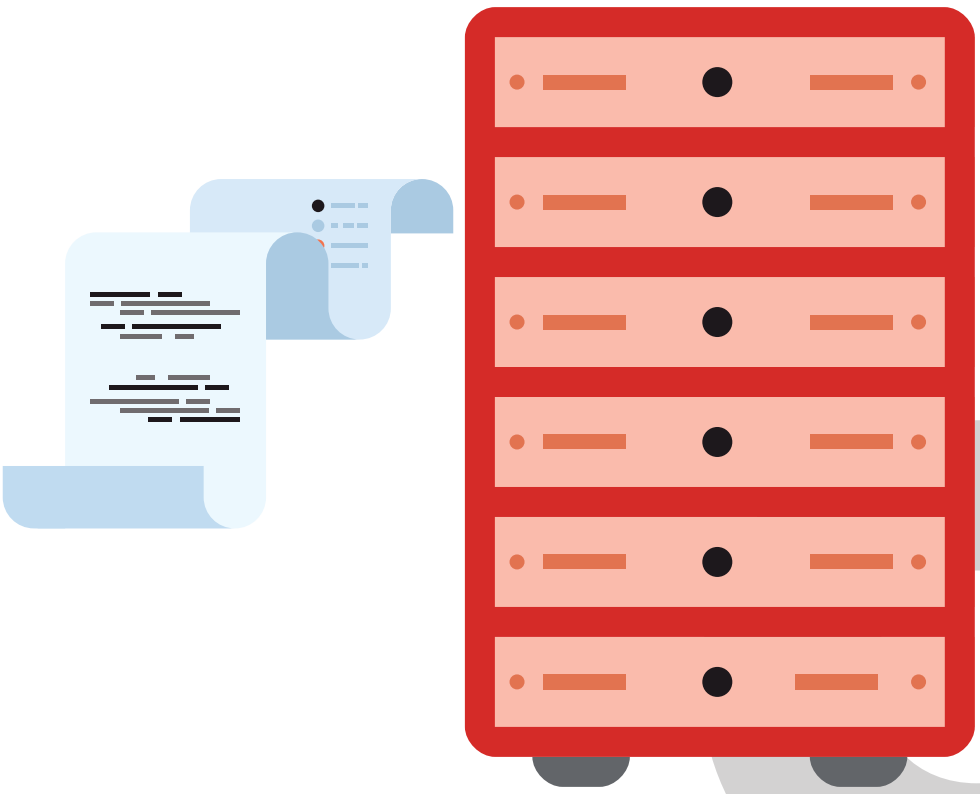


F-Secure

ELEVATION OF PRIVACY

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.

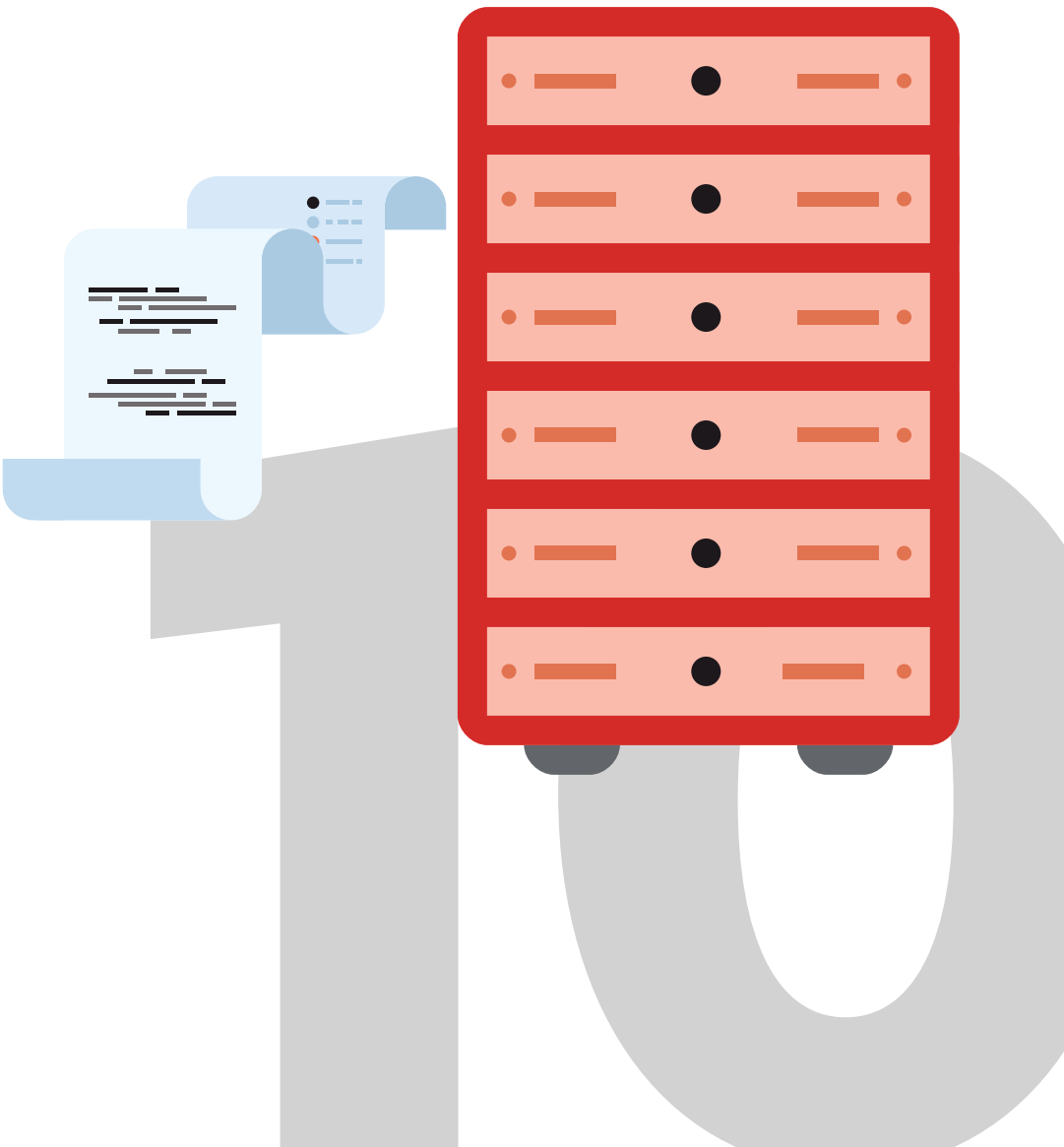


F-Secure

ELEVATION OF PRIVACY

10 Retention/ Removal

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



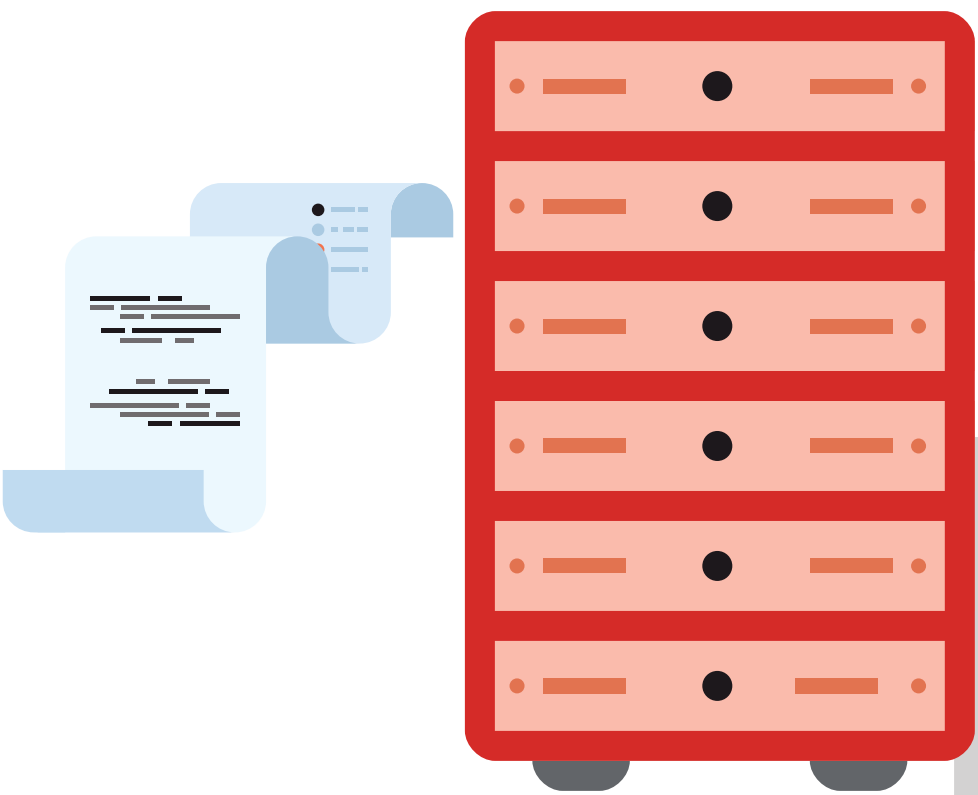
F-Secure

ELEVATION OF PRIVACY

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.

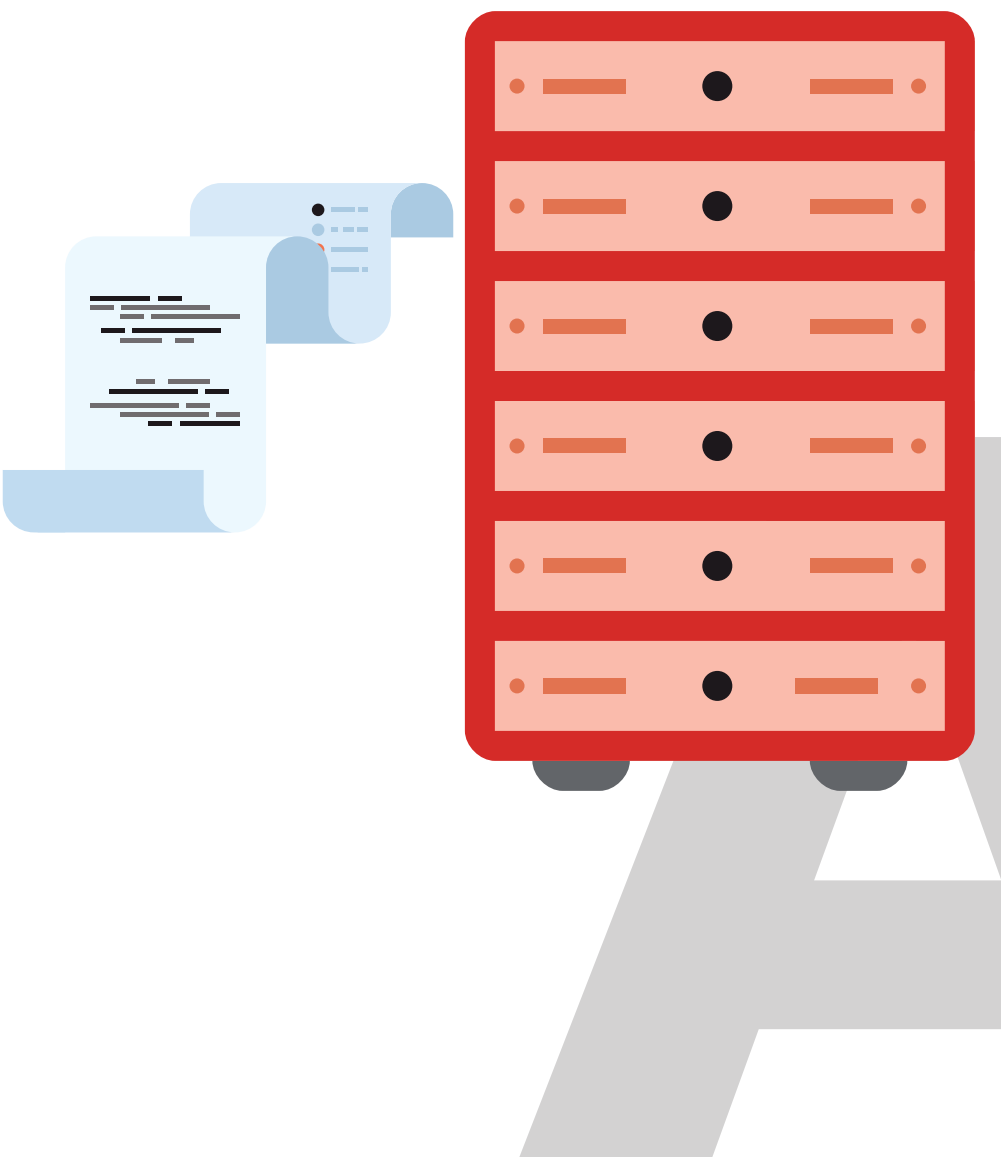


F-Secure

ELEVATION OF PRIVACY

A Retention/ Removal

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

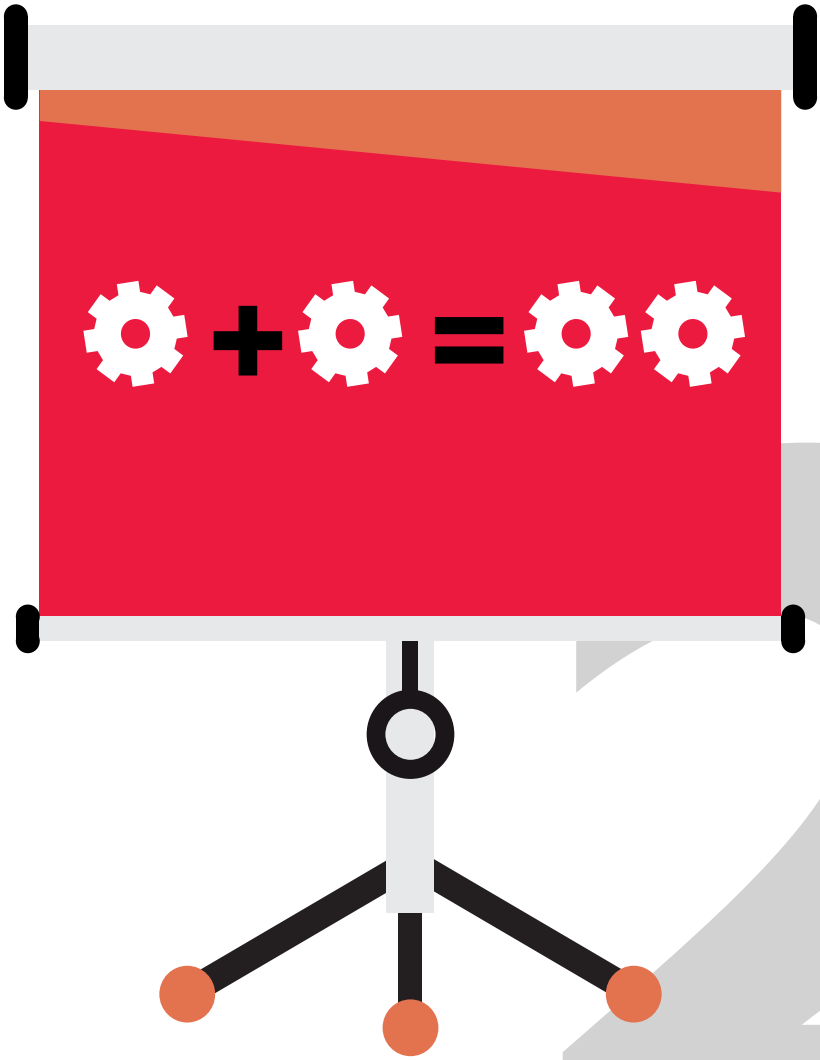


F-Secure

ELEVATION OF PRIVACY

2 Inference

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

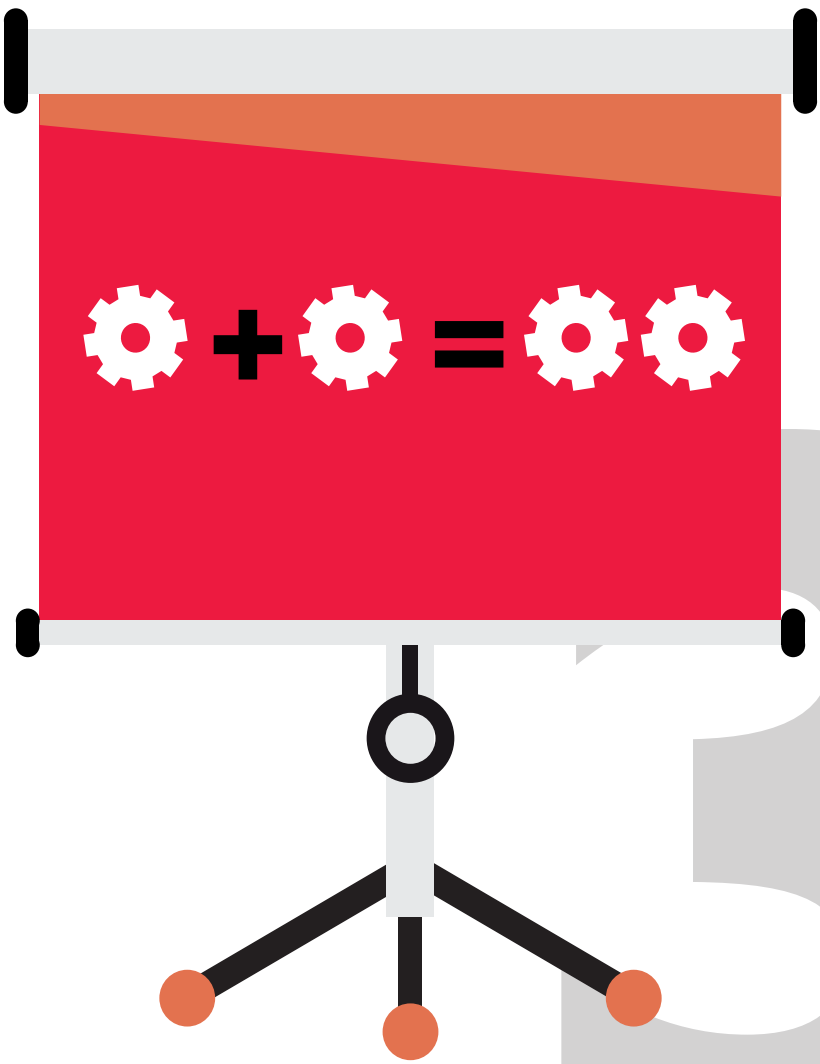


F-Secure

ELEVATION OF PRIVACY

3 Inference

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

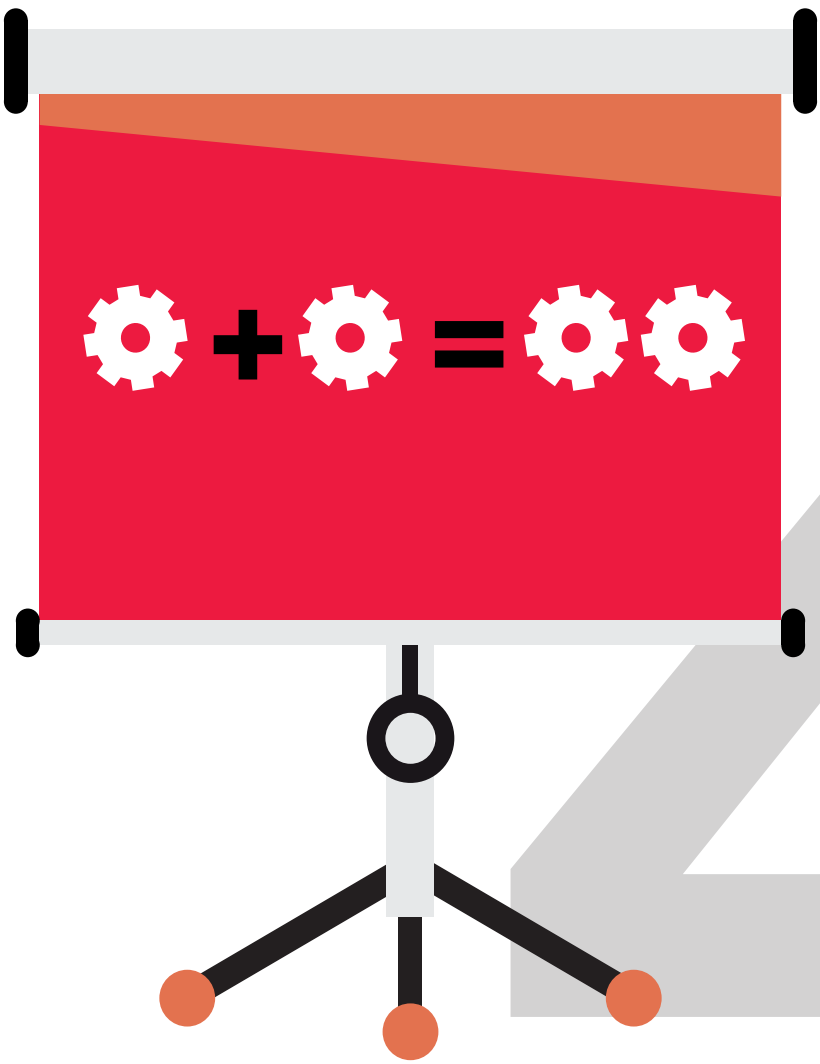


F-Secure

ELEVATION OF PRIVACY

4 Inference

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

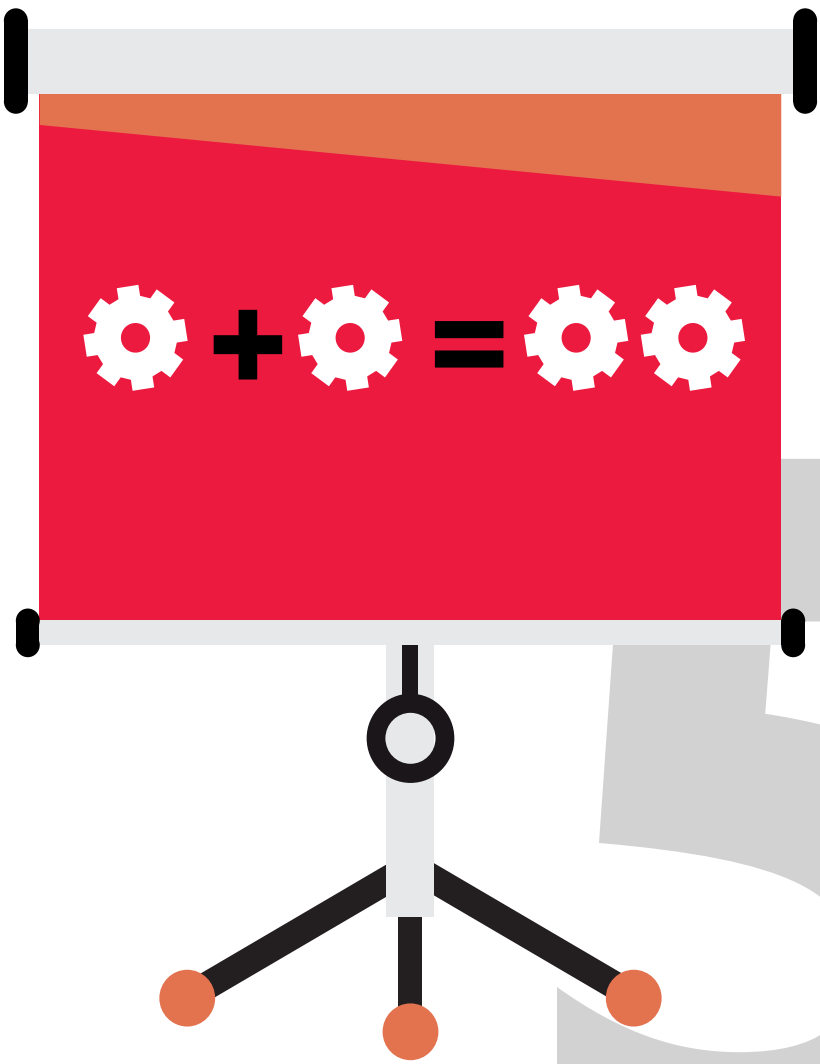


F-Secure

ELEVATION OF PRIVACY

5 Inference

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

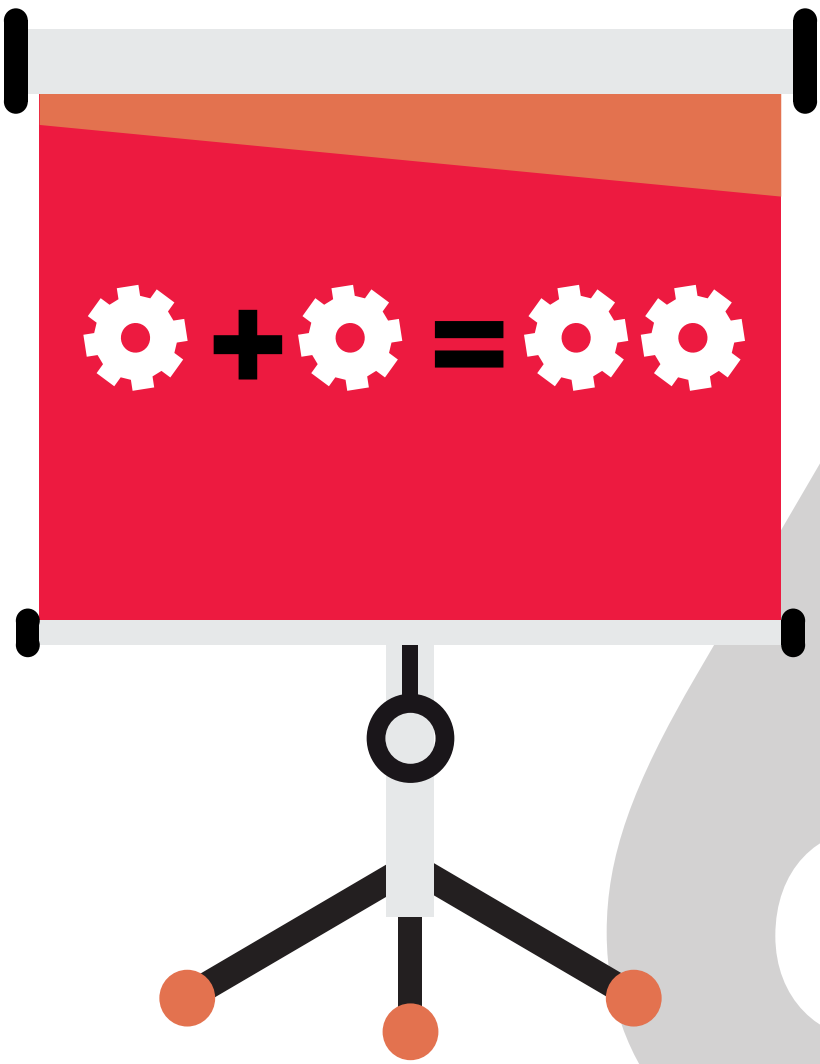


F-Secure

ELEVATION OF PRIVACY

6 Inference

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

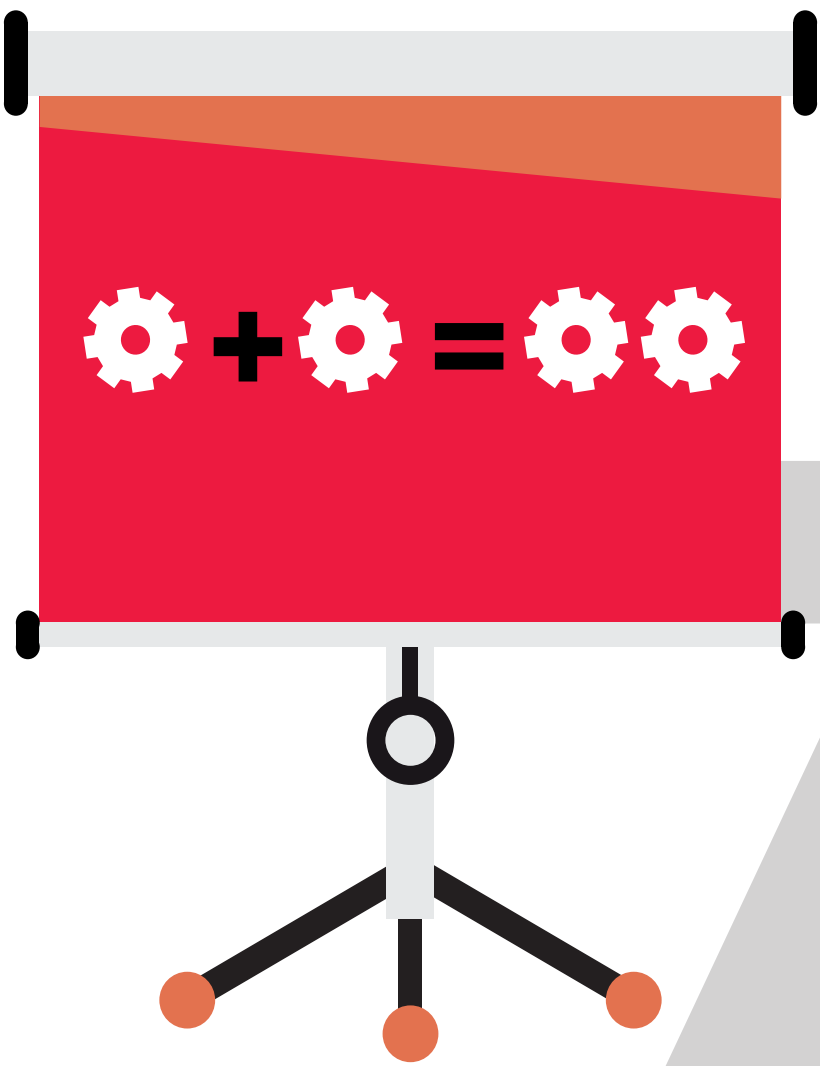


F-Secure

ELEVATION OF PRIVACY

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.

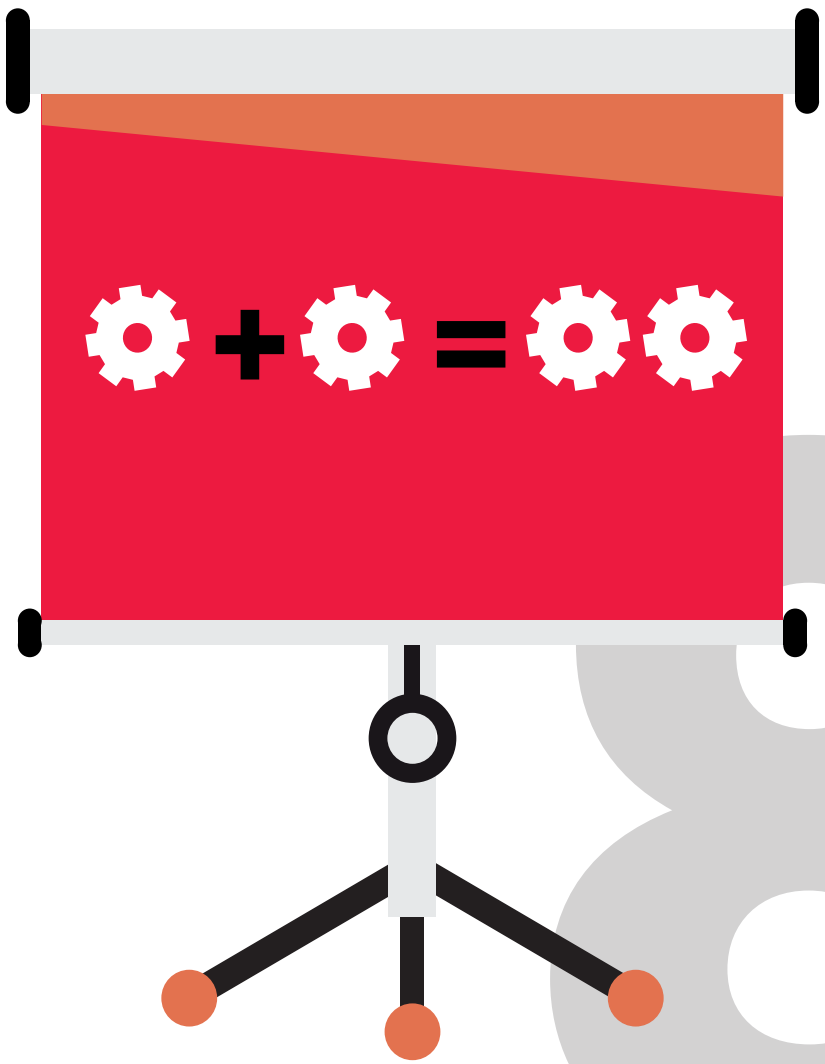


F-Secure

ELEVATION OF PRIVACY

8 Inference

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

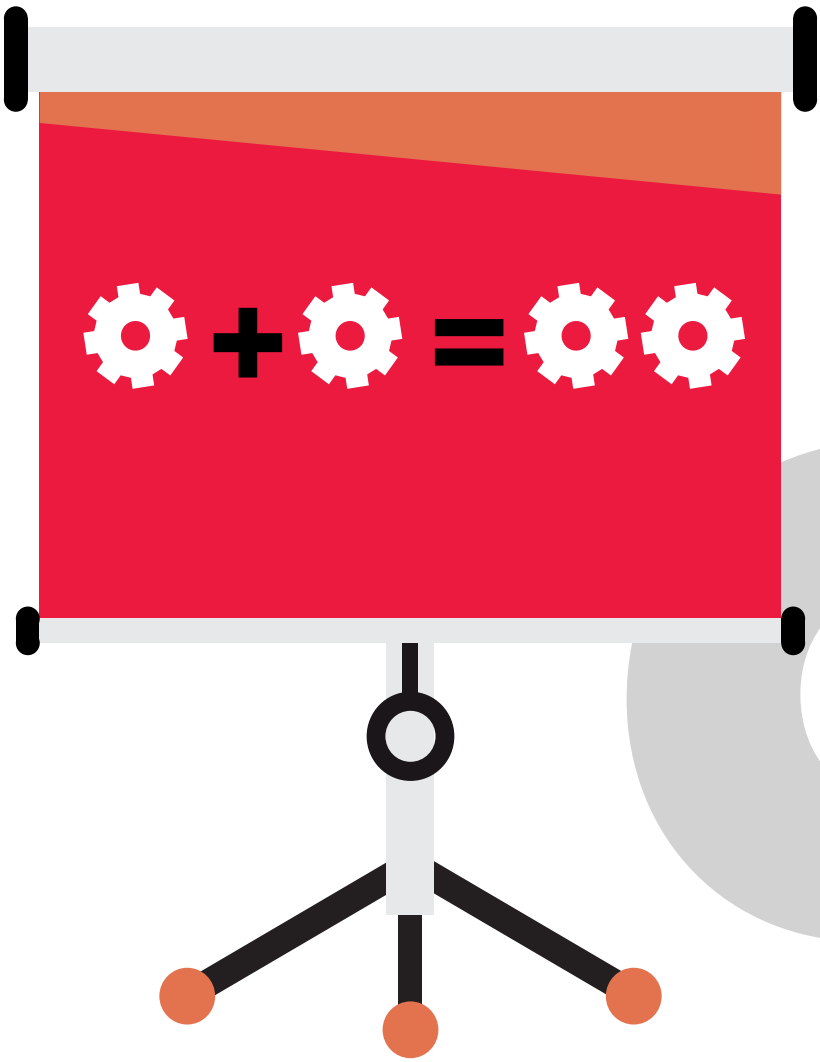


F-Secure

ELEVATION OF PRIVACY

9 Inference

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

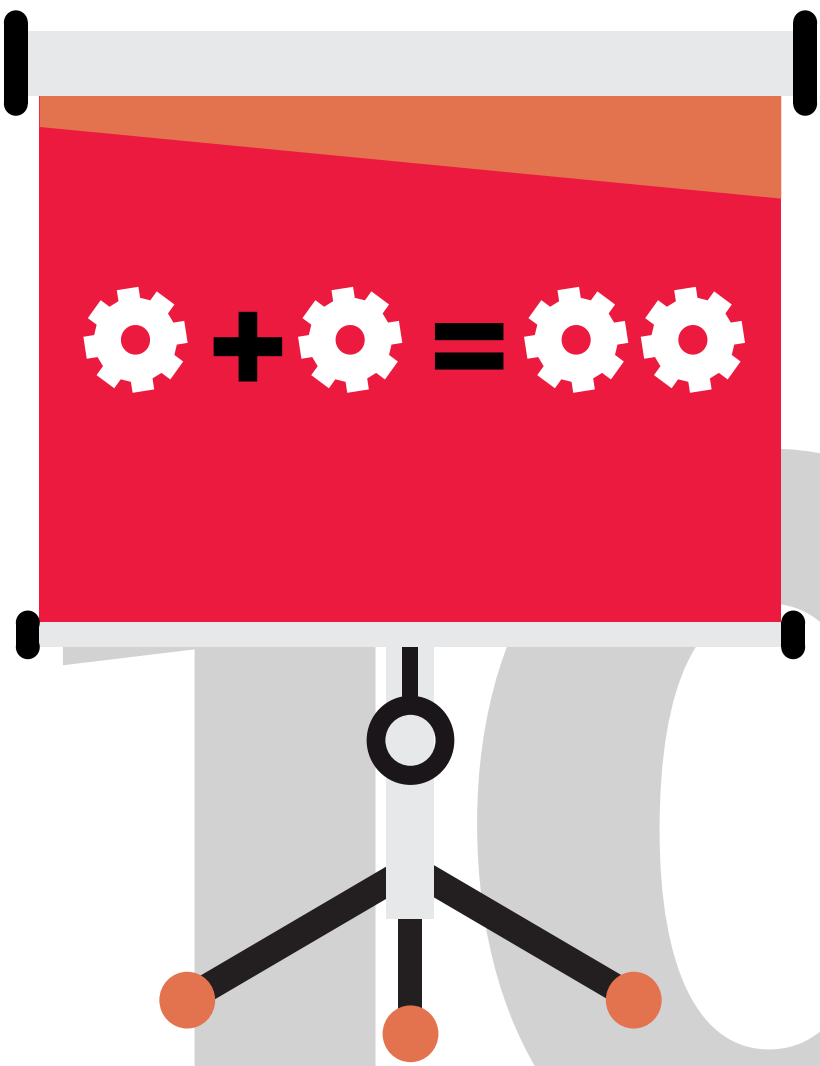


F-Secure

ELEVATION OF PRIVACY

10 Inference

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

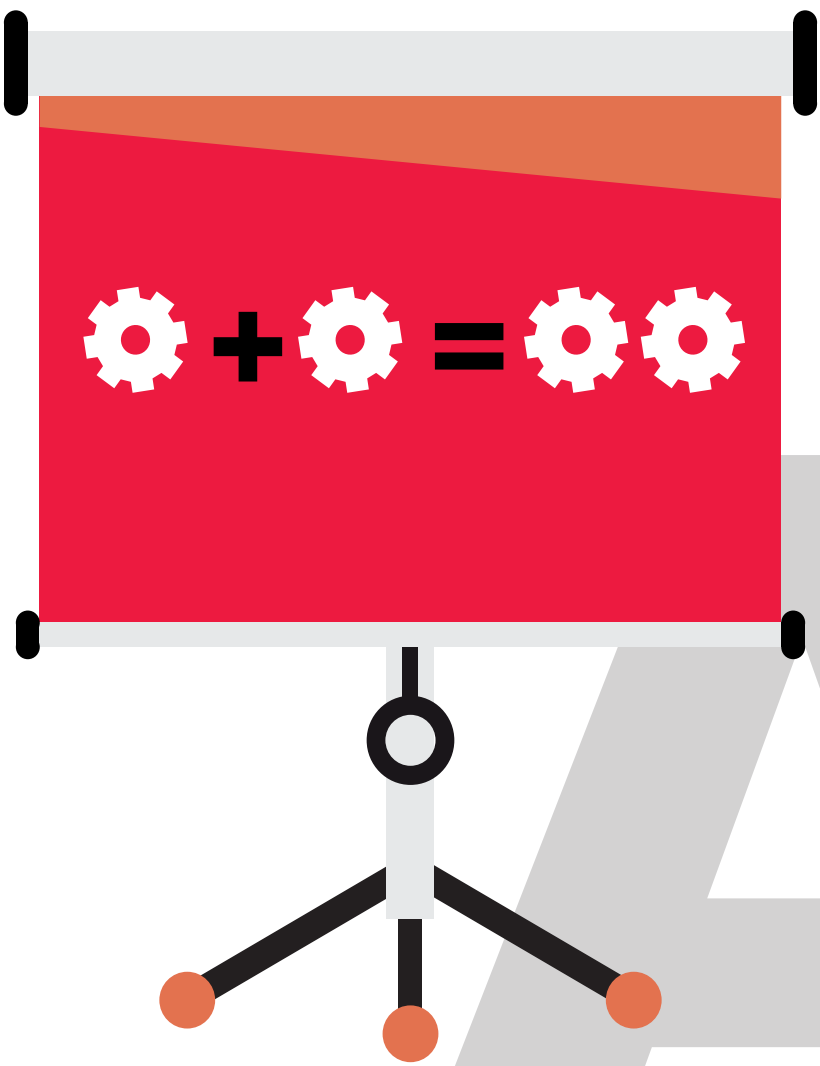


F-Secure

ELEVATION OF PRIVACY

A Inference

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



F-Secure

ELEVATION OF PRIVACY

2 Minimisation

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

F-Secure

ELEVATION OF PRIVACY

3 Minimisation

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

3

F-Secure

ELEVATION OF PRIVACY

4 Minimisation

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

4

F-Secure

ELEVATION OF PRIVACY

5 Minimisation

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

F-Secure

ELEVATION OF PRIVACY

6 Minimisation

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

F-Secure

ELEVATION OF PRIVACY

A

Minimisation

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

F-Secure

ELEVATION OF PRIVACY