LEGAL

Data Processing Agreement

Our standard terms for processing personal data on behalf of customers, under Article 28 GDPR. This text forms part of every agreement for our services, unless we sign something else together.

Last updated November 10, 2026 · Version 1.0

CONTENTS

1. Parties and scope
2. Roles and instructions
3. What data, and whose
4. Security
5. Confidentiality
6. Subprocessors
7. Transfers outside the EEA
8. Personal data breaches
9. Requests from data subjects
10. Audits and accountability
11. Return and deletion
12. Duration, precedence and law

1. Parties and scope

This data processing agreement applies between AssistSec, registered with the Dutch Chamber of Commerce under number 42175591, with its registered address at Hooizolder 385, 9205 CR Drachten (the processor), and the customer that has an agreement with us for penetration testing, continuous testing or the use of our customer portal (the controller).

It forms part of that agreement and applies to the extent that we process personal data on the customer's behalf in performing it. If the parties have signed a separate data processing agreement, that one prevails.

2. Roles and instructions

The customer determines the purpose and means of the processing and is the controller. We process personal data only on the customer's behalf and on its documented instructions. The agreement, the agreed scope of a test and this data processing agreement together constitute those instructions.

If we believe an instruction conflicts with the GDPR or with other law, we say so at once, before carrying it out. We may depart from instructions only where Union or Dutch law requires a processing of us, in which case we inform the customer beforehand, unless that law forbids it.

3. What data, and whose

The processing covers the data that comes with our services. As a rule these are the following categories.

> **Portal accounts**
> Name, work e-mail address and role of the staff the customer gives access to the customer portal, with their sign-in and activity records.
>
> **Contact details**
> Names and contact details of the customer's contact persons, and a delivery address when a printed report is requested.
>
> **Test accounts**
> The accounts and access details the customer provides for a test.
>
> **Test data**
> What a test records about the systems under test, including personal data that appears in those systems, their responses or the source code provided. Which data that is depends on the content of the tested environment, which is the customer's to decide.

Data subjects are, as a rule, the customer's staff and contact persons, and the people whose data is in the tested systems, such as the customer's

users or clients.

The customer warrants that it may have the systems in scope tested and that there is a legal basis for the processing. We recommend using test environments or test data where possible, so a test touches as little real personal data as it can.

4. Security

We take the technical and organisational measures Article 32 GDPR requires, appropriate to the risk. They include at least the following.

- Encryption of all traffic to and from our systems.
- Separate encryption of stored secrets, such as test accounts, keys and integration tokens.
- Access by role, where the customer's staff see only their own environment and our pentesters only the projects they are assigned to.
- Two-step sign-in for accounts in the customer portal.
- An activity log of what happens in the customer's environment, readable by the customer.
- Wiping of workspaces in which source code was read as soon as the job ends, and deletion of uploaded code archives right after their scan by default.

A current description of these measures is published at Security and privacy. That page accompanies this agreement as the overview of the measures; we do not weaken the measures without informing the customer first.

5. Confidentiality

Everyone who processes the customer's personal data under our authority is bound to confidentiality, by contract or by law. Access to the customer's data is limited to those who need it for the engagement.

6. Subprocessors

The customer gives us general written authorisation to engage subprocessors. The categories and the main parties are published at Security and privacy; we provide the current list with countries of establishment when the agreement is entered into, and afterwards on request.

Which language model provider belongs to an engagement is agreed per engagement, as described at How we use AI.

We inform the customer before any change to the list. If the customer objects within fourteen days on reasonable grounds, the parties look for a solution together, and the customer is not kept on the disputed subprocessor against its will where that is reasonable. We impose on every subprocessor, by contract, the same obligations as those in this data processing agreement, and we remain fully liable to the customer for its work.

7. Transfers outside the EEA

We process personal data within the European Economic Area, unless agreed otherwise with the customer. Where a service needs a party outside the EEA, for instance the chosen model provider, that happens only with an appropriate safeguard under Chapter V of the GDPR, such as an adequacy decision or standard contractual clauses, and that choice is recorded in the agreement.

8. Personal data breaches

If we discover a personal data breach affecting data we process for the customer, we notify the customer without undue delay. We state what we know about the nature of the breach, the data and people affected, the likely consequences and the measures we have taken or propose, and we add to that as we learn more.

Notifying the supervisory authority and the data subjects is the customer's role as controller. We give the help that is reasonably needed, and we do not report a breach to an authority on the customer's behalf unless the law requires us to.

9. Requests from data subjects

If we receive a request from someone about their personal data, for instance for access or erasure, we forward it to the customer without delay and do not answer it ourselves. Where needed we help the customer, with appropriate measures, to answer such requests within the legal deadlines, and with the obligations of Articles 32 to 36 GDPR, taking the nature of the processing into account.

10. Audits and accountability

On request we make available to the customer the information needed to demonstrate that these commitments are met. The customer may have compliance audited, itself or through an auditor it appoints, once a year or more often when there is reason to, with reasonable notice, under confidentiality and without access to other customers' data. Each party bears its own costs of such an audit.

11. Return and deletion

After the agreement ends we delete the personal data we process for the customer, or return it if the customer so chooses, and delete the copies. On request we confirm the deletion in writing. We keep only what Union or Dutch law requires us to keep, and only for as long as that duty lasts.

During the agreement the customer can delete findings, reports and other content in the portal itself, alongside the retention periods that run on their own.

12. Duration, precedence and law

This data processing agreement lasts as long as the agreement lasts, and after that for as long as we still hold personal data for the customer. Where this text and the agreement conflict, this text prevails as regards the processing of personal data. Liability follows the arrangement in the agreement.

This data processing agreement is governed by Dutch law. It is published in Dutch and in English; where the two versions differ, the Dutch text prevails. The date and version number at the top show the version in force, and we announce a new version to existing customers beforehand.

Questions about this agreement can go to contact@assistsec.nl.

Back to top