Annex: Sessions Data Processing Terms

Version 1.4 · November 2026

These Data Processing Terms are an annex to the Sessions Terms of Delivery and Use and serve as a data processing agreement within the meaning of Article 28 GDPR (Article 9.6 of those terms). If the Customer and Hart voor Projecten conclude a written data processing agreement based on a model of the Customer, that agreement prevails. This is an English translation; in case of any difference, the Dutch version prevails.

Article 1 Roles and subject matter

1.1 Terms defined in Article 1 of the Sessions Terms of Delivery and Use (the terms), such as Customer, facilitator, participant, session and progress file, have the same meaning here. Terms from the GDPR, such as personal data, processor and personal data breach, have the meaning given in the GDPR.

1.2 The Customer is the controller of the personal data that Hart voor Projecten processes when facilitators and participants use Sessions (Article 2). Hart voor Projecten is the processor of those data.

1.3 Hart voor Projecten is itself the controller of the data of the person ordering and the contact person (ordering, invoicing, contact). Those data are covered by the privacy policy of Hart voor Projecten, not by these Data Processing Terms.

1.4 Hart voor Projecten processes personal data only to provide Sessions as described in the Terms of Delivery and Use. It does not use them for its own purposes, does not sell them and does not use them to train AI models.

Article 2 Which data, of whom, for what purpose

Element	Content
Purpose	Enabling online sessions with a team: preparing, putting online, taking part, showing on the presentation screen and producing the results.
Nature	Storing, organising, displaying, passing on to the devices in the session, and deleting.
Data subjects	Facilitators, participants and persons mentioned in the content of a session, such as stakeholders in a project.
Data	The names that participants enter (a first name is enough); the content of the session (points, ideas, cards, proposals, actions, agreements), insofar as it contains personal data; a logo of the Customer; in the Goals-Efforts Network, an image for the vision; technical keys per session and per device; internet addresses to prevent misuse: in Sessions shortened and for at most 10 minutes, in the web server's error logs for at most 14 days.
Excluded	Special categories of personal data, personal data relating to criminal convictions and offences, citizen service numbers (BSN) and classified information. The Customer does not enter these (Article 7.5 of the terms). Sessions does not ask for email addresses or accounts of participants.
Duration	As long as Hart voor Projecten processes data in Sessions for the Customer. An online session is deleted 24 hours after it was put online or reopened, and never later than 7 days (Article 9.1 of the terms).

Article 3 Instructions and confidentiality

3.1 Hart voor Projecten processes the data only on documented instructions from the Customer, including with regard to transfers outside the EU. The terms, these Data Processing Terms and the use of Sessions by the Customer's facilitators constitute those instructions. The Customer gives any other instructions in writing.

3.2 If Hart voor Projecten considers that an instruction infringes the GDPR or other data protection rules, it informs the Customer immediately.

3.3 If Hart voor Projecten is required by law to disclose data, it informs the Customer in advance, unless the law prohibits this.

3.4 Only persons who need access for their work have access to the data: the administrators of Hart voor Projecten, the staff with the Sessions support role and, insofar as necessary for their task, the sub-processors in Annex A. They are all bound by confidentiality.

3.5 Hart voor Projecten does not look at the content of sessions, except where necessary for security or recovery (Article 9.7 of the terms).

Article 4 Security

4.1 Hart voor Projecten takes appropriate technical and organisational measures to secure the data, as required by Article 32 GDPR. Annex B lists the main ones.

4.2 Hart voor Projecten may adjust the measures, provided the level of security does not decrease.

4.3 Hart voor Projecten first tests a new version of Sessions in a separate acceptance environment before it goes to production.

Article 5 Sub-processors

5.1 The Customer consents to the sub-processors listed in Annex A.

5.2 If Hart voor Projecten wishes to add or replace a sub-processor, it notifies the Customer's contact person, or the privacy and security address the Customer has provided in writing, at least 30 days in advance. The Customer may object within that period, stating reasons.

5.3 If the parties cannot reach agreement, the Customer may return its start codes that are still new, in return for a refund of the order price.

5.4 Hart voor Projecten imposes on each sub-processor, by contract, the same data protection obligations as in these Data Processing Terms. It remains liable to the Customer for the performance of those obligations by its sub-processors, within the limits of Article 11.1.

Article 6 No transfers outside the EU

Hart voor Projecten and its sub-processors process the data within the European Union (Article 9.8 of the terms). Transfers outside the EU take place only with the Customer's prior written consent and with safeguards in accordance with Chapter V of the GDPR.

Article 7 Assistance and rights of data subjects

7.1 If Hart voor Projecten receives a request from a data subject, for example for access or erasure, it forwards the request to the Customer within five working days. It does not answer the request itself, unless the Customer asks it to.

7.2 Hart voor Projecten reasonably assists the Customer with requests from data subjects, with a data protection impact assessment (DPIA) and with a prior consultation of the Dutch Data Protection Authority. Much of this assistance is already covered by the security information for Sessions.

7.3 If the assistance takes more than 4 hours in a calendar year, Hart voor Projecten may charge the hours above that at its usual hourly rate, after providing a written estimate in advance. Assistance with a personal data breach caused by Hart voor Projecten or a sub-processor is free of charge.

Article 8 Personal data breaches

8.1 If Hart voor Projecten discovers a (suspected) personal data breach affecting the Customer's data, it reports this within 24 hours to the Customer's contact person, or to the privacy and security address the Customer has provided in writing.

8.2 The report contains what is known at that time:

- what happened and when;
- which data and approximately how many data subjects are affected;
- the likely consequences;
- the measures taken or to be taken;
- a contact person at Hart voor Projecten.

8.3 Hart voor Projecten supplements the report as soon as more is known, and assists the Customer with a notification to the Dutch Data Protection Authority and to data subjects. The Customer makes those notifications itself.

8.4 Hart voor Projecten records every personal data breach, with the facts, the consequences and the measures taken.

Article 9 Information and audits

9.1 On request, Hart voor Projecten provides the Customer with the information needed to demonstrate compliance with these Data Processing Terms. For this purpose it maintains an up-to-date security fact sheet.

9.2 The Customer may carry out an audit itself or have it carried out by an independent expert bound by confidentiality: as a rule at most once a year, and in addition after a personal data breach or at the request of a supervisory authority. The Customer announces the audit in writing at least 30 days in advance, or at least 5 working days in advance after a personal data breach.

9.3 An audit must not disrupt Sessions or other customers. A load test or penetration test on production takes place only by written agreement.

9.4 The Customer bears the costs of an audit. If the audit shows that Hart voor Projecten does not comply with these Data Processing Terms on a material point, Hart voor Projecten bears the costs and remedies the shortcoming as soon as possible.

9.5 Instead of an audit, Hart voor Projecten may provide a recent report by an independent expert, if the Customer reasonably considers it sufficient.

Article 10 Retention and deletion

10.1 Sessions deletes an online session with all its data 24 hours after it was put online or reopened. If Hart voor Projecten extends this period (Article 9.1 of the terms), it announces this in advance, and the period never exceeds 7 days. The facilitator can also delete a session earlier (Article 9.2 of the terms).

10.2 Sessions clears data on participants' devices when the session is over.

10.3 A session may remain in the encrypted backups for up to 14 days. After that, the backups are overwritten. Hart voor Projecten uses backups only to restore the service.

10.4 During the session, the facilitator can download the content and save it as a progress file; this counts as returning the data. Sessions then deletes the data in accordance with paragraph 1. Progress files and downloads are held by the Customer, not by Hart voor Projecten.

10.5 When processing ends, Hart voor Projecten retains no session data, except until the backups have been overwritten. On request, it confirms in writing that the data have been deleted.

Article 11 Liability, precedence and term

11.1 Liability between the parties is governed by Article 11 of the terms, including for damage caused by a breach of these Data Processing Terms or of the GDPR. This does not affect the rights of data subjects under Article 82 GDPR.

11.2 In case of conflict between these Data Processing Terms and the Terms of Delivery and Use, these Data Processing Terms prevail as far as the protection of personal data is concerned.

11.3 These Data Processing Terms apply as long as Hart voor Projecten processes data in Sessions for the Customer. Articles 3, 4, 8 and 10 continue to apply as long as data remain in backups.

11.4 Hart voor Projecten may change these Data Processing Terms in the manner described in Article 12.1 of the terms. A change that reduces the protection of the data applies only after the Customer's written agreement.

11.5 These Data Processing Terms are governed by Dutch law. Article 12.5 of the terms applies to disputes and Article 12.6 to translations.

Annex A Sub-processors

Party	What	Where
One.com Group AB (part of group.one), Carlsgatan 3, 211 20 Malmö, Sweden, company registration number 559205-2400	Hosting of the Sessions servers (production and acceptance)	Data centre in Copenhagen, Denmark
WebBuilds B.V. (Ploi), Nijkerk, the Netherlands, Chamber of Commerce 94117233	Server management: setting up, updating and monitoring, with technical access to the servers	The Netherlands and Germany (UpCloud, Amsterdam and Frankfurt)

Not a sub-processor:

- Microsoft 365 sends the emails from Sessions. These contain only data of the person ordering and the contact person, and no session content.
- Phare checks a health-check URL of Sessions; no personal data are involved.
- The backups are kept on a NAS owned by Hart voor Projecten in the Netherlands.

Annex B Security measures

Area	Measures
Access	Facilitators work with a start code, participants with the code or QR code of a single session; participants have no account. Each facilitator and each participant receives a random 128-bit key; the server stores only a SHA-256 hash and the key never appears in a web address. Administration only with two-factor authentication, with as few administrators as possible.

Misuse	Limits on guessing codes and on the number of new sessions per hour per internet address. For this purpose, Sessions keeps internet addresses in shortened form for at most 10 minutes; the web server's error logs keep them for at most 14 days.
Connection and browser	HTTPS only, with HSTS. A Content Security Policy: scripts, fonts and connections only from the site itself. No embedding in other sites, no third parties in the pages, no analytics or tracking cookies. Sessions sets only three cookies it needs to work, only for its own site and not readable by scripts in the page: hvps_access (the facilitator's start code, signed; until the end date of the code plus the week in which a session can be reopened, or until the browser closes if the administrator sets it that way), hvps_lead (which sessions the facilitator leads on this device, at most five, signed; 2 days) and hvps_hs (a check for a secure connection when redirecting to HTTPS; 30 seconds).
Data	An online session is deleted 24 hours after it was put online or reopened, never later than 7 days; the facilitator can delete it earlier. Progress files and downloads are created by the facilitator's browser; the server does not store them. No AI in Sessions.
Servers	Our own cloud servers at one.com in Copenhagen, Denmark (not shared hosting), managed with Ploi. SSH login only with a key, not as root. A firewall, automatic security updates, a daily restart, and file editing through WordPress switched off. A separate acceptance environment.
Backups and recovery	An encrypted backup every night, retrieved to a NAS owned by Hart voor Projecten at another location in the Netherlands, with RAID protection. Restoring is practised.
Monitoring	An external check every 5 minutes, and monitoring of the servers. Alerts go to the administrator.
Development	Automated tests for every version, an independent code review and a user test before a release. A new version goes to the acceptance environment first.