InContext
CONSULTANCY GROUP

Privacy Policy

InContext Consultancy B.V. & InContext Assesment & Development B.V.

1. Introduction

1.1. InContext Consultancy B.V., registered in Baarn and listed in the Chamber of Commerce under registration number: 32117178, and InContext Assessment & Development B.V., also registered in Baarn under registration number: 32085871, are organizational and consultancy firms providing corporate training and education, as well as gamified learning through the use of games & simulations (hereinafter referred to as 'InContext').

1.2. InContext engages in activities related to advising, coaching, guidance, and organizational training. In addition, InContext assists in the development, management, and trading of products to enhance the effectiveness of organizations and their personnel. It also provides services in the form of consultancy and advice.

1.3. In the course of its business operations, InContext processes personal data. It typically acts as a 'Processor' within the meaning of the General Data Protection Regulation (GDPR), but it also processes personal data as a 'Data Controller'. Within the EU AI Act we work with AI as both a ‘Provider’ and ‘Deployer’.

1.4. The processing of personal data by InContext relates, among other things, to the following categories:

1. Contacts of current and former Clients for sales, intakes, stakeholders, and invoicing (hereinafter: **'Clients'**);
2. Employees of Clients who come to us to participate in programs specially developed for their organization (hereinafter: **'Participants'**);
3. Prospective clients whom we actively or reactively approach for marketing purposes (hereinafter: **'Prospects'**);
4. Employees and former employees of InContext (hereinafter: **'Employees'**) and their designated contacts (hereinafter: **'Contacts'**);
5. Job applicants (hereinafter: **'Applicants'**);
6. Contacts of current and former Suppliers for primary processes and/or supporting products/services (hereinafter: **'Suppliers'**);
7. External personnel hired to handle workload peaks or due to specific expertise (hereinafter: **'Freelancers'**).

1.5. In this Privacy Statement, we explain:

- Which personal data we process concerning the categories as mentioned in Article 1.4 and in what manner;
- For what purposes we process this data and on what legal basis;
- What rights individuals in these categories have regarding the data we process about them;
- Who you can contact regarding this Privacy Statement.

2. What Personal Data Do We Process?

In the course of its business operations, InContext processes various personal data. Below is a general list of personal data processed in this context. The specific personal data processed depends on the specific group mentioned in 1.4 and the purpose for which they are processed. The purposes of processing can be found in section 3.

Personal data processed by InContext includes:

2.1. Name, address, and place of residence;
2.2. Date of birth and gender;
2.3. Email address and telephone number;
2.4. Bank account number (IBAN);
2.5. Citizen Service Number (BSN), identification number (and copy of identification), photo, CV;
2.6. Dietary preferences and/or injuries;
2.7. Certificate of Good Conduct (VOG) (upon specific request from our Clients, Employees/Freelancers may be asked to provide a VOG);
2.8. IP address;
2.9. Video/visual material during performances/interventions.

3. For What Purposes Do We Process This Data and on What Legal Basis?

The purposes for which personal data is processed by InContext are explicitly defined in advance. InContext does not process personal data for secondary purposes or purposes other than those for which the personal data was collected. Below is a list of purposes for which personal data is processed for each group, along with the legal basis.

Clients Personal Data: Name, Address, Place of Residence (NAW), Email Address, Telephone Number, and IBAN.	
Purpose	Legal Basis
Maintaining contact related to sales, intakes, stakeholders, and invoicing.	- Consent under Article 6(1)(a) GDPR - Performance of a contract under Article 6(1)(b) GDPR - Legitimate interest, namely the proper management of service provision under Article 6(1)(f) GDPR
Processing payments:	- Performance of a contract under Article 6(1)(b) GDPR - Legal obligation (tax record-keeping) under Article 6(1)(c) GDPR

Participants Personal Data to be processed at the request of the Client, such as: Name, Address, Date of Birth, Gender, Email Address, Telephone Number, Industry/Position, Dietary Preferences, Injuries, Personality Test, and Video/Visual Material during performances/interventions.	
Purpose	Legal Basis
Maintaining contact related to the workshops being attended.	- Consent under Article 6(1)(a) GDPR - Performance of a contract under Article 6(1)(b) GDPR - Legitimate interest, namely the proper management of service provision and meeting expectations regarding service quality under Article 6(1)(f) GDPR
Providing feedback to Participants, forming groups, assigning Participants, and matching them with Employees/Freelancers who guide them in the workshops being attended.	- Performance of a contract under Article 6(1)(b) GDPR - Legitimate interest, namely the proper management of service provision and meeting expectations regarding service quality under Article 6(1)(f) GDPR
Facilitating catering services based on dietary preferences.	- Performance of a contract under Article 6(1)(b) GDPR - Legitimate interest, namely the proper management of service provision and meeting expectations regarding service quality under Article 6(1)(f) GDPR
Collecting information about injuries to consider in case of physical components in workshops.	- Legitimate interest, namely the proper management of service provision and meeting expectations regarding service quality under Article 6(1)(f) GDPR
Granting access to our online environments using login credentials and passwords. Some of our online environments use personal data to function effectively.	- Performance of a contract under Article 6(1)(b) GDPR - Legitimate interest, namely the proper management of service provision and meeting expectations regarding service quality under Article 6(1)(f) GDPR
In the case of interventions / performances, InContext may capture images or videos for the purpose of providing a visual representation to the Participants. This data is not used for commercial purposes unless explicit consent has been requested and granted. Participants may upload or send photos or documents to InContext on their own initiative.	- Consent under Article 6(1)(a) GDPR

Prospects Personal Data: Name, Address, Gender, Email Address, Telephone Number, and Industry/Position.	
Purpose	Legal Basis
Actively or reactively contacting for commercial and marketing purposes, including sending newsletters and all requested content and their follow-up.	- Consent under Article 6(1)(a) GDPR - Legitimate interest, namely the proper management of service provision and meeting expectations regarding service quality under Article 6(1)(f) GDPR
Employees Personal Data: Name, Address, Date of Birth, Gender, Email Address (business and personal), Telephone Number (business and personal), IBAN, Citizen Service Number (BSN), Copy of Identity Document, Photo (for the website), Personality and Capacity Test Results, Certificate of Good Conduct (VOG), and Video/Visual Material during performances/interventions.	
Purpose	Legal Basis
Keeping records for internal administration, salary payments, and pension administration.	- Performance of a contract under Article 6(1)(b) GDPR - Legal obligation (tax record-keeping) under Article 6(1)(c) GDPR - Legitimate interest, namely the proper management of service provision and meeting expectations regarding service quality under Article 6(1)(f) GDPR
If Clients require it, we request our Employees to obtain a Certificate of Good Conduct (VOG) and provide it to the client.	- Performance of an obligation in the (data processing) agreement with the Client under Article 6(1)(b) GDPR

Applicants Personal Data: As part of the CV: Name and address, email address, telephone number, photo, personality and capacity test results, and work experience.	
Purpose	Legal Basis
Assessing the job application.	- Consent under Article 6(1)(a) GDPR - Legitimate interest, namely the recruitment of quality personnel under Article 6(1)(f) GDPR
To gain a comprehensive understanding of an individual's capabilities in a later stage of the job application process, we: - Administer a (Facet5) personality test. - Administer a capacity test. The test results are then discussed with the Applicant and, if the application is not pursued further, deleted from the server.	- Consent under Article 6(1)(a) GDPR - Legitimate interest, namely the recruitment of quality personnel under Article 6(1)(f) GDPR
Suppliers Personal Data: Name, Company Name, Job Title, Business Email Address, and Telephone Number	
Purpose	Legal Basis
Maintaining contact, including for procurement and invoicing.	- Performance of a contract under Article 6(1)(b) GDPR. - Legitimate interest, namely the proper management of service provision and meeting expectations regarding service quality under Article 6(1)(f) GDPR.
Processing payments.	- Performance of a contract under Article 6(1)(b) GDPR. - Legal obligation (tax record-keeping) under Article 6(1)(c) GDPR.
Contacts Personal Data: Name and telephone number.	
Purpose	Legal Basis
Informing or questioning an Employee's Contact in case of an emergency.	- Necessary for vital interests under Article 6(1)(d) GDPR

Freelancers Personal Data: Name, Company Name, Job Title, Business Email Address, Telephone Number, Certificate of Good Conduct (VOG), and Video/Visual Material during performances/interventions.	
Purpose	Legal Basis
Maintaining contact in connection with the execution of agreed-upon assignments.	- Performance of a contract under Article 6(1)(b) GDPR. - Legitimate interest, namely the proper management of service provision and meeting expectations regarding service quality under Article 6(1)(f) GDPR.
Processing payments.	- Performance of a contract under Article 6(1)(b) GDPR. - Legal obligation (tax record-keeping) under Article 6(1)(c) GDPR.
If Clients require it, we may request a Certificate of Good Conduct (VOG) and provide it to the client.	- Performance of an obligation in the (data processing) agreement with the Client under Article 6(1)(b) GDPR.

4. With Whom Can We Share Personal Data?

InContext uses the following sub-processors when processing its data:

Sub-processor	Location	Categories of data processed
Accensys	Woerden, Netherlands	IT infrastructure + mail server
BCS Den Bosch	Den Bosch, Netherlands	Employee payroll processing
Bouvy Advies	Blaricum, Netherlands	Pension administration + insurance for employees
DigitalOcean	Amsterdam, Netherlands	Hosting servers and databases where a part of our online tools runs. We use the servers/data centers of DigitalOcean, which is based in Amsterdam and certified ISO/IEC 27001:2013 & AICPA SOC 2 Type II.
Exact Netherlands B.V.	Delft, Netherlands	CRM and administrative data in the ERP system Exact Online

Forge (Laravel LLC)	North Carolina, United States	Configuration and setup of servers where our online tools run, see DigitalOcean and TransIP for more information about the servers.
Google Analytics	Dublin, Ireland	Service that provides us with insights into how our website is used.
HubSpot	Cambridge, United States	Placing cookies that collect data about website visitors and the opening of email messages sent by us.
Human Collective	Amsterdam, Netherlands	Facet5 personality tests
LinkedIn Insights Tag	Dublin, Ireland	LinkedIn browser cookie that collects IP addresses, timestamps, page events, and demographic information via LinkedIn.
Mollie	Amsterdam, Netherlands	All data processed by Mollie is guaranteed to be stored on Dutch servers. These servers are located in highly secure data centers, under the supervision of a specialized NOC team. Mollie complies with all guidelines for internet payment security established by the European Banking Authority. They also undergo continuous oversight by De Nederlandsche Bank (The Dutch Central Bank).
Postmark	Chicago, United States	Sending emails from our online tools.
Sitesmid.nl (Active Campaign)	Aldeboarn, Netherlands	Placing cookies that collect data about website visitors and the opening of email messages sent by us.
TransIP	Leiden, Netherlands	Hosting servers and databases where a part of our online tools runs. We use the servers/data centers of TransIP, which is based in Amsterdam and certified ISO/IEC 27001:2013 & AICPA SOC 2 Type II.
Vimeo	's Hertogenbosch, Netherlands	Hosting videos used in our online tools.
Woocommerce Ireland Limited	Dublin, Ireland	Processing order information when purchasing an online license via the website.

Data processing agreements have been concluded with the above-mentioned parties.

5. Cookies

We use cookies to enhance your experience on our site. In accordance with regulations, we are obligated to inform you about how our website uses cookies.

5.1. On our website

Cookies are small text files placed by websites on the computer or peripheral device you use to visit the website. Cookies collect information about the interaction with and usage of the website. Thanks to cookies, we can provide a tailored experience on our website.

5.2. In our applications

We use cookies in our applications only to track the active session of a Participant (so they don't need to log in again via tokens/codes if they lose connection).

5.3. General

All our cookies are 'first-party' and are used only within our own domain for the above-mentioned purposes. These cookies are encrypted and stored on the user's side (not in our system/database). Our standard cookie retention period is 2 hours after the last activity on the site.

6. How Do We Protect Your Personal Data?

InContext employs various technical and organizational measures to protect your personal data from destruction, loss, alteration, unauthorized disclosure, or unauthorized access. These measures include administrative, physical, and technological safeguards. Individuals working with us are bound by confidentiality and are required to adhere to our instructions aimed at ensuring the adequate protection of your data. With processors we engage, we enter into data processing agreements that guarantee adequate security and confidentiality.

To implement these measures, we follow a Security Plan, Continuity Plan, and an Exit Plan.

In accordance with the EU AI Act, we count as both a Deployer and Provider of AI systems. However, both our usage and creation of AI systems never involves (not anonymised) personal data of clients and/or participants.

- As a Deployer we make use of General Purpose AI (GPAI) systems to analyse and process data, but this never includes personal data as that will either be excluded or fully anonymised and untraceable to the respective person. This usage of AI is therefore within the category of ‘Minimal / No-Risk’.
- As a Provider we make IT systems that can make choices based on received data (e.g. a business simulation processing the result of a mock sale). These systems make minimal to no use of personal data (see specific descriptions below for more details per tool) and are designed in accordance with both the GDPR and the EU AI Act and are categorised as ‘Minimal / No-Risk’ systems.

7. Security Plan

Technical and organizational measures that InContext has taken to secure and maintain the security of personal data against loss, unauthorized access, alteration, or unlawful processing, as well as to ensure the (timely) availability of data.

a.) Measures to Ensure that Only Authorized Personnel Have Access to Personal Data for the Described Purposes

Named Accounts
InContext provides its employees and sub-processors with access through named accounts combined with a personal password. These accounts are granted access rights based on the job group to which the employee belongs. The use of these accounts is adequately logged, and these accounts only have access to personal data necessary for the respective person.

Password Policy
Passwords for all accounts meet a series of requirements to make them secure (and not easily guessable). Where possible, Two-Factor Authentication is used.

Personal Data (Participant Data) Provided by Clients
Only the InContext Project Desk department receives participant data from our clients. They are responsible for correctly applying privacy agreements/legislation to this data.

- Participant data is stored by the Project Desk department in a secured participant folder.
- Any communication with participants after a training is conducted via the Project Desk department.
- The Project Desk department may share participant information GDPR-compliant with facilitators and third parties if necessary.
- Facilitators are responsible for returning or destroying paper documents* with personal data used during an intervention.
- The Project Desk department securely destroys participant data, both digitally and in hard copy.

**Paper documents refer to attendance lists/participant lists, Facet5 and TeamScape reports, (copy) certificates.*

b.) Measures Regarding Data Storage and Device Security

Physical Security Measures of the Premises
InContext has secured its premises with multiple locks and alarms. Employees have access through keys and are instructed on how to activate and deactivate the alarm.

Loss/Theft/Data Leak of Devices
Employees are obligated to immediately report loss, potential data leaks, and/or theft to the Privacy Officer.

Device Encryption
Devices are remotely wiped in case of loss or theft:
- For Mac OS, FileVault2 is activated, which fully encrypts the hard disk and cannot be released without the recovery key or user password.
- For Windows, Bitlocker is activated, which fully encrypts the hard disk and can only be released with the automatically generated recovery key. This key changes with each new unlock request.

Data Retention Periods, Job Roles/Job Groups, and Their Processing – Online Tools
Privacy by Design: We collect as little information as possible; all personal information, such as names, is always optional. Our tools are accessible online via login codes, so no installation or (email) accounts are required for participants.

Table 1 lists the job roles and/or job groups that have access to specific personal data and indicates the processing they may perform regarding personal data.

Job Role/Group	(Category) Personal Data	Type of Processing
Project desk	Name and address details, date of birth and gender, email address and telephone number, dietary preferences and/or injuries, and video/image material during sessions/interventions.	Participant lists
Game leaders / hosts – Fizzinity & TeamUP game	To play Fizzinity or TeamUp, participants need to provide a self-selected name, and a team name is required.	Stored securely in our database. All answers provided during the game are deleted from the database within 60 days of the game date (and client-specific versions after 12 months). When a team is archived, all participant data and their answers are removed. Only the team name and score are retained for ranking purposes.
Game leaders / hosts – QT-platforms (Teamwork QT / Agile QT)	To play any of the games on the QT platforms, participants need to choose a name, this can optionally be their real name.	Stored securely in our database. All answers provided during the game are deleted from the database within 60 days of the game date.
Game leaders / hosts – TFI TeamFlowIndex & LinkXs Online game & Tegeltjes tool & Coffee&Co simulation & Awareness Assessment tool	No personal data is collected as it's played anonymously.	Stored securely in our database. All answers provided during the game are deleted from the database within 60 days of the game date.
Game leaders / hosts – Selfie360 tool	Optional: name and email address	Stored securely in our database. All optional participant data and answers provided while using the tool are deleted from the database within 60 days of the tool usage date.

Game leaders / hosts – Leave Your Mark app	Mandatory: password and email address. Optional: name and address details, date of birth and gender, email address, and telephone number.	Stored securely in our database. All participant account data is deleted 1 year after their last use: Data from other accounts (trainers & admins) will remain intact.
Administrators & Clients – Gooische Dogtag	Administrators: name, password and email address. Clients: mandatory: name, password and email address. Optional: address details, telephone number, information of registered pets including vet name and number	Stored securely in our database. Deleted upon request of client or administrators.
Game leaders / hosts – Ixplora (platform)	Optional: password and email address.	Stored securely in our database. All answers provided during the game are deleted from the database within 60 days of the game date. User accounts are deleted 1 year after their last activity.

8. Continuity Plan

Our measures to ensure the timely availability of Personal Data:

Requirement to Centrally Store Documents by Employees
InContext mandates its employees to store documents centrally on the server in designated client and participant folders. This ensures project continuity and reduces dependency on individual persons.

Backup Server
InContext utilizes an external cloud-based backup server. A copy of the server is created every night, ensuring data integrity in the event of a server interruption or crash.

9. Exit plan

The exit plan outlines how personal data, which we process on behalf of our clients, will be deleted when the relationship is terminated.

Transfer to the Client
InContext obliges its employees to store documents on the server in designated client and participant folders. In the event a client requests the transfer of personal data, InContext can promptly fulfill this request.

Destruction Actions and Documentation

- Participant lists are not retained for more than 4 weeks after the completion of an execution/intervention.
- Physical participant lists are destroyed using a secured paper container emptied by a specialized party.
- Digital participant lists are removed from the server by the Projectdesk department.
- Any email correspondence between our facilitators and participants is deleted annually before year-end. We also require our employees/freelancers to confirm the deletion in writing.

10. How Long Do We Retain Personal Data?

InContext's guiding principle regarding the retention of personal data is that data should not be kept longer than necessary. In determining retention periods, InContext considers the following criteria:

- Does the period follow from a legal obligation?
- What is the nature and sensitivity of the personal data?
- Does the removal of personal data affect the process negatively?
- Is there a difference in intrusion into the personal sphere between longer or shorter retention of personal data?
- What is the likelihood of unlawful data use?

Below is a non-exhaustive list of relevant retention periods for personal data processed by InContext:

10.1. We retain fiscal data for 7 years (legal obligation).
- This includes data such as general ledger, debtor and creditor administration, inventory administration, sales and purchase administration, and payroll administration.

10.2. Participant lists are not retained for more than 4 weeks after the completion of an execution/intervention.

10.3. Email correspondence between our facilitators and participants is deleted annually before year-end. We also expect our employees and freelancers to confirm the deletion.

10.4. Prospect data is retained for up to 5 years after the last contact. This includes website visits, email data, and responses to surveys and questionnaires.

11. Your Rights Regarding Your Personal Data

The legislation concerning the protection of personal data grants individuals the following rights with respect to their personal data:

I. The right to inquire whether personal data concerning them is being processed and, if so, to access that data.
II. The right to request rectification and erasure of that data.
III. The right to object to processing or request limitation of processing.
IV. The right to withdraw consent for processing if the processing is based on consent.
V. The right to receive or transfer data to an organization designated by the data subject, in a structured, commonly used, and machine-readable format.
VI. The right to file a complaint with a supervisory authority overseeing compliance with rules on the protection of personal data. In the Netherlands, this authority is the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) located in The Hague (www.autoriteitpersoonsgegevens.nl).

12. Contact Information

To exercise the rights described above, you can send an email to: privacyofficer@incontext.nl. You may also use this email address if you wish to file a complaint about how InContext has processed your personal data.

This privacy statement may be amended by InContext at any time. Therefore, we recommend checking the statement periodically for updates. If we make changes to this statement in the future, we will publish the amended statement on our website, indicating the date on which the changes take effect (https://incontext.nl/en/privacy-statement/).

Date of last change:	**20-10-2026**
Author:	**Bram Jonkers**
Details:	**Name:** Bram Jonkers **Function:** Lead Developer & Data Privacy Officer **E-mail:** privacyofficer@incontext.nl **Phone nr.:** +31 35 628 68 48

13. Attachment 1 – Privacy Intake Form – Tools

Here is a description of the process that a participant goes through when using one of our tools. This process is the same for Awareness Assessment, Cofee&Co, Fizzinity, Ixplora, Linkxs, TFI, TeamUP, and Selfie360. Any deviations from this standard process are explained at the bottom for each tool.

Flow for the facilitator and participant:

- Prior to a session with participants, the facilitator creates a session:
  - The facilitator goes to the website of the respective tool.
  - The facilitator logs in to the administrator portal of this tool.
    - This is done using an account name and password managed by InContext.
    - We assume facilitators from InContext already have access. If sessions are conducted in the future without our involvement, a (new) login account will be shared with selected staff.
    - This process does not require customer data.
  - The facilitator creates a new session, resulting in a set of login codes.
    - For your information, login codes are random combinations of letters and numbers, e.g., "6A0K43."
  - The facilitator shares the login codes with the participants during the session via screen sharing, the meeting tool's chat, and/or verbally.
    - If a session is conducted by a non-InContext staff member, the customer can use the above process to create a session themselves or request InContext staff to do it and send them the login codes via email.
- The participant's process is as follows:
  - The participant is invited to a session according to the customer's standard scheduling policy.
    - This session will also include an (InContext) facilitator.
  - During the session, the facilitator shares the tool's address along with the login code the participant should use.
    - This is done via screen sharing, the meeting tool's chat, and/or verbally.
    - Login codes are distributed randomly.
      - This distribution is prepared in a slide before the session to save time during a session.
    - In the case of Coffee&Co, Fizzinity and TeamUP, there is one login code shared by the entire group.
  - With this information, the participant can access the tool via their browser and log in by entering the code.
  - Afterward, the participant is logged in and ready to use the tool.

Tool-Specific Information:

For the Align and Quadrality tools, there is a slightly different process:

- Instead of the facilitator creating a set of login codes, they create a session with a specific name, e.g., "Teambuilding March 16."
- The facilitator shares this team name with the participants in the same way that login codes would be shared as described above.
- Participants log in by selecting their session from the list of active sessions after they have gone to the tool's address.
    - Typically, there is only one active session (visible). The only case where this is not the case is when parallel sessions are running simultaneously, in which case the correct session must be selected.

For the Ixplora tool, participants have the option to use an email address and password instead of an anonymous login code:

- Participants who indicate that they want a personal account receive an email invitation for their tool account before a session.
    - This requires a name, email address, and password.
    - Account data is retained for up to 1 year after the last account activity.
        - Can be deleted earlier upon request.
- Participants can log in at any (later) time to perform the following actions:
    - View and interact with all active sessions they are participating in.
    - Modify their login credentials (email/password/name).
    - Request deletion of their account.

For the TFI tool, IP addresses are also used:

- When a participant logs into the TFI environment, their IP address, in combination with their login code, is stored in the tool's database.
    - For information about the location of this database and more, refer to our previously completed privacy document.
- These data are automatically deleted after 6 months but can be deleted earlier upon request.
- This information is not processed or used within the application itself; it is stored purely for the following purposes:
    - When a participant reports issues with using the tool, the facilitator may inspect this database upon request to identify potential problems (e.g., multiple participants logging in with the same login code).
    - Data inspection is done manually; the data is never processed or shared with other parties.
        - Data inspection is carried out directly in the database itself; there is no printout/log of the data.
    - Data inspection can only be performed by the tool's administrator/developer; no one else has or will have access to this data.

Leave Your Mark

The Leave Your Mark (LYM) tool has a different process and data requirements. Here is an explanation:

Participant Process - LYM:

- Prior to using the tool, an InContext facilitator will create an account for the participant:
  - The facilitator goes to the Leave Your Mark website environment.
  - The facilitator logs into the administrator portal of the tool using their account.
  - The facilitator creates a new user account for the participant.
    - This requires a name, email address, and password.
    - Optionally, additional information such as department, phone number, address, LinkedIn profile, and an avatar can be added.
    - These accounts are deleted if they are inactive for more than a year.
- After this period, participating in a new course requires being invited again within the environment.
  - The participant receives an email with the login details for their account.
- Prior to a session with participants, an InContext facilitator will create the session:
  - The facilitator logs into the environment using the above method.
  - The facilitator creates a course within the environment.
    - A course consists of one or more surveys and documents.
    - For surveys, there is an option to make them anonymous, so results cannot be linked to participant accounts.
  - A course and all associated data are deleted by default after 1 year.
    - Data can be cleaned up earlier or kept longer upon request.
  - The facilitator adds existing participant accounts to the course (see above for how these accounts are created).
- For the participant, the process is as follows:
  - The participant receives an email with login details for their tool account (as mentioned above), even if the participant already has an existing account from a previous session.
  - With these details, the participant can access the tool via their browser and log in using their account.
  - After this, the participant is logged in and ready to use the tool. Within the environment, the participant will automatically see the course they have been invited to.
  - Within the session, the participant can take the following actions:
    - See fellow participants.
    - Access documents that are important for the course.
    - Upload documents to the course.
      - These documents can be made visible only to the facilitator and the participant or to all other participants within the course.
      - This data is retained as long as the course is valid (1 year by default, see above).
    - Complete surveys made available by the facilitator.
  - The participant can log in at any later time to:
    - View and interact with all active courses they are participating in.
    - Modify their login details (email/password).
    - Modify or provide (optional) personal information.

        - Required: name.
        - Optional: department, phone number, address, LinkedIn profile, and an avatar.
    - The InContext facilitator can log in at any time to:
        - Modify their account as per the participant actions above.
        - Add and remove participants (as described above).
        - Add, manage, and remove courses.
        - Add, manage, and remove documents relevant to a course.
        - View course results.
            - This data is anonymized if that setting is enabled

Summary of Required Data within LYM:

- User account per participant:
    - Required: name and email.
    - Optional: department, phone number, address, LinkedIn profile, and an avatar.
    - Data retained for 1 year after the last account activity.
    - Can be deleted upon request earlier.
- Session data per session:
    - List of participant user accounts.
    - Answers to surveys and/or documents uploaded by participants.
    - Data retained for 1 year after session creation.
    - Can be deleted upon request earlier

Gooische Dogtag:

Just like LYM, Gooische Dogtag makes use of user accounts that consist of a name, email address and password. Data of these accounts is processed the same way as the LYM application.

Gooische Dogtag does not contain paticipants but does contain clients. The type of data saved about a client is documented in paragraph 7. Data of clients is collected, processed and deleted in the same way as participant data in the LYM application.