

Privacy and cookie statement of InTense B.V.
v. 2021

1. Who is InTense B.V.?

InTense B.V. (“InTense”) - a Dutch limited liability company with its seat in Zwolle, The Netherlands, registered at the Chamber of Commerce under KvK-number 05078336 - is a training and coaching institute that operates worldwide in the field of safety, health and security.

InTense is a leading global expert in safety culture change. InTense focuses on the most important asset of its clients and change agent: the employees of the clients. People are important, also the processing of personal data. For this reason, InTense created this privacy policy to ensure that any data processing is compliant with the applicable data protection laws and regulations.

InTense processes the personal data of those visiting the website, people working for InTense and those who participate in any InTense safety and health program or any InTense services (Consulting, Engagement, Follow-up and Measurement) with care. Personal data are carefully and secured processed and safeguarded. In Tense complies with the provisions of the EU General Data Protection Regulation (“GDPR”) and its national implementing and supplementing legislation, as well as any other future applicable legislation.

2. Importance of this Privacy and Cookies Policy

InTense is committed to ensure the privacy and safety of Personal data.

This policy provides general information about how In Tense collects and processes Personal data, how they can be used and to whom they can be disclosed.

3. Which Personal data does In Tense collect and process?

In Tense collects and processes information from natural persons (“Personal data”), when it regards:

- Its employees, freelance facilitators and content managers/trainers and Country managers (name, address, telephone number, bank account, BSN, salary or fees, VAT or tax number or trade register number (whatever applies), agreed benefits, copy ID, medical issues, information regarding experience and education/CV and appraisals, worked hours, travel history, travels for trainings etc.) to execute the agreement InTense concluded with them;
- Job applicants, or candidates for an employment agreement or for a freelance agreement/assignment (name, address, telephone number, information regarding experience and education/CV and if applicable assessment information);
- Individual persons with whom In Tense is engaged in doing business (in case of legal entities the name of the legal representative and contact details and function/role within organization);
- Participants in the programs of In Tense (names and if certificates are issued also date of birth, presence in the training, scores/results, questions, emails) to execute the training as per agreement with the employer of the participants;
- Persons to whom InTense provides services such as Consulting, Engagement, Follow-up and Measurement (names, contact details, if applicable payment details, information necessary to provide tailored services);
- Persons who participate in online programs of InTense (name, contact details, position, if



applicable the persons' manager/leadership team, feedback on leadership and safety culture, contact details of colleagues where applicable);



- Persons hired by InTense for their specific expertise (name, contact details, expertise, payment details)
- Other data that may be collected are transactions data (such as which InTense products and services were purchased), technical data (such as IP Addresses, for online programs login data, technology on devices used to access the website or the online program), profile data (such as preferences, feedback and survey responses), and marketing and communications data.

A total overview of data that are collected/processed is registered in the data processing register in which InTense records the processing of Personal data per business department.

Where possible InTense will pseudomize or anonymize personal data to protect them.

InTense does not collect, process or store special categories of personal information such as race, membership of a trade union, religion, sexual preferences, etc., except for medical information of their employees/facilitators and content managers or those who work for InTense on a freelance basis because of health and safety reasons.

For visitors of the website: See cookie statement in article 12.

4. Data controller

InTense is data controller and therefore responsible for the collection, processing, storage and security of any data as meant in the GDPR.

5. How personal information is collected

InTense uses different methods to collect data dependent on the interaction and the InTense programs and services that were offered or provided:

- Direct interactions by corresponding with InTense by regular mail, e-mail, phone or otherwise through social media;
- Purchasing an InTense product or service;
- Applying for a job or other position;
- Following an online program and creating an account for this program in order to be able to login;
- Marketing requests;
- Enter a survey;
- Contact InTense for feedback and/or coaching
- Automated technologies and interactions.

6. How personal data are used/legal ground for processing

InTense processes Personal data and uses them for the following purposes:

- Employee/salary administration;
- Tax/finance administration;
- To provide health, safety and security programs and related services;

- For responding on queries and to provide relevant information on its business/on health, safety & security;
- For diagnosing problems with online programs;
- For communication purposes
- For certification purposes
- Where it is necessary for InTense’s legitimate interests and the interests of the individual whose data are processed and fundamental rights do not override those interests;
- Where InTense needs to comply with legal obligations;

The legal ground for these processing activities are:

- To execute agreements such as employment agreements or sales agreements for InTense Programs and related services and to be able to provide the purchased program and/or related services;
- InTense processes Personal data when a natural person applies for a job (“Candidate”). InTense has a legitimate interest to process this information to process the job application and may disclose such information for example to take up a reference when InTense obtained consent of the Candidate;
- InTense also processes Personal data to fulfil legal obligations such as tax obligations or its obligations as Employer or processes data to do its business, such as Personal data of participants of an InTense Program or related services to execute the agreement that InTense entered with for example employers of the participants.

The Personal data that are collected are adequate, relevant and limited to what is necessary in relation to the purposes.

InTense does not sell any information or Personal data, or offer any direct marketing services of third parties. InTense does not share any information or Personal data with third parties without prior written consent of the natural person involved, unless required by law and/or required by official Authorities such as the police and the Court of Justice or unless necessary for the execution of the agreements as mentioned above. InTense may use personal data for marketing communications or when information is requested.

InTense does not use extensive technologies to collect, process, follow and store private information of natural persons. When private persons interact with the website, InTense does not use anonymous identifiers to identify the visitors of the website. However for the working of the website, InTense uses essential cookies as mentioned in article 12.

7. Data processors

InTense may use third parties for certain services that need the processing of Personal data, such as

- Accountant/ payroll processors,
- Insurers,
- Pension providers,
- Travel agencies,
- IT providers, such as the company hosting our website

All data processors of In Tense have to comply with the GDPR (or if applicable local data protection laws and regulations) and additional rules and regulations concerning data protection and will only process Personal data when necessary to execute agreements.

8. How long does In Tense stores Personal data?

- All information within In Tense is stored for a definite period of time (as long as necessary) or for a period of seven years after termination of an agreement as required by the Tax laws and regulations.
- Only Personal data necessary for the execution of agreements or to fulfil legal obligations or for which a legitimate interest of In Tense exists is recorded and stored.
- Personal data will be destroyed or deleted if no longer necessary.

9. How does In Tense protect Personal data?

In Tense implemented the necessary administrative, technical and organizational measures in order to ensure a level of security that is appropriate for the specific risks that InTense identified. InTense protects Personal data against destruction, loss, alteration, unauthorized disclosure or access to Personal data transmitted, stored or otherwise processed by applying technologies such as pseudomization. Some information is only accessible for a limited amount of person (Authorized Persons).

Amongst others the following measures are taken:

- Logical access control: Access to laptops and to files is only allowed for authorized persons (mainly restricted to certain Employees and/or contractors), and controlled and secured against unauthorized access to IT-systems by usernames and passwords;
- Financial/banking data are restricted to people who need to have access to this data to perform their jobs, and in order to access the application source code a user/password authentication is required;
- Software protection: All data stored on servers are protected against viruses by virus scanners and by regular backups;
- InTense does not use the public cloud to store and backup her information, but uses a private cloud and hired a contractor for security of her IT systems.

10. Rights that someone has over his/her data and how to exercise rights

A person whose personal data are processed ("data subject") has the following rights:

- Right to information and right to access Personal data: a data subject may request at any time more information on the processing activities and the Personal data that InTense is keeping from this person.
- Right to rectification and right to access Personal data: a data subject has the right to obtain from InTense without undue delay the rectification or completion of any inaccurate or incomplete Personal data.
- Right to deletion of Personal data (right to be forgotten): Deletion of Personal data is allowed to request when processing is no longer necessary for achieving the purposes for which they were collected or otherwise processed; or when processing was based on the

data subject's consent and the data subject decided to withdraw this consent; or when there are reasonable grounds to object to processing of the Personal data; or when Personal data have been unlawfully processed; or when Personal data have to be erased in compliance with a legal obligation. InTense refuses to delete Personal data by way of an exception for compliance with a legal obligation or for the establishment exercise or defence of legal claims or for certification reasons (in case a participant to an InTense program will be certified).

- Right to restriction of processing: a data subject can ask InTense to restrict the processing of the Personal data in the following situations: when the accuracy of the Personal data is contested for a period enabling InTense to verify this accuracy, when the processing appears to be unlawful and the data subject requests InTense restriction of use in stead of deletion, pending verification whether the legitimate interests of InTense override the interests of the data subject in the framework of an objection.
- Right to object the processing of Personal data: When processing is based on legitimate interest, the data subject has the right to object to the processing of Personal data. InTense will in that case no longer process the Personal data unless InTense has compelling legitimate grounds to do so or because such a processing is necessary in the establishment, exercise or defence of a legal claim or for tax reasons.
- Right to data portability: a data subject has the right to receive all personal data in case the processing is carried out by automated means or in case the processing is based on consent or on the necessity for the performance of a contract.

InTense will respond to any legitimate request of a data subject within one month. Occasionally it may take InTense longer than a month if the request is particularly complex or if the data subject makes a number of requests. In that case InTense will notify this person and keep him/her updated.

11. International transfers of personal data – for EU residents

InTense may transfer personal data outside the European Economic Area (EEA), but only to a country or territory that ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. This is a measure for those who are EU residents.

12. Cookies

Cookies are small pieces of data that are temporarily stored on a computer or mobile device via the browser of the visitor of a website. InTense uses a plugin that includes only essential cookies, being the CookieYes GDPR Cookie Consent Notice Plugin. This plugin uses the following cookies:

- viewed_cookie_policy – is the primary cookie that records the user consent for the usage of the cookies upon “accept” and “reject”. It does not track any personal data and is set only upon user action (accept or reject).
- CookieLawInfo-checkbox-necessary/cookieLawInfo-checkbox-non-necessary – records the default button state of the responding category. It works only in coordination with the primary cookie.

∨

- CookieLawInfoConsent – records the default button state of the corresponding category & the status of CCPA. It works only in coordination with the primary cookie.

∨

The provider of the plug-in is: <https://www.webtoffee.com/>

All cookies are stored for 11 months.

11. Data breach

InTense has a data breach protocol that will be followed in case any security incident is detected in the IT system and/or a data breach is suspected.

12. Changes

InTense reserves the right to amend this policy from time to time. The amendments will apply as of the moment that the amendment is published.

13. Complaints/questions/remarks

Complaints, questions or remarks can be send to InTense: info@in-tense.nl

The contact person for data protection within In Tense is:

Mr Eddie van der Wereld

Zwartewaterallee 25

8032 DZ Zwolle

The Netherlands

In case a data subject is not satisfied with the complaint handling of InTense, the data subject has the right to submit its complaint to the Data Protection Authority of the Netherlands.