DATA PROTECTION POLICY

1. Introduction

In the course of conducting business, INNA Group companies collect, use and store personal data about its employees, customers, business partners and other individuals. INNA has a responsibility to ensure that it handles this information responsibly to protect individuals' personal data.

This Data Protection Policy is designed to help INNA comply with the European General Data Protection Regulation (GDPR). INNA also ensures to comply with all applicable national legislation wherever it operates.

This Policy applies to all employees belonging to INNA group of companies ("INNA") and Boards of Directors of INNA companies. This Policy applies to all companies and operating countries of INNA. This Policy and related guidelines and work practices are designed to ensure that also all employees are aware of and comply with their obligation to protect the privacy of all individuals and the security of such individual's Personal Data. INNA has also issued internal instructions for its employees regarding data protection. In case of any discrepancies between this Policy and other internal instructions, this Policy prevails.

In any data protection matters, the primary contact person for data subjects is the locally designated role or function responsible for the day-to-day handling of data protection and compliance matters.

2. Data protection concepts

Controller	A controller is the party that determines the purposes and means of processing personal data.
Data subject	A data subject is an individual whose personal data is being processed.
Joint controllers	Sometimes two or more organizations might work together to decide why and how personal data is processed. This is referred to as "joint controllership" and should be governed by a joint controller agreement that determines the controllers' respective responsibilities.
Personal data	Personal data means any information relating to an identified or identifiable natural person (“data subject”). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier, or one or more factors specific to the individual’s physical, physiological, genetic, mental, economic, cultural, or social identity.
Processing	Processing means the handling of personal data, including collecting, using, adapting, transmitting, storing, and erasing personal data.

Processor	A "processor" is an organization that processes personal data solely on behalf of, and under the instructions of, a controller. Controller-processor relationships must be governed by a data processing agreement ("DPA").
Special categories of personal data	Some categories of personal data are generally prohibited from processing, unless specific derogations apply. Such categories are sometimes referred to as 'sensitive data' and include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

3. Data protection principles

Personal data processing must be planned in advance. INNA's data protection policy, guidelines, and data protection legislation must be followed already when planning the collection of data. The party responsible for the project or change in the processing must ensure in a documented manner that the data subject's privacy is appropriately protected, taking into account the personal data to be collected and the need for protection. INNA must comply with each of the principles described below.

Fairness and lawfulness

INNA must only process personal data on certain specific legal grounds. The processing must be based on either legislation, contract, INNA's legitimate interest, or another lawful basis for processing according to the data protection regulation mentioned in section 4. The processing must take into account the legitimate expectations of the data subject and any elevated risks to the privacy of data subjects.

Data minimization and purpose limitation

Personal Data may only be collected for specified, explicit and legitimate purposes that are compatible with the original reason for collecting the personal data, and only to the extent necessary for achieving that purpose. INNA's systems and procedures should be designed to uphold these principles.

Accuracy

INNA must ensure that it takes active steps to ensure that the personal data it has on its files is accurate and uptodate. Incorrect and outdated information should not be processed.

Integrity and confidentiality

INNA must implement appropriate technical and organizational measures to achieve an adequate level of security for its personal data processing activities. INNA must also ensure it maintains the integrity of its personal data processing activities, taking steps to prevent accidental data loss. In doing so, it will take into consideration relevant state-of-the-art technology; the costs of implementation; and the nature, scope, context, and purposes of the processing.

Transparency

INNA must ensure it is transparent with data subjects about what personal data it processes, for which purposes, on which legal grounds, and how the processing is performed. Transparency is implemented through various means, including providing information about processing activities on INNA's webpages. All data subjects shall be provided with information about what personal data is being processed and how the personal data is being processed. INNA provides transparent and clear information to data subjects on how to exercise their rights as data subjects

Storage limitation

INNA must have a systematic approach to maintain records to comply with applicable laws and regulations, to protect its interests, and for business continuity. Personal data, however, should not be stored for unnecessarily lengthy periods or without an overriding interest given the risk this poses to the privacy of individuals.

INNA is developing comprehensive retention policies for personal data based on legal requirements and separately defined purposes. The company will implement processes to ensure compliance with retention periods; whereby personal data may only be used for as long as it is necessary for the purpose of processing. When the purpose ends, data will be destroyed and/or transferred to archives, unless legislation requires specific storage obligations.

INNA commits to establishing procedures for the timely removal of data that has become unnecessary and outdated, and to implementing planned processes for the secure destruction of personal data in accordance with data protection requirements.

Accountability

The accountability principle requires INNA to take responsibility for and demonstrate compliance with the data protection principles described above. As a data controller, INNA is obligated to implement appropriate technical and organizational measures to fulfill the accountability requirements.

Accountability requires appropriate documentation. To meet this obligation, INNA must prepare and maintain an internal record of processing activities, keep external privacy notices up to date, document personal data breaches, and carry out data protection impact assessments (DPIAs) when required. INNA is also committed to providing its personnel with data protection training and instructions to maintain sufficient competence and, where necessary, demonstrate that such training has been provided.

Data security and confidentiality

INNA shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, considering the nature, scope, context and purposes of the processing. Such measures may include, where relevant, staff instructions and training, confidentiality obligations, physical security, access controls, information system security, logging and monitoring, encryption, pseudonymization or anonymization, audits and regular review of security measures.

Access to systems and databases containing personal data shall be restricted to authorized persons who have a documented need for such access in connection with their work duties. Access rights shall be granted, reviewed and removed in accordance with applicable access management procedures.

4. Legal basis for processing personal data

INNA can only process personal data if it identifies specific legal grounds permitting such processing. As a data controller, INNA must always be aware of which lawful basis it is relying upon when carrying out a processing activity. Personal data cannot be processed without a lawful basis for processing. More restrictive conditions apply to special categories of personal data, as explained below.

Legal obligation (Article 6(1)(c) of the GDPR)	INNA may process personal data to the extent necessary to fulfil a legal obligation (e.g., Know Your Customer (KYC) obligations).
Performance of a contract (Article 6(1)(b) of the GDPR)	The processing is necessary for INNA to fulfil its obligations under a contract that it has entered with the data subject (e.g., retaining bank account details to pay a salary under an employment contract), or to

	take steps at the request of the data subject prior to entering into a contract.
Legitimate interests (Article 6(1)(f) of the GDPR)	INNA may process personal data where such processing is necessary for the purposes of legitimate interests pursued by INNA or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (e.g., maintaining a database of customer or business partner information, or collecting emergency contact details of employees). The legitimate interests must be specific and justified when weighed against the fundamental rights of the data subjects, including their right to privacy. INNA ensures this balance by conducting a legitimate interest assessment.
Consent (Article 6(1)(a) of the GDPR)	The data subject has agreed to the processing. Consent must be freely given, specific, informed, and unambiguous. Data subjects must be informed that they can withdraw their consent at any time.
Other	Although rarely applicable, there are additional grounds on which personal data may be processed, namely the protection of the vital interests of the data subject or the performance of tasks carried out in the public interest.

Legal basis for processing special categories of personal data

INNA does not, as a rule, process special categories of personal data unless required by law or strictly necessary for defined purposes. When such data must be processed, INNA applies enhanced safeguards, including strict access controls, purpose limitation and secure handling. Where the processing may pose a high risk to individuals, a Data Protection Impact Assessment (DPIA) will be carried out.

Direct marketing

When conducting direct marketing activities, INNA must ensure that there is a lawful basis for the processing of personal data, that data subjects receive sufficient information about the processing, and that data subjects are able to exercise their rights, including the right to object/opt-out, right of access, right to rectification, erasure, and restriction. INNA complies with local regulations and market practices in its direct marketing activities.

5. Data subject's rights and information to data subjects

The GDPR gives data subjects several rights as regards the processing of their personal data. INNA must observe those rights and ensure that adequate procedures are in place to accommodate data subjects.

Enquiries by data subjects to exercise their rights must be dealt with swiftly and INNA must act on an enquiry within one month after it was received. In certain cases, longer time may be necessary and justified. INNA is under a duty to take all reasonable actions to check the identity of the data subject. An enquiry received by any employee of INNA should always be immediately forwarded to INNA's locally designated role or function responsible for the day-to-day handling of data protection and compliance matters for further action, according to INNA's internal instructions.

Right to information	Data subjects have the right to information when personal data is collected. INNA's companies have published internal privacy notices on their respective company intranets, describing how employee personal data is processed. Third parties are informed via privacy notices available on INNA web pages.
Right of access	Data subjects have the right to receive confirmation of whether their personal data are being processed by INNA and, if so, to gain access to their personal data by receiving a copy of the personal data being processed (often referred to as a data subject access request).
Right to rectification, erasure ('right to be forgotten'), and restriction	Data subjects have the right to have inaccurate or incomplete personal data concerning them rectified or supplemented without undue delay. In some cases, data subjects have the right to request erasure of their personal data ('right to be forgotten'). Examples include when consent is the legal basis for processing and the data subject withdraws their consent, or when the data subject demonstrates that the data are no longer necessary for the purposes for which they were collected. In certain circumstances, data subjects can demand that the processing of their personal data be restricted. This means that INNA may only store the personal data and not process them further without the data subject's consent. The right to restriction applies, among other things, when the data subject considers that the data is inaccurate and has requested rectification. The data subject can then request that the processing of the personal data be restricted while their accuracy is verified. The individual must be informed when the restriction ends.
Right to object	Data subjects have the right to object to INNA's processing of personal data when the processing is based on INNA's legitimate interests. When a data subject objects, INNA must cease processing unless it can demonstrate compelling legitimate grounds that override the interests, rights, and freedoms of the data subject. When personal data are processed for direct marketing purposes, data subjects have the absolute right to object at any time to processing of their personal data for such purposes, and INNA must cease all direct marketing processing upon receiving such objection.
Right to data portability	Data subjects have the right to receive personal data they have provided to INNA and to transmit those data to another controller (the right to data portability) where the processing is based on consent or contract and is carried out by automated means. The personal data must be provided in a structured, commonly used, and machine-readable format. Where technically feasible, the data subject may request that the personal data be transmitted directly to another controller. This right applies only to personal data that the data subject has actively provided to INNA. INNA will assess each data portability request individually. If the request is manifestly unfounded or excessive, INNA may refuse the request or charge a reasonable fee for its implementation. If INNA refuses a request, the data subject will be notified within one month of receipt of the request, including the

reasons for refusal and information about the possibility of lodging a complaint with the competent supervisory authority.

INNA is not obligated to accommodate data subject requests in certain circumstances, including where such requests would conflict with INNA's legal obligations, where the requests are manifestly unfounded or excessive, or where applicable law provides specific exemptions to data subject rights.

6. Record of processing activities

In accordance with the GDPR, INNA shall maintain a record of all processing activities involving personal data carried out within the INNA group. The record must contain certain mandatory information, including a description of the categories of personal data processed, the legal basis for processing, and the purposes of the processing. Upon request, the record must be made available to the relevant data protection authority.

7. Data breach procedure

A personal data breach is a security incident that results in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data that INNA transmits, stores, or otherwise processes (e.g., as a result of hacking, sending a confidential email to the wrong recipient, or a system error that causes data to be lost). If a personal data breach occurs that may result in a risk to the rights and freedoms of data subjects, INNA must report this to the relevant data protection authority as required by applicable legislation no later than 72 hours after the breach is discovered. When personal data breach is likely to result in a high risk to a data subject, INNA shall also communicate the data breach to the affected individuals without undue delay.

Please note that INNA may also need to notify other third parties of a data breach, such as insurance companies and relevant parties in accordance with contractual obligations. INNA has established internal instructions for the data breach process. Every employee is obligated to comply with these internal instructions for the data breach process.

8. Use of data processors and international data transfers

A written agreement must be concluded between the data controller and processor regarding the processing of personal data. INNA provides property management services to housing companies and, in this connection, processes personal data relating to residents. Depending on the specific arrangement, INNA may act either as a data processor on behalf of the client company or as an independent data controller, with the client company acting as a separate data controller.

INNA acts as a data controller when processing personal data for its own business purposes, such as when processing contact information of representatives from client companies and prospective client companies. When outsourcing its operations, INNA also engages subcontractors who may process personal data on its behalf.

Examples of outsourcing personal data processing include purchasing data processing services (such as CRM or HR systems) from a service provider. When a subcontractor processes personal data on INNA's instructions, the parties must enter into a written data processing agreement that specifies how the service provider (processor) processes personal data on behalf of and under the instructions of INNA. INNA's responsibility as a data controller for the security of data processing remains even when processing is outsourced to a subcontractor. The subcontractor has no right to process data for its own

purposes and may only process data within the scope of the assignment and in accordance with INNA's instructions.

INNA has prepared a standard appendix on personal data processing, which it endeavors to use in agreements concluded with subcontractors. The content and scope of the data processing agreement depend on the type of personal data being processed, the scope of processing, and the associated risk assessment.

Key elements of data processing agreements:

• The role of each contracting party (data controller, data processor)
• Categories of personal data and categories of data subjects
• Processing activities and specific tasks to be performed by the processor and the processor's responsibilities
• Tasks and responsibilities that remain with the data controller
• Processor's obligation to notify the controller of planned changes regarding subcontractors and to obtain authorization for such changes
• Processor's commitment to ensure that personnel authorized to process personal data are subject to confidentiality obligations
• Level of data security and related technical and organizational measures and responsibilities
• Deletion and/or return of personal data upon termination of the agreement
• The processor's obligation to provide the data controller with all information necessary to demonstrate compliance with data processing obligations
• The data controller's or its authorized representative's right to conduct data protection audits regarding the processor's operations
• A written agreement must be made between the data controller and processor regarding personal data processing. The processor may only process personal data on behalf of INNA in accordance with the data processing agreement.

When applicable, INNA must ensure adequate protection measures when transferring personal data outside of the EU/EEA. This can be done through one of the following ways:

Option 1 *Transfers on the basis of an adequacy decision*	Personal data can be transferred outside of the EU/EEA if the country or entity to which it is being transferred is deemed to have adequate protection by the EU Commission.
Option 2 *Appropriate safeguards*	If Option 1 is not available, INNA must enter into an agreement with the non-EU/EEA party using the EU Standard Contractual Clauses for international transfers (**"SCC"**). Prior to entering the SCC, INNA must examine the circumstances surrounding the transfer to the non-EU/EEA recipient and assess the adequacy of personal data protection in the importing country. This assessment must be documented in a transfer impact assessment **("TIA").** If the TIA reveals that the importing non-EU/EEA country does not provide adequate protection for personal data, supplementary measures (legal, technical, or organizational) must be implemented in addition to the SCC.
Option 3 *Specific derogations*	If Options 1 or 2 are not available, personal data can be transferred outside of the EU/EEA if a special legal exception (or "derogation" as it is called) applies. Examples of such specific derogations are:

(a) explicit consent from the data subject after the data subject has been informed of the possible risks of such transfer due to the absence of an adequacy decision and appropriate safeguards;

(b) transfer is necessary for the performance of a contract between the data subject and the data controller, or the implementation of pre-contractual measures taken at the data subject's request;

(c) transfer is necessary for the establishment, exercise, or defense of legal claims.

9. Privacy by design and privacy by default

INNA applies the principles of privacy by design and privacy by default in all its operations. Before implementing IT systems and procedures, appropriate technical and organizational measures must be implemented to meet GDPR requirements and protect the rights of data subjects. Data protection requirements are identified and considered in all processes, services, systems, and operations and documented as part of the project plan ("privacy by design"). Personal data must not be processed unnecessarily or more extensively than necessary for the intended purpose. This obligation covers the amount of personal data, retention periods, the scope of processing, and data accessibility. Data must not be disclosed unlawfully or without a legal basis to an unlimited number of persons ("privacy by default").

10. Data protection impact assessments

INNA will conduct DPIA before engaging in data processing activities that are likely to result in high risks to the rights of freedoms of individuals (e.g. installing camera surveillance in office areas). A data protection impact assessment is a process to help identify and minimize the data protection risks of a processing activity. Please contact INNA's locally designated role or function responsible for the day-to-day handling of data protection and compliance matters for more information and/or instructions.

11. Personal data on social media platforms

When INNA maintains accounts on social media platforms (e.g., Facebook, Instagram, Twitter, YouTube) for communication and marketing purposes, it acts as a data controller for the processing of personal data on its own accounts to the extent that INNA controls such publications and has the ability to modify or delete such information.

When INNA uses tools provided by social media platforms (e.g., marketing or analytics tools), joint controllership may exist between INNA and the social media platform provider.
To the extent that INNA acts as a data controller, it must ensure that its processing activities comply with the requirements set out in this Policy.

12. Use of cookies and other tracking methods on websites and apps

As a website or app owner, INNA acts as a data controller and is responsible for providing users with appropriate information and obtaining consent before using cookies that collect, store, or process personal data.

When INNA uses cookies on its websites or apps, it must maintain and provide a cookie policy. The cookie policy must be readily accessible on the website or app and must inform users of the purposes for which cookies are used (e.g., marketing, statistical, or functional cookies), how personal data collected about the user is processed, and whether such information is shared with third parties.
In addition to maintaining a cookie policy, websites and apps must display a banner or pop-up form that informs users of INNA's cookie policy and requests user consent (or allows rejection) for the use of cookies. Consent must be specific for each purpose, and users must provide separate consent for each specific use of cookies.

13. Roles and Responsibilities

INNA Group's CEO is responsible for ensuring that INNA complies with applicable legislation in all group company operations. This includes compliance with data protection legislation and other regulations. The CEO's responsibility is to ensure that data protection management and governance is assigned within the organization.

INNA's management team members are responsible for ensuring compliance with data protection legislation and its integration into business operations, as well as for ensuring the implementation of data protection requirements and data subjects' rights within their areas of responsibility and for allocating sufficient resources.

Management is responsible for ensuring that employees receive the necessary data protection training to perform their duties in a compliant and secure manner.
INNA's management team also commits to supporting the locally designated role or function responsible for the day-to-day handling of data protection and compliance matters.

INNA ensures that data protection procedures and policies are maintained and kept up to date.

All employees and supervisors shall be responsible for the lawful processing of personal data. Employees shall receive ongoing data protection training and guidance on information security practices. Each employee shall follow the employer's instructions in the processing of personal data and the implementation of data protection. Employees shall identify and manage data protection risks related to their own services and data and shall comply with privacy-by-design principles. Each employee shall report any risks or deficiencies they observe related to data protection or the rights of data subjects to the data protection contact person or their own supervisor.

INNA's stakeholders include customers, partners, affiliated companies within the group, suppliers, subcontractors and any other relevant third parties. Data protection within the supply chain shall be governed by applicable contractual arrangements and data protection legislation.
INNA shall ensure that all parties have sufficient information and understanding of data protection issues. The Management Team shall be responsible for overseeing compliance with this Policy.If you have any questions about the content of this Data Protection Policy or its application, please contact the locally designated role or function responsible for the day-to-day handling of data protection and compliance matters.

14. Training

INNA provides general training for its management and employees on data protection compliance. Training is provided on an ongoing basis. Each employee is responsible for following INNA's instructions regarding the processing of personal data and implementing data protection requirements.

15. Reporting concerns and consequences of violation

Each employee has an obligation to report any risks or deficiencies related to data protection or data subjects' rights that they observe to the locally designated role or function handling the day-to-day implementation of data protection and compliance activities. This reporting obligation particularly applies to personal data breaches, which must be immediately reported upon discovery.

If you discover a violation of this Policy or any other INNA's policy, you must report it to the CEO, head of business unit, or your supervisor. Concerns may also be raised through INNA's whistleblowing system, which is available on INNA's country-specific websites. INNA will not tolerate any attempt to take adverse action against an employee for reporting genuine concern regarding suspected wrongdoing. INNA does not tolerate any illegal or unethical behavior. Violations of this Data Protection Policy are likely to damage INNA's brand and reputation. Failure to comply with this Data Protection Policy is taken seriously and may result in disciplinary action appropriate to the violation, including, but not limited to, termination of the employment relationship.

16. Review and follow up

Compliance with this Data Protection Policy by all INNA Group companies and employees will be monitored and reviewed on an ongoing basis, as appropriate, including through ongoing assessments of data protection practices. Any relevant matters identified are followed up internally.

Effective date	Version	Change description
25.5.2018	v1	original
20. December 2023	v2	updated
1st of September 2025	v3	updated
18th June 2026	v4	updated