infomineo
VALUE ADDED BUSINESS SERVICES

Data Privacy Policy

Document Management Information

Document Title: Data Privacy Policy

Document Status: Final

Document Publication History:
(All revisions made to this document must be listed in chronological order)

Version	Date	Author(s)	Remark
2.0	July 16	Achraf El Allam	Version update

Version History:

Version	Page	Date	Description of Change
2.0	All	July 16	Version update
1.0	All	May 18	Document Creation

1. Objective

As part of its responsibility, Infomineo is committed to international compliance with data protection laws. This Data Protection Policy applies worldwide to Infomineo and is based on globally accepted, basic principles on data protection. Ensuring data protection is the foundation of trustworthy business relationships and the reputation of Infomineo as an attractive employer or partner. The Data Protection Policy provides one of the necessary framework conditions for cross-border data transmission. It ensures the adequate level of data protection prescribed by the GDPR (General Data Protection Regulation) and the national laws (Morocco, namely Act 09-08) for cross-border data transmission, including in countries that do not yet have adequate data protection laws.

2. Scope

This policy aims at the protection of privacy to personal data processing when the person responsible for processing—being either an individual or a legal entity—is established on Moroccan territory or in EU countries.
This policy applies where we are acting as a Data Controller with respect to the personal data of employees or users of our Services; in other words, where we determine the purposes and means of the processing of that personal data. It also applies to Infomineo website, as well as other interaction (e.g. customer support conversations, user surveys and interviews etc.) you may have with Infomineo.

3. Responsibility

The Management are responsible for data processing in their area of responsibility. Therefore, they are required to ensure that the legal requirements, and those contained in the Data Protection Policy, for data protection are met. Management staff are responsible for ensuring that organizational, HR, and technical measures are in place so that any data processing is carried out in accordance with data protection.

4. Abbreviations/Definition

- **Data** is anonymized if personal identity can never be traced by anyone, or if the personal identity could be recreated only with an unreasonable amount of time, expense and labor.
- **Consent** is the voluntary, legally binding agreement to data processing.
- **Data subject** under this Data Privacy Policy is any natural person whose data can be processed.
- **Processing personal data** means any process, with or without the use of automated systems, to collect, store, organize, retain, modify, query, use, forward, transmit, disseminate or combine and compare data. This also includes disposing of, deleting and blocking data and data storage media.

- **Third parties** are anyone apart from the data subject and the Data Controller. Transmission is all disclosure of protected data by the responsible entity to third parties.
- **Highly sensitive data** is data about racial and ethnic origin, political opinions, religious or philosophical beliefs, union membership or the health and sexual life of the data subject. Under national law, further data categories can be considered highly sensitive or the content of the data categories can be structured differently.

5. Personal data protection principles

- **Fairness and lawfulness**; When processing personal data, the individual rights of the data subjects must be protected. Personal data must be collected and processed in a legal and fair manner.
- **Restriction to a specific purpose;** Personal data can be processed only for the purpose that was defined before the data was collected. Subsequent changes to the purpose are only possible to a limited extent and require substantiation.
- **Transparency;** The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be aware of, or informed of:
  - the identity of the Data Controller
  - the purpose of data processing
  - third parties or categories of third parties to whom the data might be transmitted.
- **Data reduction and data economy;** Before processing personal data, you must determine whether and to what extent the processing of personal data is necessary in order to achieve the purpose for which it is undertaken. Where the purpose allows and where the expense involved is in proportion with the goal being pursued, anonymized or statistical data must be used. Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by national law.
- **Deletion;** Personal data that is no longer needed after the expiration of legal or business process-related periods must be deleted. There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the corporate archive has evaluated the data to determine whether it must be retained for historical purposes.

- **Factual accuracy**; **up-to-dateness of data;** Personal data on file must be correct, complete, and – if necessary – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.
- **Confidentiality and data security;** Personal data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.

6. Reliability of data processing

Collecting, processing and using personal data is permitted only under the following legal bases. One of these legal bases is also required if the purpose of collecting, processing and using the personal data is to be changed from the original purpose.

1) Customer and partner data

a. **Data processing for a contractual relationship**; Personal data of the relevant prospects, customers and partners can be processed to establish, execute and terminate a contract. This also includes advisory services for the partner under the contract if this is related to the contractual purpose. Prior to a contract – during the contract initiation phase – personal data can be processed to prepare bids or purchase orders or to fulfill other requests of the prospect that relate to contract conclusion. Prospects can be contacted during the contract preparation process using the information that they have provided. Any restrictions requested by the prospects must be complied with.

b. **Data processing for advertising purposes**; If the data subject contacts Infomineo to request information (e.g. request to receive information), data processing to meet this request is permitted. Customer loyalty or advertising measures are subject to further legal requirements. Personal data can be processed for advertising purposes or market and opinion research, provided that this is consistent with the purpose for which the data was originally collected. The data subject must be informed about the use of his/her data for advertising purposes. If data is collected only for advertising purposes, the disclosure from the data subject is voluntary. The data subject shall be informed that providing data for this purpose is voluntary. When communicating with the data subject, consent shall be obtained from him/her to process the data for advertising purposes. When giving consent, the data subject should be given a choice among available forms of contact such as regular mail,

e-mail and phone. If the data subject refuses the use of his/her data for advertising purposes, it can no longer be used for these purposes and must be blocked from use for these purposes. Any other restrictions from specific countries regarding the use of data for advertising purposes must be observed.

c. **Consent to data processing Data** can be processed following consent by the data subject. Before giving consent, the data subject must be informed in accordance with Data Protection Policy principles. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone conversations, consent can be given verbally. The granting of consent must be documented.

d. **Data processing pursuant to legal authorization**; The processing of personal data is also permitted if national legislation requests, requires or allows this. The type and extent of data processing must be necessary for the legally authorized data processing activity, and must comply with the relevant statutory provisions. Reliability of data processing Collecting, processing and using personal data is permitted only under the following legal bases. One of these legal bases is also required if the purpose of collecting, processing and using the personal data is to be changed from the original purpose.

e. **Data processing pursuant to legitimate interest**; Personal data can also be processed if it is necessary for a legitimate interest of Infomineo. Legitimate interests are generally of a legal (e.g. collection of outstanding receivables) or commercial nature (e.g. avoiding breaches of contract). Personal data may not be processed for the purposes of a legitimate interest if, in individual cases, there is evidence that the interests of the data subject merit protection, and that this takes precedence. Before data is processed, it is necessary to determine whether there are interests that merit protection.

f. **Processing of highly sensitive data**; Highly sensitive personal data can be processed only if the law requires this or the data subject has given express consent. This data can also be processed if it is mandatory for asserting, exercising or defending legal claims regarding the data subject. If there are plans to process highly sensitive data.

g. **Automated individual decisions;** Automated processing of personal data that is used to evaluate certain aspects cannot be the sole basis for decisions that have negative legal consequences or could significantly impair the data subject. The data subject must be informed of the facts and results of automated individual decisions and the possibility to

respond. To avoid erroneous decisions, a test and plausibility check must be made by an employee.

h. **User data and internet;** If personal data is collected, processed and used on websites or in apps, the data subjects must be informed of this in a privacy statement and, if applicable, information about cookies. The privacy statement and any cookie information must be integrated so that it is easy to identify, directly accessible and consistently available for the data subjects. If use profiles (tracking) are created to evaluate the use of websites and apps, the data subjects must always be informed accordingly in the privacy statement. Personal tracking may only be effected if it is permitted under national law or upon consent of the data subject. If tracking uses a pseudonym, the data subject should be given the chance to opt out in the privacy statement. If websites or apps can access personal data in an area restricted to registered users, the identification and authentication of the data subject must offer sufficient protection during access.

2) Employee data

a. **Data processing for the employment relationship**; In employment relationships, personal data can be processed if needed to initiate, carry out and terminate the employment agreement. When initiating an employment relationship, the applicants' personal data can be processed. If the candidate is rejected, his/her data must be deleted in observance of the required retention period, unless the applicant has agreed to remain on file for a future selection process. Consent is also needed to use the data for further application processes or before sharing the application with other third parties. In the existing employment relationship, data processing must always relate to the purpose of the employment agreement if none of the following circumstances for authorized data processing apply. If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the corresponding national laws must be observed. In cases of doubt, consent must be obtained from the data subject. There must be legal authorization to process personal data that is related to the employment relationship but was not originally part of performance of the employment agreement. This can include legal requirements, collective regulations with employee representatives, consent of the employee, or the legitimate interest of the company.

b. **Data processing pursuant to legal authorization**; The processing of personal employee data is also permitted if national legislation requests, requires or authorizes this. The type

and extent of data processing must be necessary for the legally authorized data processing activity, and must comply with the relevant statutory provisions. If there is some legal flexibility, the interests of the employee that merit protection must be taken into consideration.

c. **Collective agreements on data processing;** If a data processing activity exceeds the purposes of fulfilling a contract, it may be permissible if authorized through a collective agreement. Collective agreements are pay scale agreements or agreements between employers and employee representatives, within the scope allowed under the relevant employment law. The agreements must cover the specific purpose of the intended data processing activity, and must be drawn up within the parameters of national data protection legislation.

d. **Consent to data processing;** Employee data can be processed upon consent of the person concerned. Declarations of consent must be submitted voluntarily. Involuntary consent is void. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In certain circumstances, consent may be given verbally, in which case it must be properly documented. In the event of informed, voluntary provision of data by the relevant party, consent can be assumed if national laws do not require express consent. Before giving consent, the data subject must be informed in accordance with Data Protection Policy principles.

e. **Data processing pursuant to legitimate interest;** Personal data can also be processed if it is necessary to enforce a legitimate interest of Infomineo. Legitimate interests are generally of a legal (e.g. filing, enforcing or defending against legal claims) or financial (e.g. valuation of companies) nature. Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the employee merit protection. Before data is processed, it must be determined whether there are interests that merit protection. Control measures that require processing of employee data can be taken only if there is a legal obligation to do so or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. The justified interests of the company in performing the control measure (e.g. compliance with legal provisions and internal company rules) must be weighed against any interests meriting protection that the employee affected by the measure may have in its exclusion, and cannot be performed unless appropriate. The legitimate interest of the company and

any interests of the employee meriting protection must be identified and documented before any measures are taken.

f. **Processing of highly sensitive data**; Highly sensitive personal data can be processed only under certain conditions. Highly sensitive data is data about racial and ethnic origin, political beliefs, religious or philosophical beliefs, union membership, and the health and sexual life of the data subject. Under national law, further data categories can be considered highly sensitive or the content of the data categories can be filled out differently. The processing must be expressly permitted or prescribed under national law.

g. **Automated decisions**; If personal data is processed automatically as part of the employment relationship, and specific personal details are evaluated (e.g. as part of personnel selection or the evaluation of skills profiles), this automatic processing cannot be the sole basis for decisions that would have negative consequences or significant problems for the affected employee. To avoid erroneous decisions, the automated process must ensure that a natural person evaluates the content of the situation, and that this evaluation is the basis for the decision. The data subject must also be informed of the facts and results of automated individual decisions and the possibility to respond.

h. **Telecommunications and internet**; Telephone equipment, e-mail addresses, intranet and internet along with internal social networks are provided by the company primarily for work-related assignments. They are a tool and a company resource. They can be used within the applicable legal regulations and internal company policies. In the event of authorized use for private purposes, the laws on secrecy of telecommunications and the relevant national telecommunication laws must be observed if applicable. There will be no general monitoring of telephone and e-mail communications or intranet/ internet use. To defend against attacks on the IT infrastructure or individual users, protective measures can be implemented for the connections to Infomineo network that block technically harmful content or that analyze the attack patterns. For security reasons, the use of telephone equipment, e-mail addresses, the intranet/internet and internal social networks can be logged for a temporary period. Evaluations of this data from a specific person can be made only in a concrete, justified case of suspected violations of laws or policies of Infomineo. The evaluations can be conducted only by investigating departments while ensuring that the principle of proportionality is met. The relevant national laws must be observed in the same manner as Infomineo regulations.

7. Transmission of personal data

Transmission of personal data to recipients outside or inside Infomineo is subject to the authorization requirements for processing personal data. The data recipient must be required to use the data only for the defined purposes. In the event that data is transmitted to a recipient outside Infomineo to a third country this country must agree to maintain a data protection level equivalent to this Data Protection Policy. This does not apply if transmission is based on a legal obligation. If data is transmitted by a third party to a Infomineo, it must be ensured that the data can be used for the intended purpose.

8. Rights of the data subject

Every data subject has the following rights. Their assertion is to be handled immediately by the responsible unit and cannot pose any disadvantage to the data subject.

a. The data subject may request information on which personal data relating to him/her has been stored, how the data was collected, and for what purpose. If there are further rights to view the employer's documents (e.g. personnel file) for the employment relationship under the relevant employment laws, these will remain unaffected.
b. If personal data is transmitted to third parties, information must be given about the identity of the recipient or the categories of recipients.
c. If personal data is incorrect or incomplete, the data subject can demand that it be corrected or supplemented.
d. The data subject can object to the processing of his or her data for purposes of advertising or market/opinion research. The data must be blocked from these types of use.
e. The data subject may request his/her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.
f. The data subject generally has a right to object to his/her data being processed, and this must be considered if the protection of his/her interests takes precedence over the interest of the data controller owing to a particular personal situation. This does not apply if a legal provision requires the data to be processed.

9. Confidentiality of processing

Personal data is subject to data secrecy. Any unauthorized collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that he/she has not been

authorized to carry out as part of his/her legitimate duties is unauthorized. The “need to know” principle applies. Employees may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities. Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way. Managers must inform their employees at the start of the employment relationship about the obligation to protect data secrecy. This obligation shall remain in force even after employment has ended.

10. Processing security

Personal data must be safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to protect personal data must be defined and implemented. These measures must be based on the state of the art, the risks of processing, and the need to protect the data. The responsible department can consult with its Information Security Officer (ISO) and data protection coordinator. The technical and organizational measures for protecting personal data are part of Corporate Information Security management and must be adjusted continuously to the technical developments and organizational changes.

11. Data protection control

Compliance with the Data Protection Policy and the applicable data protection laws is checked regularly with data protection audits and other controls. The performance of these controls is the responsibility of the data protection coordinators, and other company units with audit rights or external auditors hired. The results of the data protection controls must be reported to managing partners. Infomineo’s Board must be informed of the primary results as part of the related reporting duties. On request, the results of data protection controls will be made available to the responsible data protection authority. The responsible data protection authority can perform its own controls of compliance with the regulations of this Policy, as permitted under national law.

12. Data protection incidents

All employees must inform their manager and data protection coordinator immediately about cases of violations against this Data Protection Policy or other regulations on the protection of personal data. The

manager responsible for the function or the unit is required to inform the responsible data protection coordinator immediately about data protection incidents. In cases of improper transmission of personal data to third parties, improper access by third parties to personal data, or loss of personal data the required company reports (Information Security Incident Management) must be made immediately so that any reporting duties under national law can be complied with.

13. Register of activities

AREAS OF ACTIVITY	TEXT LAW	REFERENCES	DEFINITION
STAFF MANAGEMENT DOCUMENTATION	LABOUR CODE	Article 373	**Chapter II: Payment of wages** The Payroll must be kept by the employer for at least two years after its closure. Accounting, tabulating and computer documents or other controls that replace the Payroll must be kept for at least two years after their adoption
	ARCHIVES ACT No. 69-99 Dahir No. 1-07-167 kaada 1428 (30 November 2007)	Article 17	Period of thirty years, after which public records are freely communicated is increased to: One-hundred years after the date of birth of the person for documents containing personal medical information and personnel files
ACCOUNTING DOCUMENTATION	COMMERCIAL CODE	Articles 26 and 105 of the Commercial Code	**Section I: Accounting requirements** **III - Conservation of accounting documents** Under the provisions of the Commercial Code and the last paragraph of Article 26 and Article 105 companies are required must keep for ten years from the closing date of the exercise of their attachment, all supporting documents have been the basis of accounting findings
	CIRCULAR No. 716 NOTE ON THE BOOK OF TAX PROCEDURES	Article II	**RETENTION OF DOCUMENTS** Pursuant to the provisions of Article 2 of the LPF, taxpayers as well as natural and legal persons responsible for the withholding of tax at source (IR / wage income and capital income, IS or IR on raw materials perceived by businesses ...) are necessarily required to hold for ten years, at the place where they are taxed, the accounting records and supporting documentation used to determine the tax base and revenue

	CORPORATE TAX	**Law No. 24-86 establishing corporate tax Article 33**	**Conservation and audits of accounting documents** Companies are required to keep for 10 years where they are imposed, double sales invoices or receipts, the receipts for expenses and investments and the necessary fiscal control accounting records, including books on which transactions have been recorded, the inventory book, detailed inventories if they are not fully copied on this book and the journal and records of customers and suppliers.
	OBLIGATIONS AND CONTRACTS DAHIR	**Code of Obligations and Contracts (DOC) Art 387, Art 375, Art 383**	**Article 387:** Any action arising out of an obligation are prescriptes fifteen years, with the exceptions in Articles 388 and 389 and those determined by the law in individual cases **Article 375:** The parties may, by special agreements, extend the limitation period beyond five years fixed by law **Article 383:** When the prescription is validly terminated, the time until the act interrupting does not count the effects of prescription and a new limitation period starts from the moment the act interrupting stopped its effect.
		Code of Obligations and Contracts (DOC) Art 769	**Article 769:** The architect or engineer and the contractor charged directly by the master are responsible when, within ten years from the completion of the building or structure in which they conducted or performed the work, the work collapses, in whole or in part, or present a clear danger of collapse, default materials, the defect in construction or through the ground. The architect who has not directed the work is only liable for defects of his plan. The ten-year period begins to run from the date of receipt of the work. The action must be brought within thirty days from the day has verified the fact giving rise to the guarantee; it is not accepted after this period

		Law No. 53-05 (Nov. 30, 2007) promulgating the Law on the electronic exchange of legal data	**Article 471.1:** "The written electronically on the same probative force as the written paper. The electronic document is admissible in evidence as well as writing on paper, provided that can be duly identified the person who issued it and it is established and maintained under conditions that ensure the integrity "
LITIGATION DOCUMENTATION	**CIVIL CODE PROCEDURE**	**Article 428**	According to Article 428 of the CPC, "judicial decisions are likely to be executed for thirty years from the date they were made; this period has expired, they are outdated. Any beneficiary of a court that wants to continue execution has the right to obtain a shipping enforceable and as simple expeditions there has sentenced ".

PERSONAL DATA PROTECTION	**ACT 09-08 Relative to the protection of individuals with regard to the processing of personal data** **Personal data**	**Article 24 of the Constitution**	Article 24 of the Constitution: Everyone has the right to protect his privacy ... Private communications in any form whatsoever, are secret. Justice alone may authorize, under the conditions and in the manner prescribed by law, access to their content, total or partial disclosure or invocation at the expense of anyone ... Treatment of personal data commenced after February 23, 2009, date of entry into force of the 09-08 law, must comply without delay with the provisions of the law. Treatment of personal data started before 23 February 2009, date of entry into force of the 09-08 law, must comply with the provisions of the Act no later than 15 November 2012.

Regulation of electrical installations	**NF C 15-100 regulation of fixed electrical installations**	**NF C 15-100**	NF C 15-100 vouches for the protection of the facility and the people and the comfort of management, use and scalability of the electrical installation.
Minimum technical requirements for video surveillance systems	**Reference APSAD R82: video surveillance**	**APSAD R82**	This reference defines the minimum technical requirements for CCTV systems with implanted inside or outside cameras. It provides guidance to design, install and maintain CCTV systems in security applications
Minimum technical requirements for the design, installation and maintenance of automatic fire detection systems	**APSAD R7 automatic fire detection rule**	**APSAD R7**	Rule APSAD R7 defines the minimum technical requirements for the design, installation and maintenance of these systems in all types of sites or buildings. It takes into account the requirements of European Insurance Committee and the development of European standards.
Minimum technical requirements for alarm systems	**NF A2P certification for alarm systems**	**The NF A2P standard**	NFA2P brand is official recognition that distinguishes materials protection against intrusion and against the fire which, by their resistance, ensure enhanced security.