FZ-DPPP - Data Privacy and Protection Policy

Document Control	Doc. Type: **Policy**	IMS Code: FZ-DPPP	Version: **1.1**	Effective Date: 03 Nov 2025	Owner: **IMS**	Classification: **PUBLIC**

Introduction

As part of its corporate responsibility, Facilization is committed to compliance with national and international data protection laws. This Data Privacy and Protection Policy is based on globally accepted, sound principles of data protection. Ensuring data protection is the foundation of creating and maintaining trustworthy business relationships, protecting customer interest as well as the reputation of Facilization.

The Data Privacy and Protection Policy provides one of the necessary framework conditions for cross-border data transmission among our subsidiaries. It ensures the adequate level of data protection prescribed by the European Union Data Protection Directive, the General Data Protection Regulation (GDPR), as well as the national laws for cross-border data transmission including countries that do not yet have adequate data protection laws.

This Data Privacy and Protection Policy applies to both Facilization Shpk. registered in Albania and its fully owned subsidiary Facilization Limited registered in Malta including all respective employees. The Data Protection policy extends to all processing of Personal Data.

This Data Protection policy comprises internationally accepted data privacy principles including GDPR without replacing the existing national laws. It supplements national data privacy laws.

Definitions AND Principles for processing Personal Data

Definitions

- 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 labour.
- Consent is the voluntary, legally binding agreement to data processing.
- Data Protection Incidents are all events where there is justified suspicion that personal data is being illegally captured, collected, modified, copied, transmitted or used. This can pertain to actions by third parties or employees.

- Data subject under this Data Protection Policy is any natural person whose data can be processed. In some countries, legal entities can be data subject as well.
- 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. Moreover, data that relates to a crime can often be processed only under special requirements.
- Personal data is all information about certain or definable natural persons. A person is defined for instance if the personal relationship can be determined using a combination of information with even incidental additional knowledge.
- 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.
- Processing personal data is required if the permitted purpose or justified interest could not be achieved without the personal data, or only with exceptionally high expense.
- Data Controller is the legally independent company whose business activity initiates the relevant processing measure.
- 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.
- Third countries under the Data Protection policy are all nations outside the European Union/EEA. This does not include countries with a data protection level that is considered sufficient by the EU commission

Principles for processing Personal Data

1. Fairness & 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.

2. Restriction to a specific purpose

Personal Data must 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 requires substantiation.

3. 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.

4. Data Reduction & 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 the national law and GDPR.

5. 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, data must remain on file until the interests that merit protection have been clarified legally, or the corporate archive has evaluated to determine whether it must be retained for historical purposes.

6. Factual accuracy and updated 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. Data subject has the right to access and update his data thru a request to the Data Protection officer.

7. 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.

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.

Customer and Partner Data

C.1. Data processing during sales activities with prospects

Personal data of the relevant prospects, customers and partners can be processed in order 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 provided by the other contracting entity is processed to prepare bids, purchase orders, and agreements or to fulfil other requests of the prospect or customer related to sales activities. Prospects can be contacted during the contract preparation process using

the information that they have provided. Any restrictions requested by the prospects must be applied.

C.2. Data processing for advertising purposes

If the data subject contacts Facilization to request information (e.g. request to receive information material about a product), 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, 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.3. Consent to data processing

Data can be processed following consent by the data subject. Before giving consent, the data subject must be informed of this Data Privacy and Protection Policy. The declaration of consent must be obtained in writing or electronically for the purposes of documentation.

C.4. 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.

C.5. Data processing pursuant to legitimate interest

Personal data can also be processed if it is necessary for a legitimate interest of Facilization. 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.

C.6. 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, the Data Protection Officer must be informed in advance.

C.7. 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.

C.8. User Data and Internet

If personal data is collected, processed and used on websites and 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 user profiles (tracking) are created to evaluate the use of websites and apps, the data subject must always be informed accordingly in the privacy statement. Personal tracking may only be effected if it is permitted under national law or upon the 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.

C.9. Third-Party Disclosure

Facilization does not sell, trade, or otherwise transfer to outside parties your Personal Information.

Employee data

D.1. 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 applicant’s 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 group companies.

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 have to be observed along with the requirements of the GDPR. In cases of doubt, consent must be obtained from the data subjects.

There must be legal authorization to process personal data that is related to the employment relationship but was not originally part of the 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.

D.2. 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.

D.3. Collective agreements on data processing

If a data processing activity exceeds the purpose 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 GDPR.

D.4. 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 provisions 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 IV.3.of this Data Protection Policy.

D.5. Data Processing pursuant to legitimate interest

Personal data can also be processed if it is necessary to enforce a legitimate interest of Facilization. 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 interests of the company and any interests of the employee meriting protection must be identified and documented before any measures are taken. Moreover, any additional requirements under national law (e.g. rights of co-determination for the employee representatives and information rights of the data subjects) must be taken into account.

D.6. 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. Moreover, data that relates to a crime can often be processed only under special requirements under national law.

The processing must be expressly permitted or prescribed under national law. Additionally, processing can be permitted if it is necessary for the responsible authority to fulfil its rights and duties in the area of employment law. The employee can also expressly consent to processing.

If there are plans to process highly sensitive data, the Data Protection officer must be informed in advance.

D.7. 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 personal 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.

D.8. Telecommunication 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 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 relevant national and international laws must be observed if applicable.

To defend against attacks on the IT infrastructure or individual users, protective measures can be implemented for the connections to the Facilization network that block technically harmful content or that analysis the attack patterns. There will be no general monitoring of telephone and e-mail communications or internet/intranet use. For security reasons, the use of telephone equipment, e-mail addresses, the internet/intranet 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 violation of laws or policies of Facilization. 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 the GDPR regulations.

Transmission of Personal Data

Transmission of Personal Data to recipients outside or inside the Facilization 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 the data is transmitted to a recipient outside Facilization to a third country, the party in this country to whom data is being transmitted must agree to maintain a data protection level equivalent to this Data Privacy and Protection policy. This does not apply if transmission is based on a legal obligation.

If data is transmitted by a third country to Facilization, it must be ensured that the data can be used for the intended purpose.

If personal data is transferred from a group company with its registered office in the European Union/European Economic Area to a group company with its registered office outside of the European Economic Area (third country), the company importing the data is obligated to cooperate with any enquiries made by the relevant supervisory authority in the country in which the party exporting the data has its registered office, and to comply with any observations made by the supervisory authority with regard to the processing of the transmitted data.

In the event that a data subject claims that this Data Privacy and Protection Policy has been breached by the group company located in a third country that is importing the data, the group company located in the European Economic Area that is exporting the data undertakes to support the party concerned, whose data was collected in the European Economic area, in establishing the facts of the matter and also asserting his/her rights in accordance with this policy against the group company importing the data. In addition the data subject is also entitled to assert his or her rights against the group company exporting the data. In the event of claims of a violation, the company exporting the data must document to the data subject that the company importing the data in a third country (in the event that the data is further processed after receipt) did not violate this Data Privacy and Protection Policy.

In the case of personal data being transmitted from a group company located in the European Economic Area to a group company located in a third country, the data controller transmitting the data shall be held liable for any violations of this policy committed by the group company located in a third country with regard to the data subject whose data was collected in the European Economic Area, as if the violation had been committed by the Data Controller transmitting the data.

Contract Data Processing

Data processing on behalf means that a provider is hired to process personal data, without being assigned responsibility for the related business process. In these cases, an agreement on Data Processing on behalf must be concluded with external providers and among companies owned by Facilization. The client retains full responsibility for correct performance of data processing. The providers can process personal data only as per the instructions from the client. When issuing the order, the following requirements must be complied with; the department placing the order must ensure that they are met.

1. The provider must be chosen based on its ability to cover the required technical and organizational protective measures.

2. The order must be placed in writing. The instructions on data processing and the responsibilities of the client and provider must be documented.

3. The contractual standards for data protection provided by the Data Protection Officer must be considered.

4. Before Data processing begins, the client must be confident that the provider will comply with the duties. A provider can document its compliance with data security requirements in particular by presenting suitable certification. Depending on the risk of data processing, the reviews must be repeated on a regular basis during the term of the contract.

5. In the event of cross border contract processing, the relevant national requirements for disclosing personal data abroad must be met. In particular, personal data from the European Economic Area can be processed in a third country only if the provider can prove that it has:

a) Data protection standards equivalent to this Data Protection policy. Suitable tools can be :

1. Agreements on EU standard contract clauses for contract processing in third countries with the provider and any subcontractors

2. Participation of the provider in a certification system accredited by the EU for the provision of a sufficient data protection level.

3. Acknowledgement of binding corporate rules of the provider to create a suitable level of data protection by the responsible supervisory authorities for data protection.

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.

1. 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 employers documents (e.g. personnel files) for the employment relationship under the relevant employment laws, these will remain unaffected.
2. If personal data is transmitted to third parties, information must be given about the identity of the recipient or the category of recipients.
3. If personal data is incorrect or incomplete, the data subject can demand that it be corrected or supplemented.
4. The data subject can object to the processing of his/her data for purposes of advertising or market/opinion research. The data must be blocked from these types of use.
5. 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.
6. The data subject generally has a right to object to his/her data being processed, and this must be taken into account if the protection of his/her interests take 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.

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 a 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. Supervisors 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.

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 (determined by the process for information classification).
The technical and organizational measures for protecting personal data are part of Company Integrated Management System and must be adjusted continuously to the technical developments and organizational changes.

Data Protection Control/Audits

Compliance with the Data Protection policy and the applicable data protection laws/GDPR is checked regularly with data protection audits and other controls. The performance of these controls is the responsibility of the Data Protection Officer, 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 the Data Protection Officer. Facilization must be informed of the primary results as part of the related reporting duties. On request, the results of the 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.

Data Incidents

All employees must inform their supervisor, data protection coordinator or the Data Protection Officer immediately about cases of violations against this Data Privacy and Protection Policy or other regulations on the protection of personal data (data protection incidents). The manager responsible for the function or the unit is required to inform the Data Protection Officer immediately about the data protection incidents.

Facilization is obligated to report these incidents to the supervisory authorities and to the affected individual within 72 hours of a breach in case of :

1. Improper transmission of personal data to third parties

2. Improper access by third parties to personal data, or

3. Loss of personal data

The required company reports (Incident Management) must be made immediately so that any reporting duties under GDPR and national law can be complied with.

Responsibilities and Sanctions

The executive bodies of Facilization 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 Privacy and 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. Compliance with these requirements is the responsibility of the relevant employees. If official agencies perform data protection controls, the Data Protection Officer must be informed immediately.

Data Protection Officer is the contact person on site for data protection. The Data Protection Officer must familiarize the employees with the content of the data protection policies. The relevant management is required to assist the Data Protection Officer with their efforts. The departments responsible for business processes and projects must inform the DPO in good time about new processing of personal data. For data processing plans that may pose a special risk to the individual rights of the data subjects, the Data Protection Officer must be informed before processing begins. This applies in particular to extremely sensitive personal data. The managers must ensure that their employees are sufficiently trained in data protection.

Improper processing of personal data, or other violation of the data protection laws, can be criminally prosecuted in many countries and result in claims for compensation of damage. Violations for which individual employees are responsible can even lead to sanctions.

Data Protection Officer

The Data Protection Officer works towards compliance with Albanian Laws on Personal Data Protection and GDPR. He is responsible for the Data Privacy and Protection policy and supervises its compliance. The Data Protection Officer is appointed by the Facilization General Manager.

Any data subject may approach the Data Protection Officer at any time to raise concerns, ask questions, request information or make complaints relating to data protection or data security issues. If requested, concerns and complaints will be handled confidentially. Decisions made by the Data Protection Officer to remedy Data Protection breaches must be upheld by the management of the company in question. Inquiries by supervisory authorities must be reported to the Data Protection Officer.

Contact Details for the Data Protection Officer and staff are as follows:

Contact: **Denisa Hasimaj**
E-mail: **dpo@facilization.com**
Tel: **+355 4 22 56 006**
Web: **www.facilization.com**
Address: **Facilization SHPK**
Rr. Sami Frashëri, P.56, Kompleksi TID,
Hyrja B, Kati 1, Tirana, Albania