Université Saint-Joseph de Beyrouth
جامعة القدّيس يوسف في بيروت

Data Protection by Design and by Default Policy

The French version of the present text was approved by the University Board during its 216th meeting on October 18, 2022 and amended during its 230th meeting on October 21, 2026

PURPOSE (OBJECTIVE, BENEFITS, SCOPE)

This Policy aims to define the principles adopted by Saint Joseph University of Beirut (hereinafter referred to as "the University") to protect data by design and throughout its retention period. It also aims to ensure data protection by default.

This Policy allows the University to address data protection in order to safeguard privacy and ensure compliance with applicable laws and regulations, particularly the General Data Protection Regulation (GDPR).

It also takes into account modern digital environments, including cloud services, collaborative platforms, and artificial intelligence tools used within the University.

This Policy applies to all Administrative Staff and instructors at the University.

DIRECTOR/MANAGER

Chief Information Security Officer – hereinafter CISO

USERS

Administrative staff members and instructors

ROLES AND RESPONSIBILITIES

CISO

CISO is responsible for ensuring that the various stakeholders comply with this policy.

Users

Users must comply with the recommendations and requirements set out in this Policy.

DESCRIPTION

General Principles

The general principles governing the protection of personal data at the University are as follows:

1. Be vigilant and proactive rather than reactive in order to detect privacy incidents before they occur.
2. Make data protection the default by specifying the purpose of processing, limiting data collection, minimizing the data shared, and destroying data when it no longer serves its original purpose.
3. Integrate data protection by design into the architecture of IT systems and all day-to-day operations.
4. Ensure privacy and data security without compromising them for other functionalities.
5. Integrate data security into all digital environments, including cloud services and remote use.
6. Limit data exposure when using digital tools, particularly collaborative platforms and artificial intelligence tools.
7. Ensure end-to-end data security throughout the retention period, from collection to destruction.
8. Ensure full transparency toward data subjects by clearly and consistently informing them about the processing of their personal data.
9. Respect the privacy and protect the best interest of data subjects by providing appropriate measures, such as strict default privacy settings, appropriate notices, and user-friendly opt-in options.

Data Protection by design

The University applies the principle of data protection by design to ensure data privacy and protection throughout the entire lifecycle, from the design of any system, service, product, or process to the destruction of the data.

Users must continuously ensure the security of the University's systems and data at all times to prevent the risk of data breaches, particularly when using mobile devices and remote connections.

This principle also applies to cloud solutions.

Data Protection by Default

The University ensures that, by default, only the personal data necessary for each specific processing purpose is processed. This includes the amount of data collected, the extent of its processing, the retention period, and data accessibility. When data is collected, the default settings must be clear, user-friendly, and provide a high level of privacy.

Data Sharing

All processing and transfer of personal data must be carried out securely. In addition, to comply with the GDPR, requests for information must be approved by the Data Protection Officer (DPO) before being sent to the relevant data owners. Therefore, any office or institution requesting data must submit the **Data Request Form** (see Annex 1), specifying the information requested and the purpose of the processing. Once the DPO's approval has been obtained, the owner of the requested data may send it to the requester.

Only the minimum amount of data required for the processing in question should be shared. It is also recommended to anonymize or pseudonymize personal data (reversible anonymization) to reduce the risk of data leaks.

Sharing data through services that have not been approved by the University is prohibited.

Secure tools should be prioritized when exchanging data.

Third-Party Solutions

Before purchasing systems or platforms that involve personal data, including cloud solutions, data privacy and security must be assessed to prevent the risk of a data breach. Personal data must not be placed on these systems without the DPO's approval, in accordance with the University's policies and regulations, particularly information security policies. The retention period for such data must be kept to a minimum.

The use of cloud or SaaS solutions must be approved in advance, taking into account data security and protection requirements.

Best Practices for Reducing the Risk of Data Leaks

- Obtain the consent of data subjects before processing any data.
- Use privacy notices to ensure transparency toward data subjects.
- Limit access to personal data to those who need it.
- Check recipients before sending emails.
- Regularly delete personal data once the purpose of the processing has been fulfilled or the retention period has ended.
- Minimize the collection, storage, use, and transfer of personal data as much as possible.
- Fully and irreversibly anonymize personal data whenever possible.
- Pseudonymize personal data and keep the key in a secure location.
- Encrypt documents (Excel, Word, etc.) containing personal data using tools approved by the University.
- Store paper documents containing personal data in secure locations (safes, locked cabinets, locked drawers, or other secure locations).

- Use multi-factor authentication (MFA) when available.
- Remain vigilant against phishing and social engineering attempts.
- Immediately report any data breach or suspected data leak.

Entering personal or sensitive data into artificial intelligence tools that have not been approved by the University is prohibited.

Standards, Guidelines, References

General Data Protection Regulation (GDPR)

Glossary	**Personal data**: any information relating to an identified or identifiable natural person. **Anonymization**: making it impossible to identify a person in an irreversible manner. **Pseudonymization**: replacing directly identifying data (last name, first name, etc.) with indirectly identifying data (alias, sequential number, etc.). If needed, pseudonymization may be reversible, unlike anonymization. **Encryption**: protecting saved documents with a password.
Abbreviations	**CISO**: Chief Information Security Officer **ISSO:** Information System Security Officer **PSG:** Administrative Staff **DPO:** Data Protection Officer **GDPR**: General Data Protection Regulation

ANNEX 1

Data Request Form

This form must be filled for all data requests. The policy stipulates that all data requests must be approved by the Data Protection Officer of USJ.

1. Specify the requested data

---

2. Specify the motive
