Qatar University

Document Number:	CSDO-IN-01-V1
Document Type:	Instructions
Document Title:	Personal Data Privacy Instructions at Qatar University
Responsible Sector:	Qatar University
Approval Date:	22nd February, 2022
Effective Date:	22nd February, 2022

Personal Data Privacy Instructions at Qatar University

Related Legal Documents:	Law No.13 of 2016 on Personal Data Privacy Protection Data Management Policy of the Ministry of Communications and Information Technology

Approval of the President:	**Date:** 22-2-2022

Personal Data Privacy Instructions at Qatar University

(This is as true as possible translation, where the Arabic version is the only official document)

In the event of any conflict between the provisions of these instructions, and Law No. (13) of 2016 regarding Personal Data Privacy Protection, or the instructions and guidelines issued pursuant thereto, the provision of the State's law, instructions and guidelines shall apply to the extent that remove that conflict.

Collection, Storage and Use of Personal Data

In accordance with the Data Management policy issued by the Ministry of Communications and Information Technology in the State of Qatar, the university is keen to ensure that the process of data collection is carried out through legitimate and impartial means. Collection of data must be limited to what is necessary to meet the university's legal requirements, or to meet the requirements related to its business and scientific activities.

The collection of personal data depends on the circumstances in which the university is collecting this data (e.g. employment procedures, promotion, filing individual claims with government agencies) and the related requirements. In principle, the university collects personal data directly from the concerned individual as much as possible. The university may also attempt to collect personal data using other legitimate sources only when it is not reasonable nor practical to collect such data directly from the individual, or for validation purposes.

Direct Data Collection

The university, when possible, standardizes the method of personal data collection through designated forms sent directly to the concerned individual to be filled out. The university receives personal data using other methods, such as: electronic communication, over the telephone, during face-to-face meetings and interviews, and financial transactions.

Third-Party Data Collection

The university may also collect and process personal data about an individual through third-party, that includes any other person or entity assigned by the university for the legitimate purpose. This method of data collection is used only when it is not possible nor practical to collect personal data from the individual directly.

Before engaging the third party in data collection, the university maintains the privacy of individuals by evaluating the privacy policies of the third party, and any possible risks associated with this engagement. In this context, the university obtains contractual guarantees from the third party to ensure that they fulfill its obligations and abide by the relevant laws and regulations while collecting or sharing personal data.

Indirect Data Collection

Indirectly collected data is the data provided to Qatar University without being requested by the university, and is often collected by:

1. Employment applications such as CVs and other personal files sent to the university that are not in response to an advertised vacancy.
2. The submission of a sick leave certificate by a student, an employee or other members of the university, that may provide access to certain medical records of the individual.
3. Misdirected postal or electronic mail – such as letters or emails.
4. Technical information related to the use of the university's website by the individual, such as: type of device used to access the website, Internet Protocol (IP) address used to connect the device to internet, Uniform Resource Identifier (URI), user's login information, type and version of the browser used, time zone setting, operating system of the device, and pages the user has viewed (including date and time). In addition, the university may collect information using website cookies.
5. Through the student's tuition fees payment process by an institution sponsoring the student, a funding body or a governmental body in the State of Qatar, the university will receive basic information about the student as well as the funding process, from the providing entity.
6. Any other data provided to the University without being requested.

The university does not retain, use or disclose indirectly collected personal data unless otherwise permitted. If it is not the case, the university will destroy or permanently delete this data.

The university has the right to retain records of the indirectly collected personal data that were obtained by any of the means mentioned above, if the individual's consent is obtained before using it.

Collection and Use of Sensitive Personal Data

Sensitive personal data is collected only in the following cases:

1. Executing a mission related to the public interest as per the State's law.
2. Implementing a legal obligation or an order rendered by a competent court.

3. Protecting vital interests of individuals.
4. Achieving purposes of scientific research for the public interest.
5. Gathering necessary information for investigation into a criminal offense, upon an official request of investigative bodies.

The university is keen to document, maintain and protect data, considering that the university is the issuing authority and the right holder. The university may store personal data in various forms, including but not limited to the following:

1. Internal databases
2. Hard or digital copies of files
3. Personal devices, including laptop computers
4. Third-party storage services such as cloud storage facilities

The university takes the precautions necessary to protect the personal data in its possession against misuse, loss, unauthorized access, modification or disclosure. These precautions include, but are not limited to:

1. Restricting access to data and limiting it to authorized persons depending on their tasks and responsibilities.
2. Raising awareness among employees on the importance of not sharing personal passwords, and the potential risks associated with it.
3. Implementing physical security measures (e.g. security guards, surveillance cameras, access cards) in all university buildings and associated lands, to prevent intrusion and access to data.
4. Ensuring all policies and procedures related to Information Technology, Data Backup and Cyber Security are implemented and up to date.
5. Raising awareness among employees and encouraging them to fully comply with the policies and procedures related to personal data.
6. Taking into consideration all matters related to third-party service providers who may have access to personal data, including customer identification service providers and cloud service providers, to ensure their compliance with the relevant State’s laws and regulations.
7. Destruction or deletion of any personal data that is no longer needed to be retained by the University.

Personal data will be kept when it is reasonably necessary for any legitimate purpose, and will be deleted once the purpose for which it was collected has been achieved. Data retention periods vary with different types of data.

The university has the right to use personal data that is reasonably necessary for one of the university's business or activity, after obtaining the consent of the concerned individual. The primary uses of personal data may include, but not limited to, the following:

1. Providing education, curricular and health services.
2. Meeting the university's legal obligations.
3. Keeping parents or legal guardians informed about different matters within the university community, through correspondence, university newsletters and magazines.
4. Direct marketing, promotional and fundraising activities.
5. Supporting the university's clubs activities, in addition to development and fundraising activities.
6. Supporting community activities, charities and other activities related to the university's functions.
7. Developing new systems, programs and services, and conducting statistical research and analytics.
8. Recruitment procedures.
9. Engagement of volunteers.

Validity and Accuracy of Personal Data and the General Rights of Concerned Individuals

The university takes reasonable steps to ensure that the personal data it hold, use, and disclose is accurate, complete and up-to-date.

Upon receiving any request related to this data, the university takes the necessary measures to respond appropriately to it in a manner that protects the rights of the concerned individuals. In case the request is rejected, the individual will be notified and will be provided with the reason(s) of the decision, when required. If the rejection relates to a requested change in personal data, the concerned individual may make a statement about the requested change and it will be attached to his/her record.

If an individual withdraws their consent to use or share their personal data for the purposes set out in this Data Privacy Instructions, that individual may not be able to access all, or some of, the services offered by the university.

The university is committed to take the following measures to ensure the general rights to an individual's personal data:

1. Reviewing the privacy protection measures before initiating new processes.

2. Identification of the data processors who are responsible for personal data protection.
3. Providing training for data processors on data protection measures, and raising awareness among them on the importance of personal data protection.
4. Establishing internal systems to receive and process complaints, data access requests, and requests for correction or deletion of data, and make them accessible to individuals.
5. Establishing internal systems that enable effective personal data management, and report any violation of the procedures set for the protection of personal data.
6. Employing appropriate technological means that enable individuals to exercise their right to access, review and modify their personal data.
7. Conducting comprehensive audits and reviews on the extent of compliance with personal data protection.
8. Verifying that the processor abides by the provided instructions, and adopts the appropriate precautions to protect personal data and to monitor them regularly.

An individual can file a complaint about how the university is managing personal data, including a privacy breach, by notifying the Office of the General Legal Counsel at the university in writing, and the university will provide the response within one month from the date of receiving the complaint.

Disclosure and Sharing of Personal Data

Personal data may be disclosed to government agencies, parents, other universities, recipients of university publications, visiting faculty, counsellors and coaches, services providers, agents, contractors, business partners, related entities and other beneficiaries, if the individual expressly consents.

The university may disclose personal data without obtaining the concerned individual's consent in these cases:

1. Disclosure of data will prevent a serious threat to the life, health or safety of an individual or to public safety.
2. Data disclosure request pursuant to a legal request or a competent court.

All data users must respect the rights of the person whose personal data is being processed, such as intellectual property rights, right to privacy, and the right to digital oblivion.

The university pursues transparency policy in dealing with the student's personal data, and directs any personal data requests to the student concerned, and/ or his or her parents or legal guardians as appropriate.

Changes to the Personal Data Privacy Instructions

In the event of any revision, change or update of this Personal Data Privacy Instructions, the updated version will be posted on Qatar University website and will be reflected on all the official documents that are approved by the university. All competent authorities, each in its jurisdiction, shall ensure the implementation and enforcement of these instructions starting from the issuance date of the updated version.

Appendix

The following terms and expressions shall have the meanings herein assigned, unless the context states otherwise:

University	Qatar University
President	President of Qatar University
Individual	A natural person whose personal data are processed
Controller	A natural or legal person who, whether acting individually or jointly with others, determines how personal data may be processed and determines the purpose(s) of any such processing personal data Processing.
Processor	The natural or legal person entrusted by Qatar University to process personal data on its behalf.
Personal Data	Data of an individual whose identity is defined or can be reasonably defined whether through such personal data or through the combination of any other data.
Personal Data Processing	Personal data Processing through one operation or more such as gathering, receipt, registration, organization, storage, preparation, modification, retrieval, usage, disclosure, publication, transfer, withholding, destruction, erasure and cancellation.
Lawful Purpose	The purpose for which personal data of an individual is processed, in accordance with the law.
Direct Marketing	Sending any advertising or marketing material, in whatsoever means, to certain individuals.
Electronic Communication	A communication by means of any of wire and wireless communications.
Third-party	Any person or entity other than the data issuer or the data user, who processes the data on behalf of the entity, and the term includes any other person or entity designated by a third party for the purpose referred to.
Data Issuer	Refers to the entity that documents, maintains and protects data, as it is holder of the right to the data and provides it to and/or exchanges it with other parties.
Data Sharing	Disclosure of data by an entity to another entity/entities.
Sensitive Personal Data	Data consisting of racial origin, children, data concerning health, a physical or mental condition of the person, religious beliefs, marital relationship or criminal offences. The President and the General Legal Counsel can add other categories of sensitive personal data, after the approval of the competent minister, if the misuse or disclosure of these data would cause a serious harm to the individual.