



THE AGA KHAN UNIVERSITY

(International) in the United Kingdom

Institute for the Study of Muslim Civilisations

**AKU-UK DATA
PROTECTION
POLICY**

2022


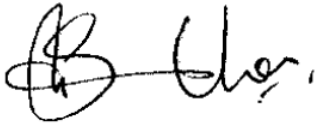


Table of Contents

1. Introduction.....	6
2. Applicability.....	6
3. Roles & Responsibilities.....	6
3.1. Data Protection Officer.....	6
3.2. Data Protection Champions.....	7
4. Exceptions.....	7
5. Data Subject.....	8
6. Data Subject Classification.....	8
7. Information Classification & Marking Scheme.....	10
8. Data Processor.....	10
9. Ownership of Subject Data.....	10
10. Protection Framework.....	10
10.1. Principles.....	11
10.2. Lawful Basis of Processing.....	11
10.2.1. Consent.....	11
10.2.2. Contract.....	12
10.2.3. Legal Obligation.....	12
10.2.4. Vital Interests.....	12
10.2.5. Public Task.....	12
10.2.6. Legitimate Interests.....	12
10.3. Data Subject Rights.....	12
10.3.1. Right to be Informed.....	12
10.3.2. Rights to Personal Data.....	13
10.4. Accountability & Governance.....	13
10.4.1. Contracts.....	13
10.4.2. Documentation.....	14
10.4.3. Data Protection by Design & Default.....	14
10.4.4. Privacy Impact Assessments.....	14
10.5. Security.....	14
10.6. International Transfers.....	15
10.7. Incidents & Breaches.....	16
11. ANNEX A – Subject Access Request Form.....	17
12. ANNEX B – Privacy Impact Assessment.....	18

AKU-UK Data Protection Policies

13. ANNEX C – Breach Notification Form.....	19
14. ANNEX D – Exception Form.....	20
15. ANNEX E – Data Privacy Champion Contact List.....	21
16. ANNEX F – Data Processor List.....	23
17. ANNEX G – Data Subject Consent Form.....	24
18. ANNEX H – Data Subject Consent Withdrawal Form.....	25
19. ANNEX I – Privacy by Design	26
20. ANNEX J – Legitimate Interest Assessment.....	29
21. ANNEX K – Privacy Policy.....	31
22. ANNEX L – Data Subject Consent Template.....	36

Document Approval

Name	Signature	Date
AKU UK Senior Management		October 2022
AKU Global Chief Information Officer (CIO)		September 2022
AKU Global Legal Representative		September 2022
AKU Global Data Protection Officer (DPO)		September 2022

Version Control

Version	Maintained by	Release date
1.0	Data Protection Team (DPT) as part of Global Data and Analytics Office (GDAO)	July 2020
2.0	Data Protection Officer (DPO)	September 2022

Referenced Documents

The following documents support this policy:

Title	Version	Maintained by
Subject Access Request Form	1.0	Data Protection Team (DPT) as part of Global Data and Analytics Office (GDAO)
Privacy Impact Assessment	1.0	Data Protection Team (DPT) as part of Global Data and Analytics Office (GDAO)
Breach Notification Form	1.0	Data Protection Team (DPT) as part of Global Data and Analytics Office (GDAO)
Exception Form	1.0	Data Protection Team (DPT) as part of Global Data and Analytics Office (GDAO)
Data Subject Consent Form	1.0	Data Protection Team (DPT) as part of Global Data and Analytics Office (GDAO)
Data Subject Consent Withdrawal Form	1.0	Data Protection Team (DPT) as part of Global Data and Analytics Office (GDAO)
Privacy by Design	1.0	Data Protection Team (DPT) as part of Global Data and Analytics Office (GDAO)
Legitimate Interest Assessment Form	1.0	Data Protection Team (DPT) as part of Global Data and Analytics Office (GDAO)
Data Subject Consent Template	1.0	Data Protection Team (DPT) as part of Global Data and Analytics Office (GDAO)
Data Protection Policy	2.0	Updated contacts, versions, signatories

List of Acronyms

AKU UK	The Aga Khan University (International) in the United Kingdom
CIO	AKU Global Chief Information Officer (CIO)
DPO	Data Protection Officer
ICO	UK Information Commissioner Office
ICT	Information and communications technology
GDPR	General Data Protection Regulation
SAR	Subject Access Requests
PIA	Privacy Impact Assessment
VoIP	Voice over Internet Protocol
EU	European Union

1. Introduction

This policy has been developed to define and set forth requirements to ensure the protection of the subject data that has been processed, stored, and transmitted by The Aga Khan University (International) in the United Kingdom referred as AKU-UK from this point forward.

2. Applicability

The policies stated herein apply to all AKU-UK employees and contractors. Third-party suppliers who connect to AKU-UK systems that process, store or transmit data subject information shall be contractually required to meet or exceed the intent of these policies.

3. Roles & Responsibilities

3.1. Data Protection Officer

The AKU-UK Data Protection Officer (DPO) shall report to the Board and bears the overall responsibility for monitoring and ensuring compliance to these policies on their behalf through the Data Protection Champions (DPC) identified for each business line within the AKU-UK. Nonetheless, to be effective, compliance activities must be a collaborative effort involving the support of all AKU-UK business stakeholders, employees, contractors and third-party service suppliers.

The DPO shall be responsible for conducting periodic and ad-hoc audits to verify and document overall group compliance to these policies. Additionally, the DPO shall be responsible for notifying UK Information Commissioner Office (ICO) of any suspected or confirmed breach or any associated liaise as required.

The DPO shall be also responsible for training DPCs and staff to raise awareness of Data Protection and foster a data privacy culture across the AKU-UK.

The contact details for the AKU-UK DPO are as follows:

Name: Umair Ismail

Title: Data Protection Officer

Tel: +44 (0)20 7380 3800

Email: DPO@aku.edu

3.2. Data Protection Champions

Data Protection Champions (DPCs) shall be identified for each of the AKU-UK business lines (and brands where applicable). AKU-UK DPCs are identified in [Annex E](#).

DPCs shall be primarily responsible for implementing the data protection programme in their businesses, confirming compliance and liaising with the DPO for correct programme and policy interpretation.

DPCs and staff shall also be responsible for ensuring policies are understood and complied with by any outsourced Data Processors (DP) and that compliance and liability requirements are stated in applicable contracts and service level agreements.

All users of AKU-UK ICT systems are responsible for properly using the security controls that are in place including technical, administrative or other appropriate measures designed to protect subject data.

4. Exceptions

Exceptions to the policies and procedures detailed herein shall only be granted after obtaining proper approvals and signoffs.

The AKU-UK DPO shall have the authority to grant exceptions to the policies and procedures detailed herein.

Requests for exceptions to established data protection policies and procedures shall be made in writing and submitted to the DPO for review and approval.

Recommendations for exceptions should be approved by relevant Business Owner, ISMC Senior Management and CIO before submission to DPO.

The request should state the business case and/or operational obstacle prohibiting the policy or procedure from implementation and propose an alternative and appropriate “compensating control” to mitigate the associated security risk.

All exceptions require the prior written approval from the AKU-UK DPO and exceptions shall be submitted using [Annex D](#).

5. Data Subject

For purposes of these policies, a “data subject” is simply defined as any person (living or dead) for which AKU-UK holds information.

Given this definition, it is understood that AKU-UK processes, stores and transmits both **Personal Data** and **Sensitive Personal Data** information associated with data subjects under following three categories:

- Employees
- Students
- Donors

Personal Data and **Sensitive Personal Data** shall be subject to the applicable controls stated herein regardless of the data subject.

6. Data Subject Classification

Personal data shall be classified according to AKU Information Security Policies as **CONFIDENTIAL** and any information that can be used to identify or distinguish one data subject (see below) from another or by combining the information with other information that you have or are likely to have in the future.

Examples of **CONFIDENTIAL** data include but are not limited to:

- A data subject’s name, address, date of birth, etc.
- A data subject’s physical description, height weight, colour of hair or eyes
- A data subject’s driver’s license or identity card number
- A data subject’s personal or national insurance number
- One or more factors specific to a data subject’s physiological, mental, economic, cultural or social identity

Additionally, this classification covers sensitive information about individuals and the University. Such information has the potential to cause a negative impact on individuals’ or the University’s interests. Information receiving this classification requires a high level of protection against unauthorized disclosure, modification, destruction, and use. Specific categories of confidential information include personally identifiable information about:

AKU-UK Data Protection Policies

- Current and former students including student academic, disciplinary, and financial records.
- Current, former, and prospective employees, including employment, pay, benefits data, and another personnel information.
- Research information related to a potential or pending patent application.
- Certain University business operations, finances, legal matters, or other operations of a particularly sensitive nature.
- Information security data, including passwords.
- Information about security-related incidents.

Sensitive Personal data shall be classified according to AKU Information Security Policies as “**HIGHLY CONFIDENTIAL**” and is any personal information that could be used in a discriminative way and is likely to be of a private nature.

This classification covers sensitive information which, if it becomes available to unauthorized users create risk for identity theft and has the potential to cause serious damage or distress to individuals or serious damage to the University’s interests if disclosed inappropriately.

Examples of **HIGHLY CONFIDENTIAL** data include but are not limited to:

- A data subject’s racial or ethnic origin
- A data subject’s political opinions
- A data subject’s religious, or other similar beliefs
- A data subject’s physical or mental health or condition
- A data subject’s sexual orientation
- A data subject’s criminal convictions or alleged criminal acts
- A data subject’s personal records
- A data subject’s bank details
- A data subject’s passport details
- A data subject’s credit and or debit card details (PAN/CVV2/Expiry Date/PIN)

Additionally, this classification would apply to the following information:

- Investigations/disciplinary proceedings
- University Strategies
- Donors, potential donors and other University clients.
- University financial Data

- “On-going” and submitted Research Papers
- Access codes for higher risk areas
- System username and passwords

Questions or clarifications regarding these definitions should be referred to the DPO (through DPC) for resolution.

7. Information Classification & Marking Scheme

AKU-UK will implement an information classification and marking scheme as defined in the AKU policy ADM-P-003 (information classification and handling) to identify and classify all information assets into one of the following categories: ‘Confidential’, and ‘Highly Confidential’.

All Personal Data will be clearly marked “Confidential” and all the Personal Data excluding the Sensitive Personal Data must be clearly marked “Highly Confidential”.

8. Data Processor

A “Data Processor” is simply defined as any natural or legal person, public authority, agency or other body which processes personal data on our behalf.

AKU-UK shall ensure that all its Data Processors comply with these policies and their intent. Deviations require prior AKU-UK DPO approval.

A current list of AKU-UK Data Processors can be found in in [Annex F](#) of this document.

9. Ownership of Subject Data

AKU-UK owns its subject databases and the information contained therein.

Subject data collected may only be processed, stored or transmitted by AKU-UK-approved Data Processors subject to its protection in accordance with these policies.

10. Protection Framework

To ensure the appropriate protection of subject data that is provided AKU-UK shall adhere to the framework principles stated below.

Policies shall be implemented at all AKU-UK (and AKU-UK DP) operating locations and apply to both categories of information (Personal Data and Sensitive Personal Data) unless where otherwise noted.

10.1. Principles

AKU-UK shall ensure that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

10.2. Lawful Basis of Processing

10.2.1. Consent

It is AKU-UK policy that both **Personal Data** and **Sensitive Personal Data** shall not be processed without a business reason or without prior consent from the data subject. Forms used to collect information from data subjects directly shall require the data subject's specific consent to do so.

AKU-UK shall implement a process to also allow data subjects the option to deny AKU-UK, the right to process their data. If requested, AKU-UK shall provide written assurance to data subjects that they do not process, store or transmit their data. Additionally, AKU-UK must obtain end user consent prior to placing "cookies" in their browsers.

All AKU-UK company employee applications shall include the provision for the employee's consent for the company to process, store and transmit information associated with their employment. Where the processing of AKU-UK employee information is carried out by a third party, applicable contractual obligations shall require employees' consent to process and transmit information associated with their employment. Note: If the third party is unwilling or unable to agree to this requirement, the information should be withheld. Information provided to third party organisations is only allowed to be used by those in connection with the product

or service contracted. Refer [Annex L](#) for the template for obtaining Data Subject consent, communication preferences and withdrawal of consent

10.2.2. Contract

AKU-UK shall collect and process personal data without explicit consent if it is required to fulfil a contract with the data subject, where the contract cannot be completed without the personal data in question.

10.2.3. Legal Obligation

AKU-UK shall collect and process personal data without explicit consent if it is required to comply with the law or regulatory requirements, in the event of any conflict between this item and other elements of this policy then compliance with the law will be prioritised.

10.2.4. Vital Interests

AKU-UK shall collect and process personal data if it is required to protect the vital interests of the data subject or of another natural person.

AKU-UK shall retain documented evidence.

10.2.5. Public Task

AKU-UK shall process data if it needs to perform a task that is in the public interest or as a part of an official duty.

AKU-UK shall retain documented evidence.

10.2.6. Legitimate Interests

AKU-UK may process specific personal data for the legitimate interest of the company if the rights and freedom of the data subject is not affected in a significant way. Cases where this is exercised shall be approved prior by the DPO. If applicable the DPO shall carry out a Legitimate Interest Assessment ([Annex J](#)) and retain the documentation.

10.3. Data Subject Rights

10.3.1. Right to be Informed

AKU-UK shall ensure that data subject is informed about the use of their data and their rights over it.

10.3.1.1 Privacy Policy

All AKU-UK properties (and websites) shall post the following “Privacy Notice” clearly stating the purpose of our data collection activities. Deviations from this Privacy Policy (*refer **Annex K***) wording requires the prior approval of the DPO.

10.3.2. Rights to Personal Data

The UK Data Protection Act 2018 (the Act) and the European General Data Protection Regulation (GDPR) gives British and European citizens (data subjects) specific rights to their personal data held by AKU-UK. The rights defined in the Act and GDPR are:

- The right of access
- The right of rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- The right to object to automated decision making and profiling.

There are limitations on these rights and not all of them are applicable to the AKU-UK - for example AKU-UK does not use automated decision making and profiling.

In exercising their rights, data subjects can make requests to AKU-UK and these requests are known as “Subject Access Requests” (SAR’s) although they may cover requests for rectification, erasure, objections, data portability and requests to restrict processing.

Data Subjects wishing to exercise their rights over the personal data AKU-UK holds should consult the policy document AKU-UK - Subject Access Request Policy for details on AKU-UK’s Subject Access Request (SAR) policy and process. The form in **Annex A** should be completed and sent to the local DPC for action.

10.4. Accountability & Governance

10.4.1. Contracts

AKU-UK shall ensure that all contracts that involve the processing of Data Subject data shall be subject to a document contract that includes the specific information and terms required by legislation.

10.4.2. Documentation

AKU-UK shall ensure that documentation is maintained for Data Subject data processing activities, data sharing and data retention.

The DPO shall maintain an information asset register identifying Personal Sensitive information asset owners and its location.

Additionally, the DPO shall maintain a systems diagram illustrating the location of high volumes of Personal Sensitive data on the AKU-UK systems.

AKU-UK shall ensure that these records are up to date and reflect current processing activities.

10.4.3. Data Protection by Design & Default

AKU-UK shall ensure the adoption of privacy by design and default for all new and significantly changed systems that collect and process personal data.

For more information, see Privacy by Design document. ([Annex I](#))

10.4.4. Privacy Impact Assessments

AKU-UK DPCs must complete a Privacy Impact Assessment (PIA) ([Annex B](#)) for new projects involving the processing, storage or transmittal of data subject information. A project is a piece of work that is managed by the central IT and Projects team.

PIAs should be completed by the DPC and submitted to the AKU-UK DPO for review and approval.

For instructions or assistance in completing a PIA, see the DPO.

10.5. Security

It is AKU-UK policy to provide appropriate security to ensure the protection of both Personal Data (Confidential) and Sensitive Personal Data (Highly Confidential) that it processes, stores or transmits.

Information processed on AKU-UK systems shall be protected in accordance with the current published AKU-UK information security policies and procedures.

For purposes of clarity, AKU-UK systems that are used to host, process, and store or transmit **Sensitive Personal Data** (Highly Confidential) shall meet or exceed the following safeguards:

AKU-UK Data Protection Policies

- Systems shall be protected from unauthorised external access (firewalls).
- System devices shall be protected by firewalls and anti-malware protection.
- Operating systems and applications shall be configured with latest security patches and updates.
- Data shall be backed up regularly and back-ups encrypted and stored in off-site location.
- Data should be securely removed before disposal of devices.

Additionally, the following safeguards should be implemented to ensure the security of **Sensitive Personal Data** (Highly Confidential) on our systems:

- Ensure that access to information is provided based on a “need to know” basis.
- Passwords to devices accessing information meet or exceed published AKU-UK requirements
- Hardcopy information is shredded when no longer required.
- Hardcopy information is stored in alarmed offices.

It should be noted that these minimum safeguards detailed herein apply to AKU-UK systems regardless of technology (wireless, software as a service, VoIP, virtualised or public, private or hybrid cloud computing etc.).

All employees with access to AKU-UK systems that process the data that includes Sensitive Personal Data (Highly Confidential), shall be required to:

- Receive data protection awareness training when being granted access; and
- Receive regular security awareness briefings designed to heighten their information security awareness and remind them of their on-going security responsibilities

10.6. International Transfers

AKU-UK can transfer **Personal Data** and **Sensitive Personal Data** from the UK to non-EU countries however data transmittal, processing and storage must meet or exceed requirements stated herein.

Sensitive Personal Data shall not be transferred to a country or territory outside the European Union (EU) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information. For clarification if the country meets this requirement, consult the DPO.

AKU-UK shall ensure via contractual obligations that **Sensitive Personal Data** does not exit the EU without legitimate business or legal purposes.

10.7. Incidents & Breaches

For purposes of this policy the following definitions apply:

“Security Incident” refers to any adverse event that affects the confidentiality, integrity or availability of information that is processed by a computer system, regardless whether information was exposed or exfiltrated. A computer virus is an example of a security incident.

“Security Breach” A security breach may mean that someone other than the data controller gets unauthorised access to Personal or Sensitive Personal data. But a data breach can also occur if there is unauthorised access within an organisation, or if a data controller’s own employee accidentally alters or deletes the data.

As soon as AKU-UK becomes aware that a personal data breach has occurred which is likely to risk data subject’s right, AKU-UK shall notify Information Commissioner’s Office (ICO) without undue delay and, where feasible, not later than 72 hours. Where the notification to the ICO is not made within 72 hours, AKU-UK shall report the reason for the delay.

When personal data breach is likely to result in a high risk to the rights and freedom of data subject, AKU-UK shall communicate the breach to the data subject without undue delay.

AKU-UK shall document any personal data breach, comprising the facts relating to the breach, its effect and the remedial action taken.

- End -

11. ANNEX A – Subject Access Request Form

AKU-UK takes security and individual rights seriously. Please fill the form to obtain the information we hold about you. We will provide the requested information within 30 days of receiving this form.

[Open form](#)

12. ANNEX B – Privacy Impact Assessment

This form needs to be filled for any new or updated projects that are likely to result in high risk to data subject's interests.

Answering "Yes" to any of the screening questions below represents a potential risk factor that will have to be further analysed to ensure those risks are identified, assessed and fully mitigated.

Open form

13. ANNEX C – Breach Notification Form

[Open form](#)

14. ANNEX D – Exception Form

AKU-UK considers exception requests in unavoidable circumstances. A detailed explanation with the business justification along with proper approvals and signoffs (as mentioned in the policy) behind the request is mandatory.

[Open form](#)

15. ANNEX E – Data Privacy Champion Contact List

Below are the contact details of the Data Protection Champions across AKU-UK:

S#	Company / Department Name	Contact Name	Job title	Email
1	Marketing & Communications	Layal Mohammed	Manager, Marketing and Communications	layal.n.mohammed@aku.edu
2	Resource Development	Sidrah Naveed	Prospect Researcher	sidrah.naveed@aku.edu
		Aziz Anwerali	Assistant Manager	aziz.anwerali@aku.edu
		Ali Faisal	Director	alifaisal.queshi@aku.edu
3	Governance Programme	Sanaa Alimia	Assistant Professor	sanaa.Alimia@aku.edu
4	Centre for Digital Humanities (CDH) & Professional Programmes	Anjum Alam	Programme Manager, CDH & Educational Programmes	Anjum.Alam@aku.edu
5	Educational Programmes	Gulizar Karaca	Manager, Educational Programmes	gulizar.karaca@aku.edu
6	Aga Khan Library	Waseem Farooq	Librarian	waseem.farooq@aku.edu
7	Finance	Rahil Hemani	Senior Manager, Academics-Finance	Rahil.Hemani@aku.edu
		Edward Grassby	Assistant Manager, Operations	Edward.Grassby@aku.edu
8	HR	Maha Paracha	HR Business Partner, HR	Maha.Paracha@aku.edu

AKU-UK Data Protection Policies

9	Publications	Donald Dinwiddie	Senior Coordinator, Publications	Donald.Dinwiddie@aku.edu
10	Research	Samantha Griffin	Research Grants Manager	Samantha.Griffin@aku.edu

16. ANNEX F – Data Processor List

S#	Organization Name	Contact Name	Telephone Number	Email	Address
1	The Aga Khan University	Shaukat Ali Khan	+922134863401	info.aku@aku.edu	Stadium Road, Karachi 74800

17. ANNEX G – Data Subject Consent Form

[Open form](#)

18. ANNEX H – Data Subject Consent Withdrawal Form

[Open form](#)

19. ANNEX I – Privacy by Design

Introduction

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. This approach ensures that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle. For example, when:

- building new IT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using data for new purposes

All projects that involve personal and/or sensitive information or intrusive technologies give rise to privacy issues and concerns. To ensure that such concerns, the project shall have a privacy by design focus. To achieve this a technique referred to as Privacy Impact Assessment shall be used.

It is vitally important to ensure that as AKU-UK progresses with new and/or shared processes, services and systems that the implementation does not result in an adverse impact on information quality or a breach of information security, confidentiality, or data protection requirements.

Article 23 of the General Data Protection Regulation mandates the Privacy by Design concept. The privacy by design approach is an essential tool in minimising privacy risks and building trust. Designing projects, processes, products or systems with privacy in mind at the outset can lead to:

- Identifying potential problems at an early stage, when addressing them will often be simpler and less costly
- Increased awareness of privacy and data protection concerns within the project
- Able to meet their legal requirements which leads to a reduced chance in any
- Data Protection breaches
- The project will not be stalled at a later point when producing information sharing protocols/agreements

Applicability

Privacy by Design applies to all staff who are involved within Project or Change management. It shall take place at the start of a new project or change to an existing project.

Privacy by Design Foundational Principles

The objectives of Privacy by Design – ensuring privacy protection and gaining personal control over one’s own information and, for organisations, gaining a sustainable competitive advantage – may be accompanied by practising the 7 Foundational Principles:

Proactive not Reactive; Preventative not Remedial

The Privacy by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. Privacy by Design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

Privacy as the Default Setting

Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.

Privacy Embedded into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

Full Functionality – Positive-Sum, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum win-win manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security – demonstrating that it is possible to have both.

End-to-End Security – Full Lifecycle Protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in

a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

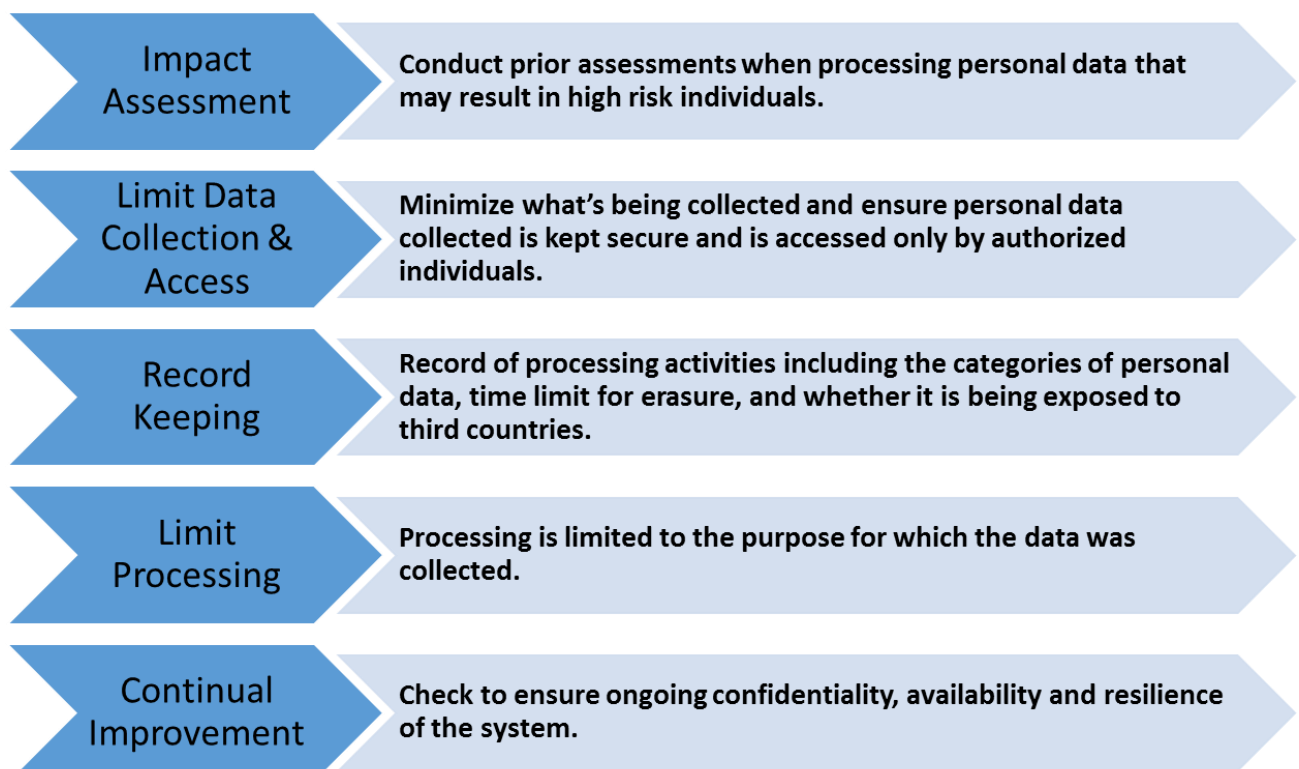
Visibility and Transparency – Keep it Open

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

Respect for User Privacy – Keep it User-Centric

Above all, Privacy by Design requires architects and operators to protect the interests of the individual by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Privacy by Design Process



20. ANNEX J – Legitimate Interest Assessment

Introduction

The legitimate interest assessment (LIA) procedure is intended to be used when it has been identified that the lawful basis of processing in a particular case might be based on legitimate interest.

Legitimate Interest Assessment Procedure

In order to fully establish, and be able to show, that legitimate interest is a reasonable basis for processing in a specific case, a three-part test must be applied.

This test requires AKU-UK to demonstrate:

- the precise nature of the legitimate interest (the Purpose test)
- that the processing is necessary for the legitimate interest (the Necessity test)
- that the data subject's interest, rights and freedoms do not override AKU-UK's legitimate interests (the Balancing test)

This procedure uses the Legitimate Interest Assessment Form (*refer below*) - which can be found at the end of this section - to document each of the above tests and provide evidence, when required, that a fair assessment has been carried out.

LIA must be revisited if AKU-UK becomes aware of any change in factors relating to its outcome. AKU-UK must conduct a new LIA if the purpose of processing changes.

The Purpose Test

The purpose test seeks to establish whether the interest stated is indeed legitimate for AKU-UK, or for a relevant third party. This test involves defining the exact reasons for the processing and the benefits of it.

The Necessity Test

In order for legitimate interest to be valid lawful basis for processing personal data, it has to be shown that the processing is actually required for the benefit to be gained. Consider whether there are other ways to achieve the objectives stated in the purpose test which does not involve processing personal data or involve less data to be processed.

The Balancing Test

Having established the nature of the interest, its benefits, the final step is to assess whether the identified interest overrides the privacy interests of the data subjects involved.

When the processing involves sensitive personal data, special care must be taken with the balancing test, as this may give additional weights to the rights of the data subject.

Assessment Decision

Once the three tests have been completed, an assessment must be made about whether, on balance, the processing may be considered to be lawful based on legitimate interest.

The decision made must be recorded on the Legitimate Interest Assessment Form together with the details of who carried out the assessment and when, and who approved the decision.

Legitimate Interest Assessment Form

In order to comply with Data Protection Act, it is important for AKU-UK to document the Legitimate Interests Balancing Test whenever they seek to rely on Legitimate Interest.

[Open form](#)

21. ANNEX K – Privacy Policy

By visiting our website, you agree with and are accepting the terms described in this Privacy Policy.

This Privacy Policy relates to data which is obtained by Aga Khan University (AKU) UK and for which AKU-UK is the Data Controller and/or Data Processor.

We take your privacy very seriously and are committed to ensuring that your privacy is protected through compliance. This Privacy Policy sets out how we use and protects any data that you may provide us. If you provide us with personal data, you can be assured that it will only be used in accordance with this privacy statement.

We will comply with data protection law and principles, which means that your data will be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes and not used in any way that is incompatible with those purposes.
- Accurate and kept up-to-date as provided by you.
- Kept only as long as necessary for the purposes it was collected.
- Kept securely.

Collection of personal data

We collect personal data about you when you:

- have made a complaint or enquiry to us.
- have been a patient with us.
- have done business with us.
- have made a data request to us.
- wish to attend, or have attended, an event.
- subscribe to our e-newsletters.
- have applied for a job or secondment with us.
- have worked with us or working with us.
- have made a donation to us.
- are studying or studied at one of our universities.

On certain occasions, we will ask you to provide us with certain data about yourself, which we will handle in accordance with the European Union's General Data Protection Regulation (GDPR) 2017/676.

AKU-UK Data Protection Policies

It is our policy to collect only the necessary data required to complete your request.

How will your personal data be secured?

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally necessitated to do so. In addition, we limit access to your personal data to those employees who have a business need-to-know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

Cookies

Additionally, when you use our website, data about how you use our website is collected automatically using “cookies”. Cookies are text files placed on your computer to collect standard internet log data and visitor behaviour data. This data is used to track visitor use of the website and to compile statistical reports on website activity.

Some of the pages on our site also use cookies set by carefully selected third party suppliers. None of our cookies store personal data. In addition to this, if you go on to a web page on our site that contains embedded content, for example a video from YouTube, you may be sent cookies from these websites. We don't control these cookies, so we suggest you check the third-party websites for more data about their cookies and how to manage them.

You can set your browser to not accept cookies and obtain up-to-date data about blocking and deleting cookies via www.aboutcookies.org

Use of personal data

We will not sell or lease your personal data to third parties unless we have your permission or are necessitated by law to do so.

We would like to send you email marketing communication which may be of interest to you from time to time. If you have consented to marketing, you may opt out later.

You have a right at any time to stop us from contacting you for marketing purposes. If you no longer wish to be contacted for marketing purposes, please click on the unsubscribe link at the bottom of the email or send an email to unsubscribe.aku@aku.edu with the subject line 'Unsubscribe'.

Disclosure of your data

We may disclose your personal data to companies and/or organisations who work with us in providing the website and associated services (such as analytics providers and website developers) and such companies and/or organisations are subject to a duty of confidentiality.

We may also disclose your personal data to third parties if we are under a duty to disclose or share your personal data in order to comply with any legal obligation or to protect the rights, property, or safety of AKU-UK, our users, or others. This includes exchanging data with other companies and organisations for the purposes of fraud protection.

We may disclose your personal data to third parties, the court service and/or regulators or law enforcement agencies in connection with proceedings or investigations anywhere in the world where compelled to do so. Where permitted and to the extent practicable, we will direct any such request to you or notify you before responding unless to do so would prejudice the prevention or detection of a crime (use justification: legal obligation, legal claims, legitimate interests (to cooperate with law enforcement and regulatory authorities)).

Legal grounds for processing personal data

We rely on one or more of the following processing conditions:

- rely on explicit consent;
- our legitimate interests in the effective delivery of data and services to you;
- to satisfy any legal and regulatory obligations to which we are subject or;
- to perform our contractual obligations to you.

Access to data

You have the right to request a copy of the data we hold about you. If you would like a copy of some or all your personal data, please email us at info.aku@aku.edu.

Retention of personal data

We will retain your personal data on our systems only for as long as we need it, given the purposes for which it was collected, or as necessitated to do so by law. We keep contact data (such as mailing list data) until a user unsubscribes or requests that we delete that data. If you choose to unsubscribe from a mailing list, we may keep certain limited data about you so that we may honour your request.

International Transfers

We may transfer your data outside the European Economic Area (EEA). Whenever we transfer your personal data out of the EEA, we will endeavour to take reasonable measures to maintain an adequate level of data protection.

Rights in relation to your data

You may have certain rights under data protection law in relation to the personal data we hold about you. In particular, you may have a right to (subject to the data protection law):

- request a copy of personal data we hold about you;
- ask that we update the personal data we hold about you, or correct such personal data that you think is incorrect or incomplete;
- ask that we delete the personal data that we hold about you, or restrict the way in which we use such personal data;
- object to our processing of your personal data; and/or
- withdraw your consent to our processing of your personal data (to the extent such processing is based on consent and consent is the only permissible basis for processing).

If you would like to exercise these rights or understand if these rights apply to you, please contact us by sending an email to info.aku@aku.com.

Third Party Website Links

Our website may contain links to other websites provided by third parties not under our controls. When following a link and providing data on that link please be aware that we are not responsible for the data provided to that third party. This privacy policy only applies to this website so when you link to other websites you should read their own privacy policies.

AKU-UK Data Protection Policies

Changes to this policy

We reserve the right to make any changes to our Privacy Policy. Any changes will be posted on this page and, where appropriate, notified to you by email. Please visit this page to check our most current privacy policy.

Contact

If you have any questions about our privacy policy or the data we hold about you, please email us at info.aku@aku.edu.

22. ANNEX L – Data Subject Consent Template

[Open template](#)