

فوري  Fawry

FAWRY

Data Protection Policy

A circular logo with a stylized blue arrow pointing up and to the right, similar to the one in the top left corner.

Version: 1.0
Status: Approved
Effective: 10-Jan-2022
Last Updated: -1 Jan - 2022

Document Control

Document Owner

Name	Eman Mohamed
Position	Head of InfoSec
Group/Department	Security Team

Approvals

Name	Designation	Date	Signature
Amani Fawzy	Chief Information Security Officer	Jan 2022	

Version Control

Ver.	Date	Description	Done By
1.0	Jan 2022	First completed version	Eman Mohamed
1.1			
1.2			

1. Purpose

The purpose of this document is to describe **Fawry's** responsibilities regarding the protection of personal data.

2. Principles of Processing Personal Data

There are based under a number of fundamental principles, such as:

- a) Personal data should be processed with fairness, lawfulness, and transparency toward the data subject
- b) Personal data should be collected for specified and legitimate purposes
- c) Personal data should be accurate and kept up to date
- d) Inaccurate personal data should be erased or rectified without delay
- e) Personal data should be processed and secured against any unlawful or unauthorized processing

Fawry shall ensure compliance with all of the abovementioned principles.

3.1 Rights of the Data Subject

The rights of the data subject are:

- a) The right of being informed
- b) The right to access
- c) The right to rectification
- d) The right to erasure
- e) The right to restrict processing
- f) The right to data portability
- g) The rights related to automated decision-making and profiling
- h) The right to object

Data subject rights are supported by appropriate procedures within **Fawry** that allow the required action to be taken within the timescales.

The timescales for data subject requests are shown in the table below.

Data Subject Request	Time scale
The right of being informed	Within one month (if the data is not supplied by the data subject)

The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The rights related to automated decision-making and profiling	Not specified
The right to object	On receipt of objection

3.2 Lawfulness of Processing

Fawry's policy specifies the appropriate actions that should be taken for documenting and processing a specific case of personal data. However, Fawry provides six alternative ways that can be used, depending on the case.

Consent: Except in specific reasons, Fawry should obtain consent from the data subject, prior to collecting and processing their data. For example, any case that involves children below the age 16 requires parental consent.

Contract performance: Explicit consent will not be required in cases where the collected and processed data are required for contract fulfillment, like cases when the contract cannot be finalized without the personal data. For example, if an address is missing in the delivery of a package, the delivery cannot be completed.

Legal obligation: Explicit consent will not be required in cases when the collected and processed data are required in order to comply with law. Taxation and employment can be examples of such cases.

Data subject's fundamental interests: A certain amount of data processing can be lawful under certain conditions (especially in the public sector), like cases when the data is needed to protect the subject's main interests or social care.

Carrying out tasks of public interest: The data subject's consent is not requested in cases where **Fawry** needs to perform a specific task that is of public interest.

Legitimate interests: Data processing is considered lawful in cases when the processing of personal data does not significantly affect the rights and freedoms of the data subject. However, the taking of such actions should be justified properly and documented.

3.3 Data Protection by Design

Fawry should adopt the principle of data protection by design and ensure that the systems collecting personal data consider privacy issues. The systems should also successfully complete one or more data protection impact assessment.

The data protection impact assessment (DPIA) includes the following:

- Determine the purpose of processing the personal data
- Determine whether the processing of personal data is necessary
- Identify the necessary controls to address the risks and comply with the legislation

In order to respect personal data privacy, **Fawry** can use techniques, such as data minimization and pseudonymization.

3.4 Processing Personal Data Contracts

Fawry should ensure that all of the personal data used are subject to a contract.

3.5 Breach Notification

In any case related to breaches of personal data, **Fawry** is responsible for considering actions that should be taken and inform the affected parties.

if a breach of personal data occurs, the relevant authority should be informed within 72 hours. These cases should be managed based on the Information Security Incident Response Procedure, which provides the process of handling information security incidents.