ESCCOM

ESWATINI
COMMUNICATIONS
COMMISSION

DATA PROTECTION

DATA PROTECTION

Data protection is the process of safeguarding important data from corruption, unlawful disclosure, compromise or loss and providing the capability to restore the data to a functional state should something happen to render the data inaccessible or unusable. Data protection rules apply to personal data that can identify individuals, such as their name, ID number, email address, or their address. Therefore, data protection is essential for security, privacy, compliance, as well as for innovation and trust in today's digital economy.

Data laws vary across countries and Eswatini has enacted the Data Protection Act, 2022 which designates Eswatini Communications Commission (ESCCOM) as the Eswatini Data Protection Authority (DPA), guarantees rights of data subjects and lays down principles for the processing of personal information.

RIGHTS OF DATA SUBJECTS (INDIVIDUALS)

The right to be informed
The right to be informed means businesses as data controllers must give individuals clear, succinct and easily understandable information on what they want to do with the data. This fosters a level of trust.

Companies dealing in data must provide privacy information including the name and contact details of the organisation, the representative, the Data Protection Officer, the purpose of data collection and processing, the legitimate interests for processing as well as retention periods.

The right to rectification
Individual data subjects have the right to rectify or correct inaccurate personal data or have it fully completed if the information is not complete. They can request rectification in writing or verbally and the company has one calendar month to respond to a request for rectification.

The right of access
The right of access gives individuals the legal right to a copy of their personal data and any other supplementary data. Individuals have a right to access regarding their personal data as held by a company. A subject access request can be made to the company concerned either verbally or in writing, and the company has 30 days to respond.

Individuals are not entitled to request access to information that relates to other people.

The right to erasure
Also called 'the right to be forgotten', means individuals can request that their data is erased permanently from the controller's databases. The request can be made verbally or in writing and the company must respond within 30 days. This right only applies in certain circumstances and is not absolute.

The right to restrict processing
Individuals have the right to suppress or block their personal data from being used. This is not absolute and applies to specific circumstances.

The right to data portability
This allows individuals to obtain and use their personal data for their own reasons. It means they can copy, transfer or move personal data from one online environment to another, safely and securely and in a frequently used machine readable format.

The right to object
Individuals have the absolute right to object to their personal data being used for marketing reasons. In other circumstances, they may also object to how their data is being processed.

Rights regarding automated profiling and decision making
Automated profiling refers to the use of technology to processing and analyse the individual's personal data. Automated individual decision-making means the resolutions taken by automation with no involvement from humans. The individual must be informed of the automated profiling and decision making, and there must be easy ways for them to challenge an automated decision or ask for a human being to check it.

THE SEVEN DATA PROTECTION PRINCIPLES

Lawfulness, Fairness & Transparency

There must be a valid legal reason for the processing of personal data. Data controllers and processors must disclose fully the reasons for collecting the data, and how it will be used.

Accountability

This is the big one, the foundation on which the other six principles rest. A data controller or processor must be able to evidence their accountability by demonstrating how they take responsibility for how they use people's data.

Purpose Limitation

Personal data must be used only for the purpose that it was collected for.

Integrity & Confidentiality

Data controllers and processors must keep personal data safe so that it does not get accidentally deleted or changed, or seen by someone who is not allowed to see it.

Minimisation

The data collected from individuals or organisation must be the minimum necessary.

Storage Limitation

Data controllers and processors must not keep personal data for longer than it is needed.

Accuracy

The data controller or processor must ensure that any personal data that they hold is accurate and where necessary, up-to-date.

CONTACT US

+268 2406 7000
info@esccom.org.sz
Eswatini Communications Commission
@ESCCOM_Eswatini
Eswatini Communications Commission
www.esccom.org.sz