DPC Art. 18

Security of Processing

TITLE 03 — OBLIGATIONS OF CONTROLLERS AND PROCESSORS · CHAPTER 01 — GENERAL OBLIGATIONS

1 Taking into account the state of the art, the costs of implementation, the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, as appropriate:

a. the pseudonymisation and encryption of personal data;

b. the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;

c. the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2 In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, including from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed.

3 The controller and the processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process that data except on instructions from the controller, unless required to do so by the laws of the State.

4 All State data is held electronically and is necessarily stored across foreign jurisdictions. Accordingly:

a. encryption at rest and encryption in transit shall be mandatory for all processing of personal data carried out by the State and its organs, departments, agencies, and instrumentalities;

b. the State shall employ cryptographic standards that are recognised as current best practice by internationally accepted standards bodies;

c. access to personal data held by the State shall be subject to multi-factor authentication and role-based access control;

d. the State shall maintain comprehensive audit logs of all access to and processing of personal data, and such logs shall themselves be protected against tampering.

5 Adherence to approved codes of conduct or certification mechanisms may be used to demonstrate compliance with this Article, in accordance with Article 15(4).

6 The controller and the processor shall regularly review and, where necessary, update the security measures referred to in this Article, taking into account technological developments, changes in the threat environment, and any incidents that have occurred.

DOCUMENT INFORMATION	
CITATION	DPC Art. 18 — “Security of Processing”, *Data Protection Code of Kaharagia* (2026).
STATUS	In force
SOURCE	`https://kahalex.kaharagia.org/article/data-protection/18`