THE CODES OF KAHARAGIA

Data Protection Code of Kaharagia

VOLUME V

Data Protection Code of Kaharagia

The Processing of Personal Data of Nationals and Residents.

PUBLISHED BY

THE SOVEREIGN'S PRINTER

ROYAL CHANCELLERY, KAHARAGIA

2026

Data Protection Code of Kaharagia

The Processing of Personal Data of Nationals and Residents.

Published by

THE SOVEREIGN'S PRINTER

Royal Chancellery, Kaharagia

First edition, 2026. First impression.

This edition reproduces the Code as in force at the status date below. The authoritative text is that published in KáhaLex; where this volume differs from it, the published text governs. This volume is a faithful reproduction and not an independent authority.

Enacted by Sovereign Decree SD-2026-0007, given 16/07/2026, taking effect upon signature

Cite as DPC Art. N — "Heading", Data Protection Code of Kaharagia (2026)

Text kahalex.kaharagia.org/codes/data-protection

Decree gazette.kaharagia.org/sovereign-decrees/sd-2026-0007

Status All 30 Articles in force from 16/07/2026; text as at 12/08/2026

KPN 549-720-26-0005-6

Set in Merriweather and Inter. Typeset in Kaharagia.

Enacting Decree

The Code is Annex A of the Decree below, which provides that the Annex forms an integral and binding part of it. Reproduced from the engrossed record; the Decree's Articles are numbered in roman, the Code's in arabic.

SD-2026-0007

Sovereign Decree Establishing and Enacting the Data Protection Code of Kaharagia

BY THE GRACE OF GOD

WE MAXIMILIAN

PRINCE OF KAHARAGIA

etc., etc., etc.,

WHEREAS respect for human dignity and private life requires the lawful and secure protection of personal data;

WHEREAS the digital administration of the State requires clear rules governing the collection, use, storage, disclosure, and security of such data;

WHEREAS the Data Protection Code of Kaharagia has been prepared for this purpose and ought now to be given full force and effect;

NOW, THEREFORE, WE, in Our Sovereign capacity and having duly considered the advice of Our Counsel, do hereby decree as follows:

Article I — Establishment and Enactment

1. The Data Protection Code of Kaharagia, comprising Articles 1 through 30 and set forth in Annex A, is hereby established, enacted, and promulgated as law within the State.

2. Annex A forms an integral and binding part of this Decree and shall have full force and effect accordingly.

Article II — Application and Interpretation

1. Subject always to the Fundamental Laws and Principles of Kaharagia, the Data Protection Code of Kaharagia shall govern the collection, use, storage, disclosure, security, and lawful processing of personal data, together with the rights of data subjects and the duties of those responsible for such processing.

2. All existing laws, decrees, regulations, and other instruments shall be interpreted and applied consistently with the Data Protection Code of Kaharagia and shall have no force to the extent of any inconsistency.

3. The authenticated text of the Data Protection Code of Kaharagia shall be maintained by the Royal Chancellery and reproduced in KáhaLex without substantive alteration.

Article III — Enactment and Publication

1. This Decree and Annex A shall take effect immediately upon Our Signature.

2. They shall be entered into the Royal Kaharagian Gazette and published accordingly.

GIVEN *under Our Hand and the Great Seal of Our Principality, at Our Court in Detroit, This 16th day of July, in the year of Our Lord Two Thousand and Twenty-Six, and the Seventeenth of Our Reign.*

Maximilian P.

Contents

Note on Citation

An Article of this Code is cited by the abbreviation, the Article number, and where helpful the heading, for example DPC Art. 1. A numbered paragraph within an Article is cited by its number and a sub-paragraph by its letter, so that DPC Art. 1(3)(b) refers to the second sub-paragraph of paragraph (3) of Article 1.

A reference in the form DPC Art. N is to an Article of this Code; the other instruments in the corpus are cited in the same way. The abbreviations are FN for the Fundamental Laws and Principles of Kaharagia, CC for the Civil Code of Kaharagia, CR for the Criminal Code of Kaharagia, Nat for the Nationality Code of Kaharagia, and DPC for the Data Protection Code of Kaharagia (this volume).

Every Article printed here was in force at the status date on the imprint page. This volume is a faithful reproduction and not an independent authority; where it differs from the text published in KáhaLex, the published text governs.

The Codes of Kaharagia

The corpus of enacted law. Each instrument was established by the Sovereign Decree named against it, given 16/07/2026 and taking effect upon signature. The authenticated text of each is maintained by the Royal Chancellery and published in KáhaLex.

Title 01 — General Provisions

Articles 1–6

Chapter 01 — Scope and Definitions

Article 1 — Purpose and Scope

(1) This Code is enacted pursuant to Article 46(5) of the Fundamental Laws of the State of the Kaharagians and establishes the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of such data within the Kaharagian legal order.

(2) This Code protects the fundamental right to the protection of personal data of every natural person whose data is processed within the scope defined by this Article.

(3) This Code applies to the processing of personal data carried out by:

(a) the State and all its organs, departments, agencies, and instrumentalities;

(b) Kaharagian legal persons, wherever they may be established or operate;

(c) any natural or legal person who has submitted to the jurisdiction of the State, to the extent that such processing concerns the personal data of Kaharagian nationals, residents, or other persons whose data falls within the Kaharagian legal order.

(4) This Code does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity that has no connection to a professional, commercial, or official purpose.

(5) The State of the Kaharagians exercises sovereignty on a personal and digital basis without physical territory. The provisions of this Code shall be interpreted in light of this character.

(6) Nothing in this Code shall be construed so as to diminish or restrict the rights and freedoms guaranteed by the Fundamental Laws. Where a provision of this Code conflicts with a provision of the Fundamental Laws, the Fundamental Laws shall prevail.

Article 2 — Definitions

(1) For the purposes of this Code, the following definitions apply:

(a) **"personal data"** means any information relating to an identified or identifiable natural person (the "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person;

(b) **"sensitive personal data"** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation;

(c) **"processing"** means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, restriction, erasure, or destruction;

(d) **"controller"** means the natural or legal person, public authority, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the State or one of its organs determines the purposes and means of processing, the State or the relevant organ shall be regarded as the controller;

(e) **"processor"** means a natural or legal person, public authority, or other body which processes personal data on behalf of the controller;

(f) **"data subject"** means an identified or identifiable natural person whose personal data is the object of processing;

(g) **"consent"** means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which the data subject, by a clear affirmative act, signifies agreement to the processing of personal data relating to him or her;

(h) **"personal data breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;

(i) **"supervisory authority"** means the independent authority established or designated under this Code to monitor and enforce the application of the data protection rules of the State;

(j) **"third party"** means a natural or legal person, public authority, or body other than the data subject, the controller, the processor, and the persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(k) **"recipient"** means a natural or legal person, public authority, or body to which personal data is disclosed, whether or not such person, authority, or body is a third party;

(l) **"filing system"** means any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised, or dispersed on a functional or geographical basis.

Article 3 — Application

(1) This Code applies to the processing of personal data by the State and all of its organs, irrespective of whether the processing takes place within or outside the infrastructure of any host jurisdiction.

(2) This Code applies to the processing of personal data by Kaharagian legal persons, regardless of where such legal persons are established, operate, or maintain their technical infrastructure.

(3) This Code applies to the processing of personal data of Kaharagian nationals and of persons who have submitted to the jurisdiction of the State, where such processing is carried out by any person or entity that has itself submitted to Kaharagian jurisdiction.

(4) The application of this Code is not dependent on the physical location of data storage, data processing equipment, or communications infrastructure. The State exercises personal jurisdiction over data processing activities in accordance with the principles set out in the Fundamental Laws, and the territorial location of data shall not, of itself, exclude the applicability of this Code.

(5) Where the mandatory law of a host jurisdiction in which a Kaharagian organ, legal person, or natural person operates imposes data protection obligations that conflict with this Code, the mandatory law of the host jurisdiction shall prevail to the extent of the conflict, in accordance with Article 42(1) of the Fundamental Laws. The controller shall document any such conflict and the measures taken to comply with both legal orders to the greatest extent possible.

(6) Where personal data is processed jointly by a Kaharagian controller and a controller subject to a foreign legal order, this Code applies to the processing activities carried out by or on behalf of the Kaharagian controller.

Chapter 02 — Principles

Article 4 — Lawfulness of Processing

(1) Processing of personal data shall be lawful only if, and to the extent that, at least one of the following conditions is met:

(a) the data subject has given consent to the processing of his or her personal data for one or more specified purposes;

(b) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;

(c) the processing is necessary for compliance with a legal obligation to which the controller is subject under Kaharagian law or, where applicable, the mandatory law of a host jurisdiction;

(d) the processing is necessary to protect the vital interests of the data subject or of another natural person;

(e) the processing is necessary for the purposes of the legitimate interests pursued by the State, its organs, or a Kaharagian legal person, except where such interests are overridden by the fundamental rights and freedoms of the data subject.

(2) Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing. Consent shall

be given by a clear affirmative act establishing a freely given, specific, informed, and unambiguous indication of the data subject's agreement. Silence, pre-ticked boxes, or inactivity shall not constitute consent.

(3) The data subject shall have the right to withdraw consent at any time. The withdrawal of consent shall not affect the lawfulness of processing carried out on the basis of consent before its withdrawal. Prior to giving consent, the data subject shall be informed of the right to withdraw. Withdrawal of consent shall be as easy to effect as its grant.

(4) Where the processing of personal data is based on the legitimate interests of the State or a Kaharagian legal person under paragraph 1(e), the controller shall conduct and document a balancing assessment, weighing the interests pursued against the rights and freedoms of the data subject, having particular regard to the reasonable expectations of the data subject.

(5) The processing of sensitive personal data as defined in Article 2(1)(b) shall be prohibited unless:

(a) the data subject has given explicit consent to the processing for one or more specified purposes;

(b) the processing is necessary for reasons of substantial public interest under Kaharagian law, on the basis of provisions that are proportionate to the aim pursued and that provide appropriate safeguards for the rights of the data subject;

(c) the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) the processing relates to personal data which has been manifestly made public by the data subject;

(e) the processing is necessary for the establishment, exercise, or defence of legal claims before Kaharagian authorities or tribunals.

Article 5 — Purpose Limitation and Data Minimisation

(1) Personal data shall be collected for specified, explicit, and legitimate purposes and shall not be further processed in a manner that is incompatible with those purposes. Further processing for archival purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered incompatible with the original purposes, provided that appropriate technical and organisational safeguards are in place.

(2) The controller shall clearly identify and document the purposes of processing before any personal data is collected. Any change in purpose shall be assessed for compatibility with the original purpose, taking into account:

(a) the link between the original purpose and the proposed new purpose;

(b) the context in which the personal data was collected, in particular the relationship between the data subject and the controller;

(c) the nature of the personal data, and in particular whether sensitive personal data as defined in Article 2(1)(b) is involved;

(d) the possible consequences of the intended further processing for the data subject;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

(3) Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. The controller shall not collect personal data beyond what is strictly required to achieve the stated purpose.

(4) Where the purpose of processing can be achieved using anonymised or pseudonymised data, the controller shall prefer anonymisation or, where that is not feasible, pseudonymisation over the processing of directly identifiable personal data.

(5) The controller shall periodically review the personal data held to ensure that it remains adequate, relevant, and necessary for the purposes of processing, and shall erase or anonymise any personal data that no longer satisfies those criteria.

Article 6 — Accuracy, Storage Limitation, and Accountability

(1) Personal data shall be accurate and, where necessary, kept up to date. The controller shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without undue delay.

(2) The controller shall establish appropriate mechanisms, including electronic self-service facilities where feasible, to enable data subjects to verify and, where appropriate, request the correction of their personal data.

(3) Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the data will be processed solely for:

(a) archival purposes in the public interest;

(b) scientific or historical research purposes; or

(c) statistical purposes,

provided that appropriate technical and organisational measures are implemented to safeguard the rights and freedoms of the data subject, including, where practicable, pseudonymisation.

(4) The controller shall establish and document a data retention policy specifying the retention periods for each category of personal data processed. The retention policy shall be reviewed at regular intervals and made available to the supervisory authority upon request.

(5) Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organisational measures. Such measures shall include, as appropriate:

(a) encryption of personal data in transit and at rest;

(b) access controls and authentication mechanisms;

(c) logging and audit trails of processing activities;

(d) regular testing, assessment, and evaluation of the effectiveness of security measures.

(6) The controller shall be responsible for, and shall be able to demonstrate compliance with, the principles set out in Article 4, Article 5, and the preceding paragraphs of this Article. This obligation includes maintaining records of processing activities, conducting impact assessments where required, and cooperating with the supervisory authority.

(7) Where the controller engages a processor, the controller shall ensure, by means of a written agreement or other binding instrument, that the processor provides sufficient guarantees to implement appropriate technical and organisational measures such that the processing meets the requirements of this Code and ensures the protection of the rights of the data subject.

Title 02 — Rights of Data Subjects

Articles 7–14

Chapter 01 — Consent and Information

Article 7 — Conditions for Valid Consent

(1) Where processing is based on consent pursuant to Article 4, the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data for one or more specific purposes.

(2) Consent shall be valid only where it is freely given, specific, informed, and unambiguous. Consent shall be expressed by a clear affirmative act establishing the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement transmitted through electronic means, an oral declaration recorded in verifiable form, or any other conduct that clearly indicates acceptance in the given context. Silence, pre-ticked boxes, or inactivity shall not constitute consent.

(3) Where consent is given in the context of a written declaration or an electronic form that also concerns other matters, the request for consent shall be presented in a manner that is clearly distinguishable from those other matters. The request shall be formulated in clear and plain language and shall not contain unfair or misleading terms. Any part of such a declaration or form that constitutes an infringement of this Code shall not be binding.

(4) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed of this right. The mechanism for withdrawing consent shall be as easy to execute as the mechanism for giving consent. Where consent was given through an electronic interface, withdrawal shall be possible through the same interface or an equally accessible one.

(5) When assessing whether consent is freely given, utmost account shall be taken of whether, among other things, the performance of a contract or the provision of a service is conditional on consent to the processing of personal data that is not necessary for the performance of that contract or the provision of that service. Consent shall not be regarded as freely given where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority of the State.

(6) Consent for the processing of sensitive personal data as defined in this Code shall be explicit. Explicit consent requires a specific, unambiguous, and affirmative statement or action by the data subject that clearly refers to the particular categories of sensitive personal data to be processed and the purposes of such processing.

(7) Where the data subject is a minor under the applicable provisions of the Civil Code of the State, the processing of personal data shall be lawful only where and to the extent that consent is given or authorised by the holder of parental authority or legal guardianship over the minor. The controller shall make reasonable

efforts, taking into account available technology, to verify that consent is given or authorised by the holder of parental authority or legal guardian.

(8) The burden of demonstrating that valid consent has been obtained shall rest with the controller. The controller shall maintain records sufficient to demonstrate compliance with the requirements of this Article, including the identity of the data subject, the date and time of consent, the information presented to the data subject at the time of consent, and the method by which consent was given.

Article 8 — Right to Information at Collection

(1) Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) The identity and contact details of the controller and, where applicable, of the controller's representative within the State.

(b) The contact details of the data protection officer, where one has been designated.

(c) The purposes of the processing for which the personal data are intended, as well as the legal basis for the processing pursuant to Article 4.

(d) Where processing is based on the legitimate interests of the controller or of a third party pursuant to Article 4, the specific legitimate interests pursued by the controller or by the third party.

(e) The recipients or categories of recipients of the personal data, if any.

(f) The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

(g) The existence of the right to request from the controller access to and rectification or erasure of personal data, restriction of processing, the right to object to processing, and the right to data portability, in accordance with this Title.

(h) Where processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

(i) The right to lodge a complaint with the competent supervisory authority of the State.

(j) Whether the provision of personal data is a requirement arising from law, from a contract, or a condition necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

(2) Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject, prior to that further processing, with information on that other purpose and with any relevant further information as referred to in paragraph 1.

(3) The information referred to in paragraphs 1 and 2 shall be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. The information shall be provided in writing, or by electronic means where appropriate. When requested by the data subject, the information may also be provided orally, provided that the identity of the data subject is established by other means.

(4) Where the controller provides its services through electronic interfaces, the information required under this Article shall be made persistently available through those interfaces in a manner that is easily navigable and retrievable by the data subject at any time.

(5) The information required under this Article shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may charge a reasonable fee taking into account the administrative costs of providing the information, or may refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 9 — Right to Information About Processing

(1) Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) All information specified in Article 8, paragraph 1.

(b) The categories of personal data concerned.

(c) The source from which the personal data originate, and where applicable, whether the data came from publicly accessible sources.

(2) The controller shall provide the information referred to in paragraph 1 within a reasonable period after obtaining the personal data, but at the latest within thirty days, having regard to the specific circumstances in which the personal data are processed. Where the personal data are to be used for communication with the data subject, the information shall be provided at the latest at the time of the first communication to that data subject. Where disclosure to another recipient is envisaged, the information shall be provided at the latest when the personal data are first disclosed.

(3) Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject, prior to that further processing, with information on that other purpose and with any relevant further information in accordance with paragraph 1.

(4) The provisions of paragraphs 1, 2, and 3 shall not apply where and insofar as:

(a) The data subject already has the information.

(b) The provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes. In such cases, the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available, and shall document the reasons for which it considers the effort disproportionate.

(c) Obtaining or disclosure of the data is expressly laid down by the law of the State to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests.

(d) The personal data must remain confidential subject to an obligation of professional secrecy regulated by the law of the State, including a statutory obligation of secrecy.

(5) The information required under this Article shall be provided in accordance with the form and accessibility requirements set out in Article 8, paragraphs 3 and 4.

Chapter 02 — Access, Rectification, and Erasure

Article 10 — Right of Access

(1) The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed. Where such processing is taking place, the data subject shall have the right to access the personal data and the following information:

(a) The purposes of the processing.

(b) The categories of personal data concerned.

(c) The recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in foreign jurisdictions or international organisations.

(d) Where possible, the envisaged period for which the personal data will be stored, or if not possible, the criteria used to determine that period.

(e) The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject, or to object to such processing.

(f) The right to lodge a complaint with the competent supervisory authority of the State.

(g) Where the personal data are not collected from the data subject, any available information as to their source.

(h) The existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(2) Where personal data are transferred to a foreign jurisdiction or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards applied in relation to the transfer.

(3) The controller shall provide a copy of the personal data undergoing processing. The first copy shall be provided free of charge. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic format.

(4) The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, that consideration shall not result in a refusal to provide all information to the data subject.

(5) The controller shall respond to a request under this Article without undue delay and in any event within thirty days of receipt of the request. That period may be extended by a further thirty days where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within the initial thirty-day period, together with the reasons for the delay.

(6) Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 11 — Right to Rectification

(1) The data subject shall have the right to obtain from the controller, without undue delay, the rectification of inaccurate personal data concerning him or her. Having regard to the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

(2) Upon rectification or completion of personal data pursuant to paragraph 1, the controller shall, without undue delay, take all reasonable steps to ensure that the rectified or completed data are accurate and consistent across all systems and records under the controller's authority.

(3) The controller shall communicate any rectification of personal data carried out in accordance with paragraph 1 to each recipient to whom the personal data have

been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

(4) Where the data subject contests the accuracy of the personal data but the controller considers the data to be accurate, the controller shall not erase the contested data but shall clearly mark the data as contested and shall retain both the original data and the data subject's position regarding its accuracy until the matter is resolved.

(5) The procedural requirements of Article 10, paragraphs 5 and 6, apply to requests under this Article.

Article 12 — Right to Erasure

(1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay, and the controller shall have the obligation to erase personal data without undue delay, where one of the following grounds applies:

(a) The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

(b) The data subject withdraws consent on which the processing is based in accordance with Article 7, and there is no other legal ground for the processing.

(c) The data subject objects to the processing and there are no overriding legitimate grounds for the processing.

(d) The personal data have been unlawfully processed.

(e) The personal data have to be erased for compliance with a legal obligation under the law of the State to which the controller is subject.

(f) The personal data have been collected in relation to the offer of information society services to a minor, as referred to in Article 7, paragraph 7.

(2) Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller shall, taking account of available technology and the cost of implementation, take reasonable steps, including technical measures, to inform controllers that are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

(3) Paragraphs 1 and 2 shall not apply to the extent that processing is necessary for:

(a) The exercise of the right of freedom of expression and information.

(b) Compliance with a legal obligation that requires processing by the law of the State to which the controller is subject, or for the performance of a task carried out in the public interest.

(c) Archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, insofar as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing.

(d) The establishment, exercise, or defence of legal claims before the courts or administrative bodies of the State or of any other jurisdiction.

(4) Where erasure is carried out, it shall be complete and irreversible, encompassing all copies, replications, and backups of the personal data within the controller's systems, except where retention of specific copies is required by law or falls within the exceptions set out in paragraph 3. The controller shall document the erasure, including the date on which it was effected and the scope of data erased.

(5) The controller shall communicate any erasure of personal data carried out in accordance with paragraph 1 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

(6) The procedural requirements of Article 10, paragraphs 5 and 6, apply to requests under this Article.

Chapter 03 — Additional Rights

Article 13 — Right to Restriction of Processing

(1) The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.

(b) The processing is unlawful and the data subject opposes the erasure of the personal data pursuant to Article 12 and requests the restriction of their use instead.

(c) The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise, or defence of legal claims.

(d) The data subject has objected to processing pending the verification of whether the legitimate grounds of the controller override those of the data subject.

(2) Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent, or for the establishment, exercise, or defence of legal claims, or for the protection of the rights of another natural or legal person, or for reasons of important public interest of the State.

(3) A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted. The controller shall provide such notice within a reasonable period before lifting the restriction, affording the data subject the opportunity to take any further action in protection of his or her rights.

(4) Where restriction of processing is applied, the controller shall clearly mark the data concerned to ensure that the restriction is respected across all systems and by all persons authorised to process data on behalf of the controller.

(5) The controller shall communicate any restriction of processing carried out in accordance with paragraph 1 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

(6) The procedural requirements of Article 10, paragraphs 5 and 6, apply to requests under this Article.

Article 14 — Right to Data Portability

(1) The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used, and machine-readable format, and shall have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

   (a) The processing is based on consent pursuant to Article 7, or on a contract to which the data subject is party; and

   (b) The processing is carried out by automated means.

(2) In exercising the right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible. Controllers shall not erect unnecessary technical barriers to such direct transmission.

(3) The exercise of the right referred to in paragraph 1 shall be without prejudice to Article 12. The exercise of the right to portability shall not constitute a request for erasure unless the data subject expressly indicates otherwise.

(4) The right to data portability shall not adversely affect the rights and freedoms of others. In particular, where the personal data concern more than one data subject, the controller shall not transmit such data where doing so would infringe upon the data protection rights of another data subject, unless appropriate measures are taken to safeguard those rights or unless the other data subject has consented to the transmission.

(5) The data referred to in paragraph 1 shall be provided in a format that complies with open, interoperable standards where such standards exist and are reasonably applicable. The controller shall document the format in which the data

are provided and shall make available to the data subject a description of the structure and content of the data sufficient to enable its meaningful reuse.

(6) The procedural requirements of Article 10, paragraphs 5 and 6, apply to requests under this Article.

(7) The right to data portability shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Title 03 — Obligations of Controllers and Processors

Articles 15–23

Chapter 01 — General Obligations

Article 15 — Responsibility of the Controller

(1) The controller shall implement appropriate technical and organisational measures to ensure that processing is performed in accordance with this Code and shall be able to demonstrate such compliance. Those measures shall take into account the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

(2) The measures referred to in paragraph 1 shall include, where appropriate:

(a) the adoption and implementation of written data protection policies setting out the controller's approach to the protection of personal data, including the allocation of responsibilities within the controller's organisation;

(b) the designation of qualified personnel or an external service provider responsible for overseeing compliance with this Code;

(c) the establishment of internal procedures for the handling of data subject requests pursuant to Title II of this Code;

(d) the implementation of technical safeguards, in particular encryption, pseudonymisation, access controls, and audit logging;

(e) the conduct of regular training and awareness programmes for all persons who process personal data under the authority of the controller.

The supervisory authority may publish guidance on the circumstances in which the adoption of formal data protection policies under sub-paragraph (a) is to be considered proportionate.

(3) The controller shall review and, where necessary, update the measures referred to in paragraphs 1 and 2 at regular intervals and in any event whenever there is a material change in the nature, scope, context, or purposes of processing, or whenever new risks are identified.

(4) Adherence to approved codes of conduct referred to in this Code or to an approved certification mechanism may be used as an element by which to demonstrate compliance with the obligations of the controller under this Article.

(5) The controller shall be responsible for, and shall be able to demonstrate compliance with, the principles set out in Article 4, Article 5, and Article 6 of this Code.

Article 16 — Data Protection by Design and by Default

(1) Taking into account the state of the art, the cost of implementation, the nature, scope, context, and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the

means for processing and at the time of the processing itself, implement appropriate technical and organisational measures designed to implement the data protection principles set out in this Code in an effective manner and to integrate the necessary safeguards into the processing.

(2) Such measures shall include:

(a) pseudonymisation and, where feasible, anonymisation of personal data at the earliest possible stage of processing;

(b) minimisation of the personal data collected and processed, so that only data which is necessary for the specific purpose is obtained;

(c) the application of access controls that restrict the processing of personal data to authorised personnel on a need-to-know basis;

(d) the separation of personal data from other categories of data where such separation enhances the protection of data subjects.

(3) The controller shall, by default, ensure that only personal data which is necessary for each specific purpose of the processing is processed. That obligation applies to:

(a) the amount of personal data collected;

(b) the extent of processing carried out;

(c) the period for which personal data is stored;

(d) the accessibility of personal data, including ensuring that personal data is not made accessible without the individual's intervention to an indefinite number of natural persons.

(4) Encryption of personal data and the use of secure communication protocols shall constitute the presumptive standard for all processing. A controller who does not employ encryption at rest and in transit shall bear the burden of demonstrating that an equivalent or superior level of protection is achieved by alternative measures.

(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).

Article 17 — Records of Processing Activities

(1) Each controller shall maintain a record of processing activities under its responsibility. That record shall contain the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller and the data protection officer or designated compliance contact;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and the categories of personal data processed;

(d) the categories of recipients to whom the personal data has been or will be disclosed, including recipients in foreign jurisdictions;

(e) where applicable, a description of transfers of personal data to foreign jurisdictions, including the identification of those jurisdictions and, in the case of transfers in the absence of an adequacy determination under Article 22, the documentation of the appropriate safeguards relied upon;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 18(1).

(2) Each processor shall maintain a record of all categories of processing activities carried out on behalf of a controller. That record shall contain the following information:

(a) the name and contact details of the processor or processors and of each controller on whose behalf the processor is acting, and, where applicable, the data protection officer or designated compliance contact of the controller or the processor;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, a description of transfers of personal data to foreign jurisdictions, including the identification of those jurisdictions and the documentation of the appropriate safeguards relied upon;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 18(1).

(3) The records referred to in paragraphs 1 and 2 shall be maintained in writing, including in electronic form. Electronic record-keeping shall be the standard means of compliance with this obligation.

(4) The controller or the processor shall make the records referred to in this Article available to the supervisory authority on request. The supervisory authority may prescribe the format in which such records are to be maintained or transmitted.

(5) The obligations set out in paragraphs 1 and 2 shall not apply to a controller or processor employing fewer than five persons, unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes sensitive personal data as defined in Article 2 of this Code.

Article 18 — Security of Processing

(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.

Chapter 02 — Data Breach and Impact Assessment

Article 19 — Notification of Personal Data Breach

(1) In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than seventy-two hours after having become aware of it, notify the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within seventy-two hours, it shall be accompanied by reasons for the delay.

(2) The processor shall notify the controller without undue delay after becoming aware of a personal data breach. The processor shall provide the controller with sufficient information to enable the controller to fulfil its obligations under this Article.

(3) The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point from whom more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(4) Where, and in so far as, it is not possible to provide the information referred to in paragraph 3 at the same time as the initial notification, the information may be provided in phases without undue further delay.

(5) The controller shall document any personal data breaches, including the facts relating to the personal data breach, its effects, and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

(6) Where a controller has engaged a processor and the personal data breach occurs in respect of personal data processed by the processor, the processor shall provide the notification referred to in paragraph 2 through the same secure electronic means by which it ordinarily communicates with the controller, unless the controller has specified an alternative channel for breach notifications.

Article 20 — Communication of Breach to Data Subjects

(1) When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

(2) The communication to the data subject referred to in paragraph 1 shall describe in clear and plain language the nature of the personal data breach and shall contain at least:

(a) the name and contact details of the data protection officer or other contact point from whom more information can be obtained;

(b) a description of the likely consequences of the personal data breach;

(c) a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;

(d) recommendations for the data subject to take in order to protect himself or herself against the potential consequences of the breach, including, where relevant, the changing of passwords, the monitoring of accounts, or the exercise of rights under Title II of this Code.

(3) The communication to the data subject referred to in paragraph 1 shall not be required where any of the following conditions is met:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) the communication would involve disproportionate effort, in which case there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

(4) Where the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require the controller to do so or may decide that any of the conditions referred to in paragraph 3 is met.

(5) Communications to data subjects under this Article shall be transmitted through the same electronic channels by which the controller ordinarily communicates with the data subject, and shall additionally be made available through the controller's primary electronic interface, where one exists.

Article 21 — Data Protection Impact Assessment

(1) Where a type of processing, in particular using new technologies and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

(2) A data protection impact assessment shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of sensitive personal data as defined in Article 2 of this Code;

(c) systematic monitoring of a publicly accessible area or service on a large scale, including the monitoring of digital spaces, platforms, or communications services operated by or on behalf of the State.

(3) The supervisory authority shall establish and make public a list of the kinds of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority may also establish and make public a list of the kinds of processing operations for which no data protection impact assessment is required.

(4) The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1;

(d) the measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Code, taking into account the rights and legitimate interests of data subjects and other persons concerned.

(5) Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

(6) Where the assessment under paragraph 4 indicates that the processing would result in a high residual risk notwithstanding the measures envisaged by the

controller, the controller shall consult the supervisory authority prior to processing. The supervisory authority shall, within a period to be specified by it, provide written advice to the controller and, where applicable, to the processor, and may exercise any of its powers conferred by this Code. The supervisory authority shall in particular advise the controller where the intended processing would infringe this Code, and shall indicate the measures to be taken to bring the processing into compliance.

(7) The controller shall review the data protection impact assessment and, where necessary, update it whenever there is a material change in the risk presented by the processing operations, including a change in the nature, scope, context, or purposes of the processing, or the introduction of new technologies.

Chapter 03 — Transfers and Processors

Article 22 — International Data Transfers

(1) All personal data processed within the Kaharagian legal order is stored in foreign jurisdictions. This Article establishes the standards and safeguards applicable to the storage and transfer of personal data across jurisdictions, in order to ensure that the level of protection afforded by this Code is not undermined.

(2) A transfer of personal data to a foreign jurisdiction may take place where the supervisory authority has determined that the jurisdiction in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

(3) When assessing the adequacy of the level of protection, the supervisory authority shall take into account the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, and the existence and effective functioning of an independent supervisory authority in the jurisdiction concerned;

(b) the relevant legislation in force in the jurisdiction, both general and sectoral, including concerning public security, defence, national security, criminal law, and public authority access to personal data, as well as the implementation of such legislation and the availability of enforceable data subject rights;

(c) the international commitments of the jurisdiction, in particular with regard to the protection of personal data, including commitments arising from legally binding conventions or instruments and from participation in multilateral or regional systems;

(d) the existence of effective administrative and judicial remedies for data subjects whose personal data is being transferred.

(4) The supervisory authority shall publish a list of jurisdictions in respect of which an adequacy determination has been made and shall keep such list under regular review. The supervisory authority may limit an adequacy determination to a specific sector or category of processing within a given jurisdiction.

(5) In the absence of an adequacy determination pursuant to paragraph 2, a controller or processor may transfer personal data to a foreign jurisdiction only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Appropriate safeguards may be provided by means of:

(a) binding contractual clauses between the controller or processor and the recipient of the personal data in the foreign jurisdiction;

(b) standard data protection clauses adopted or approved by the supervisory authority;

(c) an approved code of conduct, together with binding and enforceable commitments of the recipient to apply the appropriate safeguards;

(d) an approved certification mechanism, together with binding and enforceable commitments of the recipient to apply the appropriate safeguards.

(6) In the absence of an adequacy determination pursuant to paragraph 2 or of appropriate safeguards pursuant to paragraph 5, a transfer or a set of transfers of personal data to a foreign jurisdiction may take place only on the basis of one of the following derogations:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfer due to the absence of an adequacy determination and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken at the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for important reasons of public interest of the State;

(e) the transfer is necessary for the establishment, exercise, or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

(7) The State, including all its organs, departments, agencies, and instrumentalities, shall ensure that its own data storage arrangements comply with this Article. The State shall publish and maintain a current list of the foreign jurisdictions in which State data is held, including the categories of personal data stored in each jurisdiction and the safeguards applicable to each such arrangement.

(8) A transfer pursuant to paragraph 6 shall not involve the entirety of a database or entire categories of personal data. Where a transfer is based on the derogation in paragraph 6(4), it shall be founded on a public interest recognised in the laws of the State.

Article 23 — Processor Obligations

(1) Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Code and ensure the protection of the rights of the data subject.

(2) The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. Where the controller objects, the processor shall not proceed with the engagement of the sub-processor in question.

(3) Processing by a processor shall be governed by a contract or other legal act under the law of the State that is binding on the processor with regard to the controller and that sets out:

(a) the subject-matter and duration of the processing;

(b) the nature and purpose of the processing;

(c) the type of personal data and the categories of data subjects;

(d) the obligations and rights of the controller;

(e) the obligations of the processor as set out in paragraph 4 of this Article.

(4) The processor shall:

(a) process the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a foreign jurisdiction, unless required to do so by the laws of the State; in such a case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits such information on important grounds of public interest;

(b) ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) implement the security measures required by Article 18 of this Code;

(d) respect the conditions referred to in paragraphs 2 and 3 for engaging another processor;

(e) taking into account the nature of the processing, assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Title II of this Code;

(f) assist the controller in ensuring compliance with the obligations pursuant to Article 18, Article 19, Article 20, and Article 21, taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, delete or return all the personal data to the controller after the end of the provision of services relating to the processing, and delete existing copies unless the law of the State requires storage of the personal data;

(h) make available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

(5) Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Code. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

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

(7) The contract or other legal act referred to in paragraph 3 shall be in writing, including in electronic form. Execution of such contracts by secure electronic means, including by qualified electronic signature, shall be fully equivalent to execution in any other form.

Title 04 — Supervision, Remedies, and Final Provisions

Articles 24–30

Chapter 01 — Supervision

Article 24 — Supervisory Authority

(1) The Sovereign of the State of the Kaharagians shall be the supervisory authority for the purposes of this Code and shall be responsible for monitoring and enforcing the application of its provisions. In the exercise of this function, the Sovereign shall act as the guarantor of the fundamental right to the protection of personal data as recognised by the Fundamental Laws.

(2) The Sovereign may, by decree, delegate the whole or any part of the supervisory functions conferred by this Code to a Data Protection Officer or to another suitably qualified person or body. Any such delegation shall specify the scope, duration, and conditions of the delegated functions and may be revoked or amended at any time by further decree. The delegate shall exercise the delegated functions subject to such directions of a general character as the Sovereign may issue, provided that such directions do not compromise the independence required by paragraph 3.

(3) The supervisory authority, whether the Sovereign acting personally or a delegate appointed under paragraph 2, shall act with complete independence in the exercise of the supervisory functions conferred by this Code. In particular, the supervisory authority shall be free from external influence, whether direct or indirect, in reaching decisions on individual cases and shall neither seek nor take instructions from any person or entity with respect to such decisions.

(4) The supervisory authority shall publish an annual report on its activities, which shall include at a minimum:

(a) the number and nature of complaints received under Article 27;

(b) a summary of investigations conducted and their outcomes;

(c) a summary of corrective measures and sanctions imposed under Article 28;

(d) any guidance, opinions, or standard clauses issued during the reporting period;

(e) an assessment of emerging trends and challenges in data protection relevant to the State.

(5) The annual report referred to in paragraph 4 shall be made publicly available within ninety days of the end of the reporting period to which it relates and shall be published in the Official Gazette and on any official digital platform of the State.

(6) The supervisory authority shall maintain appropriate records of its activities and decisions and shall ensure that its processes are transparent and accessible to data subjects and controllers alike, consistent with the principle of proportionality and the administrative capacity of the State.

Article 25 — Powers of the Supervisory Authority

(1) The supervisory authority shall have the following investigative powers:

(a) to order any controller or processor to provide any information the supervisory authority requires for the performance of its functions, within such time as the supervisory authority may specify;

(b) to carry out audits and inspections of the data processing operations of any controller or processor, including the review of records, systems, and documentation relating to the processing of personal data;

(c) to obtain access to all personal data and to all information necessary for the performance of its functions, including access to any premises, equipment, or means used for the processing of personal data, subject to applicable rules of host-jurisdiction law governing entry to premises;

(d) to notify a controller or processor of an alleged infringement of this Code and to require the controller or processor to provide a written response within a specified period;

(e) to require a controller or processor to carry out a data protection impact assessment in accordance with Chapter 2 of Title III of this Code where the supervisory authority considers that a type of processing is likely to result in a high risk to the rights and freedoms of data subjects.

(2) The supervisory authority shall have the following corrective powers:

(a) to issue a warning to a controller or processor that intended processing operations are likely to infringe this Code;

(b) to issue a reprimand to a controller or processor where processing operations have infringed this Code;

(c) to order a controller or processor to comply with a data subject's request to exercise rights under Title II of this Code;

(d) to order a controller or processor to bring processing operations into compliance with this Code, in a specified manner and within a specified period;

(e) to order a controller to communicate a personal data breach to the data subject in accordance with Chapter 2 of Title III of this Code;

(f) to order the rectification or erasure of personal data or the restriction of processing in accordance with Chapter 2 of Title II of this Code, and to order the notification of such actions to recipients to whom the personal data have been disclosed;

(g) to impose a temporary or definitive limitation on processing, including a ban on processing, where the supervisory authority determines that continued processing would cause serious harm to the rights and freedoms of data subjects or would constitute a grave or persistent infringement of this Code;

(h) to order the suspension of data transfers to a recipient in a foreign jurisdiction or to an international organisation where the supervisory authority determines that the transfer does not comply with Chapter 3 of Title III of this Code.

(3) The supervisory authority shall have the following advisory powers:

(a) to issue opinions, on its own initiative or upon request, on any matter relating to the protection of personal data, including on legislative and administrative proposals affecting the processing of personal data;

(b) to approve and publish standard data protection clauses for inclusion in contracts between controllers and processors, and between controllers or processors and recipients in foreign jurisdictions;

(c) to approve codes of conduct submitted by associations or bodies representing categories of controllers or processors, and to monitor compliance with approved codes of conduct;

(d) to authorise contractual clauses and provisions to be inserted in agreements relating to international transfers of personal data where those clauses provide appropriate safeguards within the meaning of this Code;

(e) to determine whether the data protection framework of a foreign jurisdiction or the data protection rules of an international organisation affords an adequate level of protection, and to publish a list of jurisdictions and organisations so recognised.

(4) The exercise of the powers conferred by this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, in accordance with the Fundamental Laws of the State. In particular, any order or decision issued under paragraph 1 or paragraph 2 shall state the reasons on which it is based and shall inform the addressee of the right to petition the Sovereign in accordance with the Fundamental Laws.

(5) The supervisory authority shall exercise the powers conferred by this Article in a manner that is proportionate to the nature, gravity, and consequences of the infringement or risk concerned, having regard to the circumstances of each case and the administrative capacity of the State.

Article 26 — Cooperation with Foreign Data Protection Authorities

(1) The supervisory authority may cooperate with the data protection authorities of other jurisdictions for the purpose of ensuring the effective enforcement of data protection legislation and the protection of the rights of data subjects. Such cooperation may take place on the initiative of the supervisory authority or at the request of a foreign data protection authority.

(2) The supervisory authority may exchange information relevant to the enforcement of data protection legislation with foreign data protection authorities, provided that appropriate safeguards are in place to ensure the confidentiality and security of the information exchanged. In particular, the supervisory

authority shall not disclose information received from a foreign authority to any third party without the prior consent of the authority that provided the information, unless required to do so by law.

(3) The supervisory authority may provide mutual assistance to foreign data protection authorities in relation to investigations and enforcement proceedings, including by:

(a) providing information held by the supervisory authority that is relevant to an investigation being conducted by a foreign authority;

(b) conducting inquiries or inspections on behalf of a foreign authority, to the extent permitted by this Code and the Fundamental Laws;

(c) facilitating the notification of decisions or orders of a foreign authority to persons within the jurisdiction of the State.

(4) Cooperation under this Article shall at all times respect the sovereignty of the State of the Kaharagians and the constitutional prerogatives of the Sovereign. The supervisory authority shall not comply with a request for cooperation or assistance where compliance would be incompatible with the Fundamental Laws, the public order of the State, or the rights and freedoms of persons subject to the jurisdiction of Kaharagia.

(5) The supervisory authority may enter into memoranda of understanding, cooperation agreements, or other instruments with foreign data protection authorities for the purpose of establishing a framework for ongoing cooperation, information exchange, and mutual assistance. Any such instrument shall be published in summary form in the Official Gazette.

(6) Where a data subject who is a Kaharagian national or who otherwise falls within the personal jurisdiction of the State lodges a complaint with a foreign data protection authority, the supervisory authority shall, upon being informed of such complaint, use its best efforts to cooperate with the foreign authority to ensure that the data subject receives an effective remedy.

(7) The supervisory authority shall have due regard, in the exercise of its functions under this Code, to the data protection standards and best practices prevailing in jurisdictions where Kaharagians commonly reside or where controllers and processors subject to this Code operate, with a view to promoting a high and consistent level of data protection.

Chapter 02 — Remedies and Sanctions

Article 27 — Right to Lodge a Complaint

(1) Every data subject shall have the right to lodge a complaint with the supervisory authority if the data subject considers that the processing of personal data relating to him or her infringes any provision of this Code. The right to lodge a complaint shall apply irrespective of the jurisdiction in which the processing takes place, provided that the controller or processor is subject to this Code in accordance with Article 3.

(2) A complaint under paragraph 1 shall be submitted in writing, including by electronic means, and shall contain at a minimum:

(a) the identity and contact details of the complainant;

(b) a description of the facts giving rise to the complaint, including, where known, the identity of the controller or processor concerned;

(c) an indication of the provision or provisions of this Code that the complainant considers to have been infringed;

(d) a description of any steps already taken by the complainant to address the matter with the controller or processor, and any response received.

(3) The supervisory authority shall acknowledge receipt of a complaint within fourteen days and shall inform the complainant of the progress and outcome of the complaint, including the possibility of a remedy under Article 28, within ninety days of receipt. Where the complexity of the matter requires additional time, the supervisory authority may extend that period by a further ninety days, provided that the complainant is informed of the extension and the reasons therefor before the expiry of the initial period.

(4) The data subject shall have the right to an effective remedy where the supervisory authority does not handle the complaint, does not inform the complainant of the progress or outcome within the period specified in paragraph 3, or where the data subject is dissatisfied with the decision of the supervisory authority. For the purposes of this paragraph, an effective remedy includes the right to petition the Sovereign to review the matter.

(5) Without prejudice to any other administrative or judicial remedy, a data subject may at any time petition the Sovereign directly in accordance with the relevant provisions of the Fundamental Laws where the data subject considers that his or her rights under this Code have been infringed. The Sovereign shall consider such petition and may take any action that the supervisory authority is empowered to take under this Code.

(6) The supervisory authority shall establish and publish clear and accessible procedures for the lodging and handling of complaints, including the provision of complaint forms in electronic format and guidance on the information required to be submitted.

(7) The lodging of a complaint with the supervisory authority shall be without prejudice to the right of the data subject to seek compensation under Article 28(3) or to pursue any other remedy available under the laws of the jurisdiction in which the data subject is resident.

Article 28 — Remedies and Sanctions

(1) The supervisory authority may impose the following sanctions for infringement of this Code:

(a) a formal warning, in the case of a first infringement where the infringement is non-intentional and of minor gravity, requiring the controller or processor to bring its processing operations into compliance with this Code;

(b) an order to bring processing operations into compliance with this Code within a specified period not exceeding sixty days, with the possibility of extension in exceptional circumstances at the discretion of the supervisory authority;

(c) a temporary limitation on or suspension of processing for a specified period, where the supervisory authority determines that continued processing poses a significant risk to the rights and freedoms of data subjects;

(d) a definitive ban on processing, in whole or in part, where a temporary measure has proven insufficient or where the gravity of the infringement so warrants;

(e) an order to rectify, erase, or restrict personal data, and to notify such action to each recipient to whom the data have been disclosed, in accordance with Chapter 2 of Title II of this Code.

(2) For serious, repeated, or intentional infringements, the supervisory authority may, in addition to or in lieu of the sanctions referred to in paragraph 1, impose the following measures:

(a) the revocation of any licence, authorisation, accreditation, or recognition granted to the controller or processor under the laws or decrees of the State;

(b) public censure, by means of a public statement identifying the controller or processor and describing the nature and gravity of the infringement, published in the Official Gazette and on any official digital platform of the State.

(3) Any natural or legal person who has suffered material or non-material damage as a result of an infringement of this Code shall have the right to receive compensation from the controller or processor responsible for the infringement. For the purposes of this paragraph, non-material damage includes distress, loss of privacy, reputational harm, and any other form of prejudice that is not purely pecuniary in nature.

(4) A controller involved in processing shall be liable for any damage caused by processing that infringes this Code. A processor shall be liable for damage caused by processing only where:

(a) it has not complied with obligations of this Code that are specifically directed to processors; or

(b) it has acted outside or contrary to the lawful instructions of the controller.

(5) Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and are responsible for damage caused by that processing, each shall be held jointly and severally liable for the entire damage, in order to ensure effective compensation of the data subject. A controller or processor that has paid full compensation for the damage suffered may subsequently bring a claim for contribution against the other controllers or processors involved in the same processing, in proportion to their respective responsibility for the damage.

(6) A controller or processor shall be exempt from liability under paragraphs 3 to 5 if it proves that it is not in any way responsible for the event giving rise to the damage. The burden of proof shall rest with the controller or processor claiming exemption.

(7) In determining the sanction to be imposed under paragraphs 1 and 2, the supervisory authority shall take into account all relevant circumstances, including:

(a) the nature, gravity, and duration of the infringement;

(b) the intentional or negligent character of the infringement;

(c) the categories of personal data affected;

(d) the number of data subjects affected;

(e) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(f) any relevant previous infringements by the controller or processor;

(g) the degree of cooperation with the supervisory authority;

(h) the manner in which the infringement became known to the supervisory authority, including whether and to what extent the controller or processor notified the infringement.

(8) The imposition of sanctions under this Article shall be without prejudice to the right of the data subject to seek additional remedies available under the laws of the jurisdiction in which the data subject is resident or in which the damage occurred.

Chapter 03 — Final Provisions

Article 29 — Relationship with Host-Jurisdiction Law

(1) In accordance with Article 42(1) of the Fundamental Laws, where a data subject is physically present in a jurisdiction that imposes mandatory data protection obligations on controllers or processors, those obligations shall apply to the extent that they afford a higher level of protection to the data subject than the corresponding provisions of this Code.

(2) Where a conflict arises between a provision of this Code and a mandatory data protection law of a host jurisdiction that is applicable to a data subject by reason of that data subject's physical presence in that jurisdiction, the more protective standard shall prevail. For the purposes of this paragraph, the more protective standard is the standard that affords greater protection to the rights, freedoms, and interests of the data subject in the specific circumstances of the case.

(3) The State and its organs, as well as any controller or processor subject to this Code, shall, when processing personal data of persons known or reasonably believed to be physically present in a particular jurisdiction, take reasonable steps to ascertain and comply with the applicable mandatory data protection law of that jurisdiction. Such reasonable steps shall include, at a minimum:

(a) identifying the jurisdiction in which the data subject is or is reasonably believed to be present;

(b) making reasonable inquiries as to the material data protection requirements of that jurisdiction;

(c) implementing any additional technical or organisational measures necessary to comply with the mandatory data protection law of that jurisdiction, to the extent that it affords a higher level of protection than this Code.

(4) This Article does not diminish, restrict, or otherwise affect any right granted to a data subject by this Code. It operates only to extend the level of protection afforded to a data subject where the mandatory data protection law of the host jurisdiction provides a higher standard of protection. In no case shall the application of host-jurisdiction law result in a reduction of the rights that a data subject would otherwise enjoy under this Code.

(5) The supervisory authority may issue guidance, in the form of opinions, guidelines, or advisory notices, on the interaction between this Code and the data protection laws of jurisdictions in which Kaharagians commonly reside or in which controllers and processors subject to this Code commonly operate. Such guidance shall take into account the evolving legal landscape of data protection and shall be updated as necessary to reflect changes in host-jurisdiction law.

(6) Where a controller or processor demonstrates that it has taken the reasonable steps required by paragraph 3 and has acted in good faith to comply with the applicable mandatory data protection law of the host jurisdiction, that fact shall be

taken into account by the supervisory authority as a mitigating factor in any proceedings relating to an alleged infringement of this Code or of host-jurisdiction law.

Article 30 — Entry into Force and Transitional Provisions

(1) This Code shall enter into force on the date of its publication in the Official Gazette of the State of the Kaharagians. From that date, this Code shall be binding in its entirety and directly applicable to all persons and entities within the personal jurisdiction of the State, subject to the transitional provisions set out in paragraphs 2 and 3.

(2) Controllers and processors who, at the date of entry into force of this Code, are engaged in processing operations that are subject to this Code shall bring their processing operations into full compliance with the provisions of this Code within one hundred and eighty days from the date of entry into force. During the transitional period, such controllers and processors shall take all reasonable steps to progress towards compliance and shall, in any event, ensure that no processing operation carried out during the transitional period causes material harm to the rights and freedoms of data subjects.

(3) Processing operations commenced before the date of entry into force of this Code that comply with the law as it stood at that time shall be deemed lawful until the expiry of the transitional period referred to in paragraph 2, provided that the controller or processor concerned is making demonstrable progress towards compliance with this Code. Upon the expiry of the transitional period, all processing operations must comply with this Code in full, and the presumption of lawfulness under this paragraph shall cease to apply.

(4) The Sovereign may, by decree, adopt further regulations, rules, or technical standards for the implementation and application of this Code. Such implementing measures may address, inter alia:

(a) the detailed procedures for the exercise of data subject rights under Title II;

(b) the technical and organisational standards for data security under Article 16;

(c) the form and content of notifications of personal data breaches;

(d) the criteria for assessing the adequacy of the data protection framework of foreign jurisdictions;

(e) the procedures for the lodging, handling, and resolution of complaints under Article 27;

(f) any other matter that the Sovereign considers necessary or expedient for the effective implementation of this Code.

(5) References in other laws, decrees, regulations, or official instruments of the State to the protection of personal data or to the rights of data subjects shall, unless the context otherwise requires, be read as references to the corresponding

provisions of this Code. Where any such law, decree, regulation, or instrument is inconsistent with this Code, this Code shall prevail to the extent of the inconsistency, except where a provision of the Fundamental Laws provides otherwise.

(6) The supervisory authority shall, within ninety days of the entry into force of this Code, publish guidance for controllers and processors on the steps required to achieve compliance during the transitional period referred to in paragraph 2, and shall make itself available to respond to inquiries from controllers and processors concerning their obligations under this Code.

Table of Cross-References

Every reference this Code makes to an Article, of this or of another instrument. References are to Articles.

Art. 1 (2)	FN Art. 46
Art. 3 (3)	FN Art. 42
Art. 4 (4)	Art. 2
Art. 5 (5)	Art. 2
Art. 6 (6)	Arts 4, 5
Art. 7 (10)	Art. 4
Art. 8 (11)	Art. 4
Art. 9 (12)	Art. 8
Art. 11 (14)	Art. 10
Art. 12 (15)	Arts 7, 10
Art. 13 (16)	Arts 10, 12
Art. 14 (17)	Arts 7, 10, 12
Art. 15 (20)	Arts 4–6
Art. 16 (20)	Art. 15
Art. 17 (21)	Arts 2, 18, 22
Art. 18 (23)	Art. 15
Art. 21 (26)	Art. 2
Art. 23 (29)	Arts 15, 18–21
Art. 24 (32)	Arts 27, 28
Art. 27 (36)	Arts 3, 28
Art. 29 (39)	FN Art. 42
Art. 30 (40)	Arts 16, 27

Glossary

Terms used in this Code, as defined in KáhaLex, with the Articles in which each is used and the pages they begin on. Where a definition cites an Article, the citation names the instrument it belongs to.

consent A person's free and informed agreement to something. In data protection, a freely given, specific, informed, and unambiguous agreement, by a clear affirmative act, to the processing of personal data (**DPC Art. 7**); in criminal law, the voluntary agreement to a sexual act (**CR Art. 28**). *Arts 2 (2), 4 (4), 7, 8 (10–11), 12–14 (15–17), 22 (27), 26 (34)*

contract An agreement formed by an offer and a matching acceptance, binding the parties as law between them; silence is not acceptance (**CC Art. 43**). *Arts 4 (4), 7, 8 (10–11), 14 (17), 22, 23 (27–29), 25 (33)*

controller The controller determines the purposes and means of processing personal data; the processor acts on the controller's behalf and under its instructions (**DPC Art. 2**, **DPC Art. 23**). *Arts 2–30 (2–40)*

data subject The identified or identifiable individual to whom personal data relates, and who holds the rights of access, rectification, erasure, restriction, and portability (**DPC Art. 2**). *Arts 2 (2), 4–17 (4–21), 19–30 (24–40)*

filing system A structured set of personal data accessible according to specific criteria, whether held centrally or dispersed (**DPC Art. 2**). *Art. 2 (2)*

Fundamental Laws The supreme law of the State, against which every other norm is measured; an inconsistent norm is void to the extent of the inconsistency. Only the Sovereign may amend them, by the procedure in Title 10 (**FN Art. 6**, **FN Art. 38**). *Arts 1 (2), 3 (3), 24–27 (32–36), 29, 30 (39–40)*

guardianship Protective regimes for a person who lacks capacity: guardianship for total incapacity, curatorship for partial incapacity. The guardian or curator manages the person's affairs under supervision and accounts yearly (**CC Art. 13**). *Art. 7 (10)*

host jurisdiction The State or territory in which a Kaharagian national is physically present, or in which a thing is situated. The mandatory law of the host jurisdiction prevails where it applies (**FN Art. 47**, **CC Art. 4**). *Arts 3, 4 (3–4), 25 (33), 29 (39)*

obligation A legal bond requiring one person (the debtor) to render a performance to another (the creditor). It may arise from contract, unilateral declaration, unjust enrichment, a wrongful act, or the law (**CC Art. 41**). *Arts 3, 4 (3–4), 6 (6), 9 (12), 12 (15), 15–17 (20–21), 19 (24), 23 (29), 28–30 (37–40)*

parental authority The rights and duties of parents to care for, educate, represent, and manage the property of their minor child, exercised jointly and always in the child's best interests (**CC Art. 32**). *Art. 7 (10)*

personal data Any information relating to an identified or identifiable individual, the data subject. Sensitive personal data is a special category subject to stricter conditions (**DPC Art. 2**, **DPC Art. 4**). *Arts 1–25 (2–33), 27–30 (36–40)*

personal jurisdiction The State's authority over persons by reason of their nationality or consent, rather than over territory. Kaharagian law follows the national wherever they are (**FN Art. 42**). *Arts 3 (3), 26 (34), 30 (40)*

processing Any operation performed on personal data: collection, storage, use, disclosure, erasure, and the like (**DPC Art. 2**). *Arts 1–18 (2–23), 21–23 (26–29), 25 (33), 27–30 (36–40)*

public censure A sanction consisting in the formal, published condemnation of an offender in the Official Gazette (**CR Art. 10**). *Art. 28 (37)*

public order The body of fundamental principles of justice, and the rights guaranteed by the Fundamental Laws, which a foreign law or judgment may not offend; where it does, Kaharagian law is applied instead (**CC Art. 63**). *Art. 26 (34)*

recipient In data protection, a person or body to which personal data is disclosed, whether or not that person is a third party (**DPC Art. 2**). *Arts 2 (2), 8–13 (11–16), 17 (21), 22 (27), 25 (33), 28 (37)*

recognised legal person A corporation, association, foundation, trust, partnership, or other juridical entity constituted or recognised under Kaharagian law; it may bear rights and, in criminal law, be subject to sanction (**CR Art. 2**). *Arts 1–4 (2–4), 13 (16), 22 (27), 28 (37)*

Royal Kaharagian Gazette The official journal of the State, in which laws, decrees, and other instruments are published. Publication in the Gazette is a condition of a law taking effect (**FN Art. 39**). *Arts 24 (32), 26 (34), 28 (37), 30 (40)*

Sovereign The reigning Prince of Kaharagia, head of state and source of executive authority. Where the law requires sovereign assent (e.g. a sovereign decree), it refers to a formal act signed by the Sovereign in person. *Arts 24–27 (32–36), 30 (40)*

State, the The sovereign legal person of Kaharagia, perpetual and distinct from the person of the Sovereign. Its official name is "the State of the Kaharagians"; "Kaharagia" and "the Principality of Kaharagia" are also used. It holds no territory of its own; its jurisdiction is personal and consensual (**FN Art. 1**, **FN Art. 4**). *Arts 1–4 (2–4), 7–10 (10–13), 12, 13 (15–16), 16 (20), 18 (23), 21–26 (26–34), 28–30 (37–40)*

supervisory authority The authority responsible for supervising and enforcing the Data Protection Code: the Sovereign, who may delegate the function by decree (**DPC Art. 24**). *Arts 2 (2), 6 (6), 8 (11), 10 (13), 15 (20), 17 (21), 19–22 (24–27), 24–30 (32–40)*

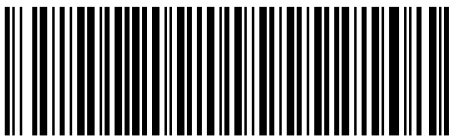
third party A person who is not a party to the contract, act or proceeding in question. In data protection, a person or body other than the data subject, the controller, the processor, and those acting under their direct authority (**DPC Art. 2**). *Arts 2 (2), 8 (11), 26 (34)*

Index of Articles

Every Article of this Code by its heading, alphabetically, with the page it begins on in parentheses. For subjects rather than headings, see the General Index.

General Index

References are to Articles, with the pages they begin on in parentheses. "passim" marks a term used throughout the Code.



KPN 549-720-26-0005-6

THE SOVEREIGN'S PRINTER

Royal Chancellery, Kaharagia