National Cyber Security Authority

DPO DATA PROTECTION OFFICE

GUIDELINES ON CHILDREN'S PERSONAL DATA PROTECTION 2026

www.dpo.gov.rw

dpp@dpo.gov.rw

Toll free: 9080

Contents

Definitions 2
1. Introduction 4
2. Purpose and Scope 4
3. Best Interests of the Child 5
4. Lawfulness of Processing and Use of Consent 6
  4.1 Identification of a Lawful Basis 6
  4.2 Parental Consent and Processing of Children's Data 6
  4.3 Processing of Sensitive Personal Data 9
5. Data Protection Principles 10
  5.1 Lawfulness, Fairness, and Transparency 11
  5.2 Purpose Limitation 14
  5.3 Data Minimisation 15
  5.4 Accuracy 16
  5.5 Storage Limitation 17
6. Data Governance and Accountability 18
7. Integrity, Confidentiality, and Security of Data 20
8. High-Risk Processing and Data Protection Impact Assessments (DPIAs) 22
9. Privacy by Design and by Default 23
10. Personal Data Breach Notifications 25
11. Profiling and Automated Decision-Making 26
12. Marketing Directed at Children 28
13. Use of Artificial Intelligence (AI) and Emerging Technologies 29
14. Data Sharing and Engagement with Data Processors 31
15. Cross-Border Transfers of Children's Personal Data 32
16. Data Subject Rights in the Context of Children 33
Annex 1 – Step-by-Step Approach to Age Assurance and Parental Consent 36
Annex 2 – Illustrative Examples of High-Risk Processing Involving Children 38

Definitions

For the purposes of this Guideline, the following terms should be understood in accordance with the DPP Law and the context of processing children's personal data:

Child - any person below the age of eighteen (18) years.

Children's personal data - any personal data relating to an identified or identifiable child, whether collected directly or indirectly.

Sensitive personal data - information revealing a person's race, health status, criminal records, medical records, social origin, religious or philosophical beliefs, political opinion, genetic or biometric information, sexual life or family details;

Processing - an operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as access to, obtaining, collection, recording, structuring, storage, adaptation or alteration, retrieval, reconstruction, concealment, consultation, use, disclosure by transmission, sharing, transfer, or otherwise making available, sale, restriction, erasure or destruction;

Data subject - a natural person from whom or in respect of whom, personal data has been requested and processed;

Data controller - natural person, public or private corporate body or legal entity which, alone or jointly with others, processes personal data and determines the means of their processing;

Data processor - public or private corporate body or legal entity, which is authorised to process personal data on behalf of the data controller.

Holder of parental responsibility- A person who has legal responsibility for the care, protection, and representation of a child and is authorised to act in the child's best interests.

Consent - freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by an oral, written or electronic statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Parental consent - consent provided by a holder of parental responsibility on behalf of a child where required.

Profiling - any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse and predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

Automated decision-making - decision-making based solely or partially on automated processing, including profiling, that may significantly affect a child.

Behavioural advertising - advertising or marketing based on monitoring or analysing a child's activities, behaviour, preferences, interactions, or browsing habits over time or across services.

Age assurance - measures used to establish, verify, estimate, or reasonably determine whether a user is a child and whether parental consent requirements apply.

Biometric data - personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a person, allowing or confirming the unique identification of that person.

Data Protection Impact Assessment (DPIA) - a structured process for identifying, evaluating, and mitigating risks to data subjects' rights and freedoms arising from planned processing activities.

Personal data breach - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Cross-border transfer - any transfer, disclosure, remote access, storage, or other processing of personal data outside Rwanda.

High-Risk Processing - processing activities likely to present significant risks to the rights and freedoms of children due to the nature, scope, context, sensitivity, or purpose of the processing.

1. Introduction

In an increasingly digital environment, the protection of children's personal data has become a matter of growing importance. Children today interact with digital technologies as part of their everyday lives — through education, communication, entertainment, healthcare, commerce, and access to public and private services — significantly increasing both the volume of personal data processed about them and the complexity of associated privacy risks. These risks extend beyond traditional concerns related to physical safety and include profiling, excessive data collection, behavioural tracking, exposure to harmful or inappropriate content, manipulative commercial practices, and potential long-term impacts on children's development, autonomy, and dignity.

The increasing participation of children in the digital environment highlights the need for clear, practical, and context-sensitive guidance to ensure that their personal data is processed in a manner that fully respects and protects their rights and interests. This is particularly relevant as public and private sector entities increasingly rely on data-driven systems, digital platforms, online services, and emerging technologies, including artificial intelligence and automated decision-making tools.

This guideline demonstrates the Data Protection and Privacy Office's (DPO) commitment to a child-centered and rights-based approach to protecting personal data. It emphasises that children are entitled to specific consideration and enhanced safeguards under the Law Nº 058/2021 of 13/10/2021 Relating to the Protection of Personal Data and Privacy (DPP Law), and that the best interests of the child should remain a primary consideration throughout the lifecycle of data processing activities.

The Guideline therefore seeks to support data controllers and data processors in translating legal obligations into practical and effective safeguards for children in both digital and non-digital environments.

This Guideline should be read together with the DPP Law and other guidance issued by the DPO. The examples provided are illustrative and should be adapted to the nature, scale, and context of processing activities.

2. Purpose and Scope

This document provides practical and operational guidance on processing children's personal data in accordance with the DPP Law and relevant national, international, and regional standards and best practices.

This Guideline is issued by the DPO to support data controllers and processors in applying appropriate safeguards when processing children's personal data, recognising children as data subjects who require specific consideration and enhanced protection.

In particular, the Guideline:

- promotes a human rights-based approach, placing the best interests of the child at the centre of all processing activities;
- adopts a risk-based and accountability-oriented approach, encouraging data controllers and processors to identify and address risks in a proactive and structured manner;
- draws on practical regulatory experience and established best practices, with the aim of providing clear and actionable guidance applicable across different sectors and contexts.

Beyond legal compliance, the Guideline seeks to foster a culture of responsible data governance, where the design and operation of systems and services actively contribute to the protection and empowerment of children in the digital environment.

This Guideline applies to all public and private entities and organisations, whether located within or outside Rwanda, that process children's personal data across sectors, including education, health, social services, digital services, telecommunications, financial services, public administration, and law enforcement, and those located outside Rwanda processing children's data.

3. Best Interests of the Child

When processing children's personal data, data controllers and processors should ensure that the best interests of the child are a primary consideration throughout the lifecycle of processing activities. This principle should guide decision-making relating to the design, implementation, operation, review, and governance of systems, services, and activities involving children's personal data.

Children may be less able to understand how their personal data is collected, used, shared, retained, or otherwise processed, as well as the potential short-term and long-term consequences of such processing. They may also be more vulnerable to risks arising from profiling, behavioural influence, excessive monitoring, commercial exploitation, exclusion, discrimination, or exposure to harmful content and environments. For this reason, processing involving children requires a higher standard of protection and safeguards adapted to the child's age, maturity, evolving capacities, and level of vulnerability.

Applying the best interests principle requires data controllers and processors to assess not only whether processing is lawful, but also whether it is appropriate, necessary, proportionate, fair, and supportive of children's rights, dignity, well-being, and development.

In practice, data controllers and processors should consider:

- the nature, purpose, and context of the processing activity;
- the age, maturity, and reasonable expectations of the child;
- the relationship between the child and the organisation or service provider;
- the potential short-term and long-term impact of the processing on the child;
- whether the processing could expose children to risks such as manipulation, exclusion, discrimination, reputational harm, or excessive monitoring;
- whether the intended objective can reasonably be achieved through less intrusive means.

Before processing children's personal data, data controllers and processors are encouraged to assess, among others:

- whether the processing activity is genuinely necessary for the intended purpose;
- whether a child and/or parent would reasonably expect the processing to take place;
- whether the processing could negatively affect the child, either immediately or over time;

- whether less privacy-intrusive alternatives are available;
- whether safeguards are appropriate to the child's age, vulnerability, and level of understanding;
- whether the processing respects the child's dignity, autonomy, and well-being;
- whether children are adequately protected from manipulation, unnecessary monitoring, profiling, or commercial exploitation.

The best interests of the child should be integrated into governance, risk assessment, procurement, system design, and operational decision-making processes involving children's personal data.

Where uncertainty exists regarding the impact of processing on children, data controllers and processors should adopt the approach that is most protective of children's rights and interests.

Where appropriate, organisations should give children an opportunity to express their views on how their personal data is collected, used and shared. The manner of consultation should reflect the child's age, maturity and ability to understand the processing. The child's views should be considered alongside their safety, rights and best interests when deciding which safeguards are necessary.

4. Lawfulness of Processing and Use of Consent

4.1 Identification of a Lawful Basis

In accordance with Article 46 of the DPP Law, personal data may only be processed where at least one of the legal grounds provided under this Article applies, while the processing of sensitive personal data is subject to the additional safeguards and grounds set out under Article 10 of the DPP Law. This requirement applies to all processing activities and calls for particular care when the data relates to children.

Selecting an appropriate legal basis is an essential step in ensuring that processing is lawful, fair, and transparent, and that children's rights are effectively protected in practice. When determining the appropriate legal basis, data controllers should consider the nature, context, and purpose of the processing as well as the potential impact on the child, including possible long-term effects.

Certain legal bases require particular attention in the context of children, notably:

- Consent, which must be valid and appropriately obtained;
- Legitimate interests, which require careful assessment to ensure that the child's rights and interests are not adversely affected.

Data controllers should ensure that the chosen legal basis is clearly identified, appropriately justified, and documented, and that it can be explained in a manner that is understandable to both children and their parents or guardians.

4.2 Parental Consent and Processing of Children's Data

Under Article 9 of the DPP Law, where a data controller, data processor, or third party knows that personal data relates to a child under the age of sixteen (16) years, processing requires the consent of a holder of parental responsibility, unless another lawful ground applies.

Under Article 9 of the DPP Law, where a data controller, data processor or third party knows that personal data relates to a child under sixteen (16) years, consent must be obtained from a holder of parental responsibility in accordance with relevant laws. Such consent is not required where processing is necessary to protect the child's vital interests. The applicable lawful basis under Article 46 and any additional requirements under Article 10 must also be considered, where relevant.

Consent in the Interest of the Child

Consent given on behalf of a child is only valid when it serves the child's best interests. This means that consent should genuinely consider the child's well-being and should not be used to justify excessive, unnecessary, or potentially harmful data processing. Data controllers must ensure that the purpose of any data processing is suitable for children, aligns with their best interests, and provides clear information to help parents or guardians make informed decisions.

Conditions for Valid Consent

Where consent is relied upon as the legal basis for processing children's personal data, it should meet the following conditions:

- it is freely given, specific, informed, and unambiguous;
- it is presented in a manner that is clear and understandable, taking into account the age and level of understanding of the child, as well as the role of the parent or guardian;
- it is verifiable, with reasonable and proportionate steps taken to confirm that consent has been provided either by a child aged 16 years or above, or by a parent or legal guardian where required under the DPP Law.

Age Awareness and Age Verification

To determine whether parental consent is required under the DPP Law for children under the age of sixteen (16), data controllers and processors should take reasonable and proportionate measures to establish, verify, or reasonably estimate whether a user is a child.

The approach adopted should be risk-based and consider:

- the nature of the service;
- the type and sensitivity of the personal data processed;
- the risks that processing may present to children;
- the likelihood that children will access or use the service.

Measures used for age awareness, estimation, or verification may include:

- self-declaration of age, combined with appropriate risk-based controls or consistency checks;
- verification through a parent's or guardian's email address, account, or verified phone contact;

- technical measures or additional verification steps where higher-risk processing is involved, particularly where:
    - sensitive personal data is processed;
    - profiling or behavioural tracking is used;
    - children may be exposed to harmful or age-inappropriate content or interactions.

Age verification or estimation mechanisms should:

- be proportionate to the risks associated with the processing activity;
- minimise the collection and retention of additional personal data;
- avoid excessive, intrusive, or unnecessary verification measures;
- be designed and implemented in a manner that is fair, transparent, and respectful of children's rights and dignity;
- not create unnecessary barriers to access or unfairly exclude children from services.

Data controllers and processors should also periodically review the effectiveness and proportionality of age assurance measures to ensure that they remain appropriate to the risks and context of processing.

Verification of Parental Consent and Responsibility

Where parental consent is required, data controllers should implement proportionate measures to verify that consent is provided by a holder of parental responsibility.

Such measures should:

- be effective and adapted to the level of risk associated with the processing;
- avoid excessive, intrusive, or unnecessary data collection;
- take into account the available technologies and the context of the service;
- be reviewed periodically to ensure their continued effectiveness.

Examples of verification approaches may include:

- confirmation via a parent's email address, user account, or phone contact;
- provision of supporting documentation, where justified by higher risk;
- use of trusted third-party verification services.

The choice of method should reflect a balance between reliability, proportionality, and data minimisation.

Situations Where Consent Is Not Required

Article 9 of the DPP Law provides that parental consent is not required when processing is necessary to protect the child's vital interests.

This may arise, for example, in situations involving:

- medical emergencies;
- safeguarding or child protection interventions;
- urgent circumstances where obtaining consent is not feasible.

When Consent May Not Be the Most Appropriate Basis

Consent may not always be the most suitable legal basis, particularly in situations where there is limited choice or a clear imbalance between the parties. In such cases, alternative legal bases may be more appropriate, including those provided by Article 46 of the DPP law, such as compliance with a legal obligation and/or the performance of a task carried out in the public interest.

This is particularly relevant in contexts such as education, where certain processing activities are necessary for the provision of schooling, as well as in the delivery of public services, including healthcare and social services. In these situations, reliance on consent may not reflect a genuine or freely given choice.

4.3 Processing of Sensitive Personal Data

Children's data often includes sensitive personal information, particularly in sectors such as health, education, and social services. Under Article 10 of the DPP Law, such data may only be processed under specific conditions and where one of the following applies:

- the data subject, or where applicable the parent or guardian, has provided consent;
- the processing is necessary for the purposes of carrying out the obligations of the data controller, of the data processor or exercising specific rights of the data subject in accordance with relevant Laws;
- the processing is necessary to protect the vital interests of the data subject or of any other person;
- the processing is necessary for the purposes of preventive or occupational medicine, public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices;
- the processing is necessary for archiving purposes in the public interest or scientific and historical research purposes or statistical purposes.

When processing sensitive data relating to children, data controllers should apply additional care and safeguards, including:

- limiting processing to what is strictly necessary;
- ensuring appropriate confidentiality and access controls;
- clearly defining and communicating the purpose of processing;
- comply with applicable sensitive personal data retention periods;
- put in place measures to strengthen the capacities of staff involved in the processing of sensitive personal data;
- implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed to the data subject, including, where appropriate, storing sensitive personal data separately from other types of data, and applying measures such as tokenisation, pseudonymisation or encryption.

Practical Examples

Examples where consent may be appropriate:

- An online educational platform offers optional features, such as participation in discussion forums or public sharing of achievements. These features are not essential to the main service and are activated only after obtaining separate parental consent, with

clear information on how the child's data will be used and who may view it. Parents and, where appropriate, children can withdraw consent at any time, resulting in the deactivation of these features and the deletion or anonymisation of related data.

- A sports club seeks parental consent before using children's photographs for promotional purposes (e.g., website, brochures). Participation in the activity is not conditional on providing consent, and parents are offered clear choices regarding how images may be used. Consent can be withdrawn at any time, and the club takes reasonable steps to remove images from future publications and, where feasible, from existing materials.

Examples where another legal basis may be more appropriate:

- A public school processes personal data such as attendance records, academic performance information, and disciplinary records as part of its core educational responsibilities. This processing is based on the school's legal obligations and public-interest mandate, rather than consent, as it is necessary for the provision and administration of education and the proper functioning of the education system.
- A public authority processes children's personal data to provide access to healthcare, social protection, child welfare, or other essential public services. This processing is based on the authority's legal mandate and public-interest responsibilities, rather than on consent, because access to essential services should not depend on consent. In such circumstances, consent would generally not be considered freely given due to the clear imbalance of power and the absence of a genuine ability to refuse without adverse consequences.

Examples involving sensitive data:

- A healthcare provider processes a child's medical data, including health history and diagnostic results, for the purpose of diagnosis and treatment. This processing is justified on the basis of medical necessity and public health purposes, with strict confidentiality and access controls in place.
- A school processes emergency contact details and health-related information (e.g., allergies) to ensure student safety. This processing is necessary to fulfil duty of care obligations and is more appropriately based on legal obligation or vital interests rather than consent.

5. Data Protection Principles

The processing of children's personal data should be carried out in accordance with the core data protection principles set out in the DPP Law, applied with particular care and attention to the specific vulnerabilities and evolving capacities of children. Data controllers and processors are responsible for demonstrating compliance with the principles.

In practice, this requires not only formal compliance, but also the adoption of child-centered and risk-aware approaches, ensuring that:

- processing is appropriate to the child's age and understanding;
- risks are identified and mitigated in advance;

- systems and services are designed to support children's rights by default.

Transparency and communication are integral to these principles and should be considered throughout the processing lifecycle, not as a separate or purely informational obligation.

5.1 Lawfulness, Fairness, and Transparency

Personal data must be processed in a manner that is lawful, fair, and transparent. In the context of children, these principles require particular care, taking into account their evolving capacities, level of understanding, and potential vulnerabilities in both digital and non-digital environments.

Applying the principles of lawfulness, fairness, and transparency in relation to children requires a holistic and child-centred approach. Together, these principles contribute to building trust, accountability, and effective protection of children's personal data.

Lawfulness

Lawfulness requires that any processing of personal data is based on a valid legal ground under the DPP Law and complies with all applicable legal requirements. In practice, this means that:

- ✓ a specific legal basis is identified before processing begins;
- ✓ the processing is necessary for the stated purpose and limited to what is justified;
- ✓ all conditions attached to the legal basis are respected, including: child and parental consent requirements under Article 9 and conditions for processing sensitive personal data under Article 10;
- ✓ processing is consistent with other relevant laws, including those relating to child protection, education, health, etc.

In the context of children, particular care should be taken to ensure that the chosen legal ground is not only valid in form but also appropriate to the situation and protective of the child's interests.

Practical Examples

- A school processes students' personal data, including attendance records, academic performance, and disciplinary information, as part of its legal mandate to provide education and ensure proper administration. This processing does not rely on consent, as it is necessary for fulfilling statutory responsibilities. The school provides clear information to parents and students about how such data is used, limits access to authorised staff and ensures that data is retained only for the period required under applicable rules.
- A healthcare provider processes a child's personal data, including medical history, diagnostic results, and treatment records, for the purpose of diagnosis and provision of medical care. This processing is lawful as it is based on legal grounds under the DPP Law, including the necessity to provide healthcare services and, where applicable, public health purposes (Article 10). It is also carried out in compliance with relevant healthcare, public health, and professional confidentiality laws and regulations governing medical practice. The processing is limited to what is necessary for the specific medical purpose and does not rely on consent where this would not be appropriate in the context of essential healthcare services. Appropriate safeguards are applied, including: strict confidentiality obligations for healthcare professionals; restricted access to authorised medical personnel; secure storage and handling of medical records. Information about the

processing is provided to both the child (in a manner adapted to their age and understanding) and the parent or guardian.

Fairness

Fairness requires that personal data is processed in a manner that is respectful of the child's rights, reasonable in the circumstances, and does not lead to unjustified, disproportionate, or harmful outcomes.

In the context of children, fairness involves recognising that children:

- may not fully understand how their personal data is collected, used, or shared;
- may not be able to assess risks or long-term consequences;
- may be disproportionately affected by certain types of processing, such as profiling.

For these reasons, fairness requires a higher standard of care, ensuring that processing is not only lawful, but also appropriate and protective of the child's interests.

To ensure compliance with fairness principles, data controllers and processors should:

- not exploit children's lack of awareness, experience, or vulnerability;
- not engage in practices that mislead, manipulate, or encourage excessive data sharing (including through design features or incentives);
- ensure that processing is conducted in a manner that preserves integrity, confidentiality, and trust;
- ensure that the processing is appropriate for its purpose and does not exceed what a child and their parent or guardian would reasonably expect;
- consider the best interests of the child when designing systems, products, services, and processes;
- assess whether the processing could have negative consequences for the child, including exclusion, discrimination, or reputational harm, and mitigate those risks;
- ensure that children are not disadvantaged for choosing more privacy-protective options.

Practical Examples

- A gaming platform sets high privacy settings by default, ensuring that children's profiles are not publicly visible and that features such as location sharing or interaction with unknown users are disabled unless actively enabled with appropriate safeguards. The platform does not use children's data for behavioural advertising or profiling, recognising that such practices may exploit children's vulnerabilities or influence their choices in ways they may not fully understand. It also takes steps to limit exposure to inappropriate content. In addition, the platform limits data collection to what is necessary for gameplay and provides clear, age-appropriate explanations of how data is used. Children can use the core service without being encouraged or pressured to share additional personal data. These measures demonstrate fairness by ensuring that the service operates in line with children's reasonable expectations, avoids undue influence, and respects their rights and best interests.

- A school uses CCTV systems strictly for safety and security purposes, such as monitoring entrances, exits, and common areas. The use of CCTV is limited to what is necessary and proportionate and does not extend to areas where children would reasonably expect a higher level of privacy (e.g., classrooms, changing rooms, or rest areas). To ensure fairness, the school: carries out an assessment to determine whether CCTV is necessary and proportionate; avoids continuous or excessive monitoring beyond what is required for safety; places clear and visible warning signs explaining the presence and purpose of CCTV; provides accessible information to students and parents on how footage is used, who has access, and how long it is retained; restricts access to recordings to authorised personnel only. These measures ensure that monitoring does not exceed what children and their families would reasonably expect and that children are not subjected to unnecessary or disproportionate surveillance, thereby upholding fairness in practice.

Transparency

Transparency requires that individuals be provided with clear, accessible, and understandable information about how their personal data is processed. Under Rwanda's DPP Law, transparency is a core processing principle and is closely linked to effective communication, enabling data subjects to understand how their data is used and to meaningfully exercise their rights.

Children may not understand technical language, long-term consequences, or the implications of sharing data with institutions, service providers, or other users. Thus, the information provided should be child-friendly, in plain language, and delivered in ways that match the child's age, maturity, and the context in which the service or activity is used, and that support children's best interests and understanding.

Transparency in practice means that children and, where relevant, their parents or guardians should be able to understand in a practical and timely way:

- what personal data is collected;
- why it is collected;
- how it will be used;
- whether it will be shared, and with whom;
- how long it will be retained;
- whether the processing is optional or necessary;
- what rights are available and how those rights can be exercised;
- who to contact for further information or to make a request or complaint.

This information should not be buried in lengthy legal text or provided only once. It should be made available at the point of data collection, when new data uses are introduced, when consent is requested or withdrawn, and whenever the child or parent needs to make a meaningful choice.

In the context of children, information should be:

- adapted to the age and level of understanding of the child;
- clear, concise, and meaningful, avoiding unnecessary legal or technical language;

- presented in a way that reflects the setting, including both digital and non-digital environments;
- accessible not only to adults, but also to children themselves, where they are capable of understanding the information;
- complemented, where appropriate, by information directed separately to parents or guardians.

Data controllers should consider using layered notices, short summaries, icons, diagrams, audiovisual explanations, and contextual prompts, as children may require information in different formats and at different times to understand it.

Practical Examples

- A digital platform explains its data practices using simple language, icons, and short explanations tailored to different age groups. A short summary appears when the child creates an account, with links to fuller information for parents or guardians. The platform explains what information is required to operate the service, what is optional, whether messages or content may be visible to others, and how to change privacy settings later.
- A mobile application provides a clear explanation at the moment it asks to access the camera, microphone, location, or contacts. Instead of simply displaying a technical permission request, it explains why that access is needed, whether it is necessary for the service, whether the feature is optional, and what happens if permission is refused. Where the service involves children under the relevant age threshold, the explanation is also available to the parent or guardian in a form that supports informed parental decision-making.
- A healthcare provider explains to both the child, in age-appropriate terms, and the parent or guardian, in fuller detail, how the child's medical data will be collected, used, stored, and shared with other authorised professionals involved in treatment and how rights such as access or rectification may be exercised.
- A school provides parents and students with a clear notice at enrolment and again when introducing a new system, such as a learning platform, attendance system, or CCTV arrangement. The notice explains what student data is collected, the purpose for which it is used, whether it will be shared with service providers or public authorities, how long it will be kept, and who to contact with questions or rights requests. The school also provides a shorter child-friendly explanation to students.
- A public authority collecting children's data for social protection, child welfare, or related services explains the purpose of collection, whether providing the information is mandatory, the consequences of not providing it, and the rights available under the DPP Law. Information is given in a format understandable to both caregivers and, where appropriate, the child. Contact details for follow-up questions or complaints are included.

5.2 Purpose Limitation

Personal data should be collected for specific, explicit, and legitimate purposes, and not further processed in a manner that is incompatible with those purposes. In the context of children, this

principle requires particular care. Children may not fully understand how their data could be reused in the future, and secondary uses of data may create risks that are not immediately apparent. For this reason, purposes should be clearly defined, narrowly framed, and aligned with the best interests of the child.

To comply with the principle of purpose limitation, data controllers should:

- clearly define and document the purpose of processing before collecting personal data;
- ensure that the purpose is specific and understandable, including to children and their parents or guardians;
- limit processing to what is necessary for that purpose, avoiding broad or vague descriptions such as "improving services" without further explanation;
- avoid using children's data for new or unrelated purposes, particularly where such use may not be expected by the child or parent;
- assess whether any further use of data is compatible with the original purpose, taking into account:
    - the context in which the data was collected;
    - the relationship between the child and the data controller;
    - the potential impact on the child;
- where a new purpose is identified, ensure that an appropriate legal basis exists, and that clear information is provided before proceeding.

Practical Examples

- Personal data collected by a school for educational purposes, such as attendance records, grades, or behavioural information, is used solely to support teaching, learning, and school administration. The data is not used later for unrelated purposes, such as sharing it with third parties for commercial use, as this would be incompatible with the original purpose and the expectations of students and parents.
- A public authority collects children's data to provide social services. If the authority later considers using the data for statistical or research purposes, it first assesses whether this use is compatible with the original purpose, applies appropriate safeguards, and ensures that the data is used in a manner that does not adversely affect the child.

5.3 Data Minimisation

Personal data collected and processed should be adequate, relevant, and limited to what is necessary in relation to the specific purpose for which it is processed. Children may be less aware of the implications of sharing personal data, and excessive data collection may increase the risk of misuse, profiling, or unintended exposure. Thus, data controllers should adopt a cautious and proportionate approach, ensuring that only the minimum amount of data required is collected and used.

To comply with the principle of data minimisation, data controllers should:

- identify, in advance, the specific data elements required to achieve the intended purpose;
- critically assess whether each category of data is strictly necessary, and avoid collecting data "just in case" it may be useful in the future;
- ensure that data collection is proportionate to the context, considering the age of the child and the sensitivity of their data;
- configure systems and services so that privacy-protective settings are applied by default, limiting the amount of data collected and shared;
- avoid requesting or collecting additional personal data in exchange for access to a service, where such data is not necessary for its core functionality;
- periodically review data collection practices to ensure they remain appropriate and limited.

Practical Examples

- A digital learning platform allows children to use the service without requiring the creation of detailed profiles or the provision of excessive personal information. Optional fields are clearly marked and not required for access to the main functionality.
- A sports club collects only the information necessary to manage participation and ensure safety, such as the child's name, age, and emergency contact details. It avoids requesting unrelated information, such as detailed family background or unnecessary identifiers.

5.4 Accuracy

Personal data should be accurate and, where necessary, kept up to date. Inaccurate or outdated data should be corrected or deleted without undue delay. Children's circumstances, abilities, and needs may change over time, and inaccurate data may directly impact decisions affecting the child. Ensuring accuracy is therefore essential to avoid unfair or harmful outcomes. Accuracy also requires ongoing attention throughout the processing lifecycle.

To comply with the principle of accuracy, data controllers should:

- take reasonable steps to ensure that personal data is accurate at the time of collection;
- provide clear and accessible mechanisms for updating or correcting data;
- ensure that parents or guardians, and where appropriate the child, can easily request corrections;
- periodically review data, particularly where it is used to make decisions about the child;
- distinguish between verified information and subjective assessments (e.g., behavioral notes), ensuring that opinions are recorded appropriately and reviewed where necessary;
- avoid retaining outdated or irrelevant data that may no longer reflect the child's current situation.

Practical Examples

- A school ensures that student records, such as contact details, academic performance, and relevant support needs, are reviewed and updated regularly. Parents and students are provided with a clear, simple process for requesting corrections, and updates are reflected promptly to ensure that decisions about the child are based on accurate information.
- A healthcare provider maintains accurate and up-to-date medical records, ensuring that changes in a child's health condition, treatment, or allergies are promptly recorded. Parents and, where appropriate, the child are able to request corrections where information is incomplete or inaccurate.
- An online platform allows parents or, where appropriate, older children to review and update account information, such as age, preferences, or contact details. The service periodically prompts users to confirm or update their information to ensure continued accuracy.

5.5 Storage Limitation

Personal data should be retained only for as long as necessary for the purpose for which it was collected and processed. Once that purpose has been fulfilled, the data should be deleted, anonymised, or otherwise securely disposed of, unless retention is required by law.

Keeping children's data for long periods can increase risks, such as unintended future use of the data or negative effects on the child's development and opportunities. Therefore, data controllers and processors should adopt a careful, clearly defined approach to data retention, ensuring that information is retained only as long as necessary.

To comply with the principle of storage limitation, data controllers should:

- consider that children's data may require shorter retention periods, unless longer retention is clearly justified;
- define and document clear retention periods for each category of personal data, based on the purpose of processing and applicable legal requirements;
- ensure that retention periods are limited and proportionate, considering the nature of the data and the potential impact on the child;
- implement processes for the regular review and deletion of personal data;
- ensure that systems are designed to support automatic deletion or anonymisation where appropriate.

Practical Examples

- A digital service defines a retention policy under which inactive child accounts are deleted after a defined period of inactivity. Before deletion, the service notifies the user and offers the option to retain the account, if appropriate.

- Youth organisation retains registration and contact details only for the duration of the child's participation and a limited period thereafter for administrative purposes. After that period, the data is securely deleted.

6. Data Governance and Accountability

Under the DPP Law, data controllers and processors are responsible for ensuring and demonstrating compliance with the Law. Accountability is not limited to formal compliance. It requires data controllers and processors to put in place appropriate governance, documentation, and oversight mechanisms that ensure data protection is effectively implemented in practice.

In the context of children, accountability requires a proactive, structured, and risk-aware approach, recognising that:

- children are more vulnerable to risks arising from data processing;
- the impact of misuse or inappropriate processing may be long-term;
- additional safeguards and justification are required.

Data controllers and processors should therefore ensure that the processing of children's personal data is well documented, appropriately governed, effectively controlled, and regularly reviewed throughout the processing lifecycle.

To support effective accountability and governance, organisations should implement appropriate internal measures, including the following:

Governance and Internal Organisation

Data controllers and processors should:

- adopt internal policies and procedures specifically addressing the processing of children's personal data;
- clearly define roles and responsibilities, including:
    - staff responsible for data protection compliance;
    - staff handling children's data in operational contexts;
- ensure appropriate oversight of data protection risks, particularly in relation to high-risk processing involving children;
- integrate children's data protection considerations into organisational decision-making, procurement, and system design processes.

Record-Keeping and Documentation

Data controllers and processors should maintain records of processing activities, including:

- the purposes of processing;

- categories of personal data and data subjects, including children;
- legal bases relied upon, including parental consent where applicable;
- recipients or categories of recipients;
- retention periods or criteria used to determine retention;
- security and confidentiality measures applied.

Such records should be accurate and kept up to date, proportionate to the scale and nature of the processing activities, and available for internal review and regulatory oversight where required.

Decision-Making and Risk Management

Data controllers should document decisions relating to:

- the selection of legal bases for processing;
- the use of consent and mechanisms for withdrawal;
- Data Protection Impact Assessments (DPIAs) and safeguards implemented to mitigate identified risks;
- data sharing arrangements (including outside Rwanda) and the use of processors or service providers.

High-risk processing involving children should be subject to structured review, approval, and ongoing oversight processes.

Training and Awareness

Staff involved in processing children's personal data should receive appropriate and regular training relevant to the nature, sensitivity, and context of the processing activities they perform. Such training may include confidentiality and data protection obligations, secure handling and sharing of personal data, recognising and responding to risks involving children, and applying child-centred and rights-based approaches to processing.

Depending on the sector and type of processing involved, training may also cover areas such as handling sensitive health data, secure use of digital learning platforms, management of CCTV or monitoring systems, responding to data subject rights requests, breach response procedures, age verification and parental consent mechanisms, and the safe use of emerging technologies, including AI systems involving children's data.

Monitoring and Review

Data controllers and processors should regularly review processing activities involving children to ensure continued compliance with the DPP Law and this Guideline.

Policies, procedures, and safeguards should be updated where necessary to reflect:

- changes in processing activities or technologies;

- emerging risks;
- lessons learned from incidents or assessments;
- developments in legal or regulatory requirements.

Practical Examples

- A retail company operating a loyalty programme that may involve family or child-linked accounts clearly documents what data is collected (e.g. purchase history, contact details); the purposes (e.g. account management, rewards delivery); whether children's data is processed directly or indirectly; the legal basis relied upon, including consent where applicable. The company ensures that children's data is not reused for profiling or targeted marketing, documents these restrictions internally, and maintains records of consent and withdrawal where relevant.
- A school maintains structured documentation of all categories of student data processed (academic, administrative, health-related); purposes of processing (education, safety, administration); legal bases relied upon and access rights for staff. The school ensures that decisions involving sensitive data (e.g., health data) are documented and that staff handling such data are trained accordingly.
- An organisation using external service providers (e.g., cloud services) documents the nature of data shared with processors; the purposes of processing and contractual safeguards (confidentiality, security, deletion obligations). The organisation ensures that processors are subject to clear contractual obligations and that compliance is periodically reviewed.

7. Integrity, Confidentiality, and Security of Data

Under DPP Law, personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful access, disclosure, alteration, loss, or destruction. In the context of children, this obligation requires a heightened level of care, as security failures may expose children to increased risks, including identity misuse, exploitation, discrimination, reputational harm, or long-term consequences.

Security measures should therefore be proportionate to the risks, taking into account the nature and sensitivity of the data, the context and scale of processing and the potential impact on the child if the data is compromised.

To ensure the integrity and confidentiality of children's personal data, data controllers and processors should adopt a risk-based approach, combining appropriate technical and organisational measures tailored to the nature, sensitivity, and context of the processing. Such measures should include, in particular, regular risk assessment and the implementation of safeguards proportionate to the identified risks.

Access to children's personal data should be restricted to authorised personnel who need the information to perform their duties. Organisations should define access permissions according to staff roles, remove access when it is no longer required, and periodically review access rights.

Staff and other authorised persons should receive appropriate instructions on confidentiality and the secure handling of children's information

Risk Assessment

Data controllers and processors should:

- assess risks associated with processing children's personal data before and during processing;
- identify specific risks, such as unauthorised access or disclosure, misuse of sensitive data or excessive internal access;
- consider the likelihood and severity of harm to children and, where relevant, conduct a data protection impact assessment (DPIA);
- implement safeguards proportionate to the identified risks.

Access Control and Confidentiality

Access to children's data should be strictly limited to those who need it for a defined purpose.

Data controllers and processors should:

- implement role-based access controls;
- ensure staff access is limited to the minimum necessary;
- regularly review and update access rights;
- ensure staff handling children's data are subject to confidentiality obligations and understand their responsibilities;

Technical Security Measures

Data controllers and processors should implement appropriate technical safeguards, including:

- secure authentication mechanisms (e.g. strong passwords);
- encryption or equivalent protection, particularly for sensitive data;
- system monitoring and logging to detect unauthorised access;
- regular system updates and maintenance to address vulnerabilities.

Secure Storage and Handling

Personal data should be stored and handled securely in both digital and non-digital environments.

Data controllers and processors should:

- ensure secure storage of digital data through controlled systems;
- protect paper records through locked storage and controlled physical access;
- ensure that personal data is not left unattended or exposed;

- apply secure disposal methods when data is no longer needed.

Ongoing Review

Security measures should be:

- regularly reviewed and updated;
- adapted to changes in technology and processing activities;
- tested to ensure effectiveness in practice.

Practical Examples

- A school ensures that only authorised staff can access student records. For example, teachers access only their students' academic data, while sensitive information (e.g. health or welfare data) is restricted to designated staff. Staff are trained on confidentiality obligations and the appropriate handling of children's data.
- A healthcare provider processes children's medical data in secure systems with strict access controls. Only authorised medical professionals can access records, and staff are trained in confidentiality and data protection requirements. For storing children's data in paper format, a healthcare provider ensures that records are kept in locked cabinets, not left unattended, and handled only by authorised personnel. Documents are securely destroyed when no longer needed.

8. High-Risk Processing and Data Protection Impact Assessments (DPIAs)

Data processing involving children's personal data may pose greater risks to their rights and freedoms due to their vulnerability, limited awareness of risks, and the potential long-term impact of data use. Under the DPP Law, and as further elaborated in the guidance issued by the DPO on Data Protection Impact Assessments (DPIAs).[1] Data controllers are expected to assess such risks in advance and implement appropriate safeguards.

DPIA should therefore be conducted before initiating processing that is likely to result in high risk, in particular where it involves:

- systematic monitoring of children (e.g. tracking, surveillance);
- profiling or automated decision-making;
- large-scale processing of children's data;
- processing of sensitive personal data;
- use of new or innovative technologies (e.g. AI, biometric systems);

[1] https://dpo.gov.rw/fileadmin/DPO/ComplianceTools/-_dpia-guide-and-form.pdf

- processing that may significantly affect children's behaviour, development, or access to services.

A DPIA is a structured process that enables data controllers to identify, assess, and mitigate risks at an early stage. Where high risks cannot be adequately mitigated, the data controller should reconsider or adapt the processing activity. For further information, check the guidance note on the DPIA at https://dpo.gov.rw/fileadmin/DPO/ComplianceTools/-_dpia-guide-and-form.pdf

Practical Examples

- A shopping mall introduces technologies to analyse visitor behaviour (e.g. movement patterns or dwell time). Before implementation, a DPIA is conducted to assess risks to children, including surveillance, profiling, and potential data misuse. The assessment leads to a limited scope of monitoring, the avoidance of individual identification, and the application of strict safeguards.
- A digital learning platform introduces AI-based tools to analyse student performance and provide personalised recommendations. A DPIA is conducted to assess risks such as profiling, unfair decision-making, and potential negative impact on children's development. Based on the assessment, the platform ensures transparency, limits automated decision-making, and introduces teacher oversight.
- A mobile application aimed at children includes a feature that tracks location for safety or service functionality. A DPIA assesses whether location tracking is necessary, whether less intrusive alternatives exist, and how to minimise risks. As a result, location tracking is disabled by default and activated only with clear safeguards.

9. Privacy by Design and by Default

Under Rwanda's DPP Law, personal data must be processed in a manner that is lawful, fair, transparent, and secure, and limited to what is necessary. These principles should be integrated into the design and operation of systems and services from the outset, rather than addressed only after deployment.

Where services are likely to be accessed by children, this requires a child-centred design approach, ensuring that systems:

- anticipate risks specific to children;
- provide appropriate safeguards by default;
- support children and parents in making informed and meaningful choices.

Design choices should therefore reflect the best interests of the child and ensure that children are not exposed to unnecessary risks through the service's structure or functionality.

Privacy by design and by default requires organisations to embed data protection into how services or products work, not just how they are described. In the context of children, this means ensuring that:

- privacy is the default setting, not an option;
- design does not exploit children's behaviour or lack of awareness;

- services support safe and informed use from the outset.

To implement privacy by design and by default, data controllers should:

1. **Integrate data protection into system/service/product design**
    - consider data protection requirements at the earliest stages of system development;
    - assess how the service will be used by children and identify potential risks;
    - ensure that the collection and use of personal data is necessary and proportionate;
    - limit functionality that relies on extensive data collection where less intrusive alternatives exist.
2. **Apply privacy protective defaults**
    - configure systems so that privacy-protective settings are enabled by default, without requiring user action;
    - ensure that profiles are not publicly visible by default and tracking, location sharing, or data sharing features are disabled unless necessary;
    - avoid requiring children to change settings to achieve basic privacy protection.
3. **Avoid manipulative or misleading design features that:**
    - encourage excessive sharing of personal data;
    - use incentives, pressure, or rewards to influence children's behaviour;
    - make privacy-protective options harder to select;
4. **Clearly Separate Optional Features**
    - distinguish clearly between core service functionality and optional features that require additional data processing;
    - ensure that optional features are not enabled by default, are accompanied by clear explanations and can be easily declined or withdrawn without affecting access to core services.

5 Support Informed Decision-Making

- provide clear, age-appropriate information at relevant points in the user journey;
- design interfaces that help children and parents understand choices and manage settings easily;
- ensure that controls (e.g. privacy settings, consent management) are accessible and usable.

Practical Examples

- A mobile application designed for children disables location sharing, contact access, and public profile visibility by default. These features can only be activated with clear explanations and appropriate safeguards, ensuring that children are not exposed to risks without informed choices.

- A gaming platform avoids using design features that encourage children to disclose additional personal data in exchange for rewards (e.g., unlocking levels or bonuses). Privacy settings are easy to access, and children are not steered towards less protective options.
- A learning platform provides core educational functionality without requiring extensive personal data. Optional features, such as forums or social interaction tools, are clearly separated, require additional safeguards, and are not enabled by default.
- A company running a promotional competition ensures that participation by children does not require excessive personal data. Optional marketing features are clearly separated and not pre-selected, allowing parents and children to participate without unnecessary data sharing.

10. Personal Data Breach Notifications

A personal data breach may involve the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Where the breach concerns children's personal data, it may present higher risks because children may be more vulnerable to misuse, exposure, discrimination, exploitation, or long-term harm.

A breach response should be prepared before an incident occurs. Under Rwanda's DPP Law, personal data breaches must be handled promptly. The DPO provides a Personal Data Breach Notification Form and a dedicated Report a data breach service.[2] The DPP Law and the form indicate that processors must notify the data controller within 48 hours after becoming aware of an incident, and data controllers must notify the supervisory authority within 48 hours after becoming aware of a breach.

Data controllers and processors processing children's personal data should have procedures in place to:

- detect and assess suspected personal data breaches without undue delay;
- identify what data is affected, including whether it concerns children or sensitive personal data;
- assess the likely consequences for children, including risks of identity misuse, exposure, discrimination, distress, safeguarding concerns, or unauthorised profiling;
- contain the breach and reduce harm, for example by disabling access, resetting credentials, recovering data, or stopping unauthorised disclosure;
- notify the Data Protection and Privacy Office within the applicable legal timeframe where required;
- notify affected children and/or their parents or guardians where the breach is likely to result in a high risk to their rights and freedoms;
- document the breach, decisions taken, notifications made, and corrective measures implemented;

[2] https://dpo.gov.rw/services/report-a-data-breach

- review the incident and strengthen safeguards to prevent recurrence.

Where children are affected, communications should be clear, calm, and practical. They should explain what happened, what data was affected, what risks may arise, what steps the organisation has taken, and what the child or parent can do to protect themselves.

Practical Examples

- A learning platform used by schools discovered that student profiles and assessment results were accessible to unauthorized users. The provider disables the affected function, informs the school, identifies the categories of student data exposed, and supports the data controller in assessing notification obligations. Within 48 hours, the learning platform informed the DPO. Parents and students also received clear information about the incident, the data involved, and the measures taken to prevent recurrence.
- A clinic identifies unauthorised access to children's medical records. Because the data is sensitive, the clinic treats the incident as high-risk, restricts access, investigates the source, informs the supervisory authority within 48 hours, and communicates with parents or guardians in a way that explains the possible consequences and available support.

11. Profiling and Automated Decision-Making

Children require particular protection in relation to profiling and automated decision-making because such processing may significantly influence their behaviour, opportunities, choices, or development. Children may not fully understand how their personal data is analysed, how recommendations are generated, or how automated systems may affect decisions concerning them.

In the context of children, profiling and automated processing may create heightened risks, including:

- excessive monitoring of behaviour, habits, or preferences;
- exclusion, discrimination, or unfair treatment;
- inaccurate or disproportionate assessments;
- long-term impacts resulting from persistent profiling;
- exposure to harmful or inappropriate content;
- reduced autonomy due to excessive reliance on automated systems.

For this reason, profiling and automated processing involving children should be approached with particular caution, ensuring that processing is:

- necessary and proportionate;
- transparent and understandable;
- subject to meaningful safeguards and oversight;
- aligned with the best interests of the child.

Data controllers and processors should ensure that children are not treated merely as sources of behavioural data, but as individuals entitled to heightened protection and respectful treatment in both digital and non-digital environments.

Data controllers processing children's personal data should:

Limit Profiling Activities

- avoid profiling children unless it is strictly necessary for a legitimate and proportionate purpose;
- assess whether the same objective can be achieved without profiling or through less intrusive means;
- ensure that profiling does not result in unfair outcomes, exclusion, or unnecessary monitoring;
- avoid persistent or large-scale behavioural tracking of children.

Where profiling is used, data controllers should:

- clearly explain how profiling works and what effects it may have;
- apply additional safeguards appropriate to children's rights and interests;
- ensure that profiling does not expose children to inappropriate or harmful content.

Ensure Human Oversight

Where automated tools or systems contribute to decisions affecting children, data controllers should ensure:

- meaningful human involvement in decision-making;
- the possibility to review, challenge, or explain decisions;
- that automated processing does not produce unfair, inaccurate, or disproportionate outcomes.

Particular care is required where decisions may affect access to services, participation in programmes or activities as well as opportunities, welfare, or safety.

Prevent Harmful or Inappropriate Outcomes

Data controllers should take reasonable measures to ensure that systems relying on recommendations, algorithms, automated ranking, or scoring do not expose children to:

- harmful or inappropriate content;
- unsafe interactions or environments;
- discriminatory or exclusionary outcomes;
- manipulative recommendation patterns encouraging excessive engagement.

Practical Examples

- A gaming platform does not recommend content or in-game purchases based on detailed behavioural profiling of children, particularly where such recommendations may encourage excessive engagement or spending. The platform ensures that recommendation systems prioritise age-appropriate content and do not rely on intrusive monitoring of behaviour.
- Social media platform used by children applies preventive measures and safeguards to prevent algorithms from repeatedly promoting harmful, inappropriate, or age-inappropriate content. The platform also limits the use of engagement-based profiling that could encourage compulsive use or exposure to harmful material.

12. Marketing Directed at Children

Marketing directed at children requires particular care because children may be less able to recognise commercial influence, assess persuasive techniques, or understand how their personal data is used for advertising purposes.

Marketing practices involving children's personal data should therefore be:

- fair and transparent;
- respectful of children's vulnerabilities and evolving capacities;
- proportionate and aligned with the best interests of the child.

Data controllers should avoid practices that:

- exploit children's emotions, fears, or lack of experience;
- encourage excessive spending or engagement;
- pressure children into sharing personal data;
- blur the distinction between entertainment, education, and advertising.

Therefore, data controllers should ensure that marketing activities involving children's personal data are fair, transparent, proportionate, and respectful of children's rights and vulnerabilities. In particular, data controllers should:

Avoid Behavioural Advertising Targeting Children

- avoid using children's browsing history, interactions, preferences, or location data to deliver targeted advertising;
- avoid tracking children across services, platforms, or devices for marketing purposes;
- avoid combining data from multiple sources to create behavioural or commercial profiles of children.

Ensure Fair and Transparent Marketing Practices

- clearly distinguish advertising and promotional content from other content or services;
- ensure that children and parents can easily recognise when content is promotional in nature;

- avoid presenting marketing in a misleading, manipulative, or overly persuasive manner;
- ensure that access to services, activities, or benefits does not depend on agreeing to unnecessary marketing-related processing or data sharing.

Limit Data Collection for Marketing Purposes

- avoid collecting more personal data than is necessary for promotional or communication activities;
- ensure that optional marketing activities are clearly separated from core services and functionalities;
- provide clear and accessible mechanisms allowing children and/or parents to refuse, manage, or withdraw from marketing communications at any time.

Practical Examples

- A company organising a competition for children collects only the information necessary to administer participation and clearly explains how the data will be used. Participation is not conditional on agreeing to receive marketing communications.
- A restaurant or entertainment venue offering child-focused promotions ensures that marketing materials are clearly identifiable as advertising and do not pressure children into disclosing additional personal information in exchange for rewards or benefits.

13. Use of Artificial Intelligence (AI) and Emerging Technologies

The use of artificial intelligence (AI) and emerging technologies involving children's personal data may present heightened risks to children's rights, freedoms, development, dignity, and well-being. Such technologies may increase the scale and complexity of data processing, enable extensive monitoring or profiling, influence children's behaviour and choices, or affect access to opportunities, services, and information.

Children may be less able to understand how AI systems operate, how decisions or recommendations are generated, or the potential long-term consequences of automated processing. For this reason, data controllers and processors deploying AI systems involving children's personal data should apply a particularly high standard of protection and ensure that processing remains lawful, fair, transparent, necessary, proportionate, and aligned with the best interests of the child.

The use of AI or emerging technologies does not reduce or replace the obligations of data controllers and processors under data protection law. Data controllers and processors remain responsible for ensuring that processing involving AI systems complies with all applicable data protection principles and safeguards.

Where AI systems are likely to process children's personal data, data controllers and processors should, in particular:

- assess whether the use of AI is genuinely necessary and whether the intended objective can reasonably be achieved through less intrusive means;

- conduct a DPIA where AI systems may present high risks to children's rights and freedoms;
- ensure meaningful human oversight over decisions or recommendations affecting children;
- do not use AI systems that may manipulate, exploit, or unfairly influence children's behaviour, vulnerabilities, emotions, or choices;
- avoid excessive monitoring, behavioural analysis, or profiling of children;
- ensure that children and parents receive clear, accessible, and understandable information regarding the use of AI systems and their potential effects;
- regularly review AI systems to identify and address risks, inaccuracies, bias, discriminatory outcomes, or unintended harmful impacts on children;
- ensure that AI systems processing children's personal data are subject to appropriate governance, testing, monitoring, and security safeguards.

Particular caution should be exercised where AI technologies involve:

- behavioural prediction or recommendation systems;
- automated assessment, scoring, or ranking of children;
- facial recognition or other biometric technologies;
- emotion recognition or behavioural inference systems;
- AI-enabled educational technologies;
- systems capable of influencing children's choices, behaviour, interactions, or online engagement.

Particular caution should also be exercised regarding technologies intended to infer emotions, psychological states, attention levels, or behavioural characteristics of children, especially in educational, monitoring, or safety-related contexts.

Practical Examples

- An educational platform using AI tools to analyse student performance conducts a DPIA before deployment, limits the amount of personal data processed, and ensures that important educational decisions are not based solely on automated assessment or scoring.
- A social media platform used by children implements safeguards to prevent recommendation algorithms from repeatedly promoting harmful, addictive, or age-inappropriate content, and limits the use of engagement-based profiling designed to maximise screen time or behavioural influence.

14. Data Sharing and Engagement with Data Processors

Sharing children's personal data with third parties requires particular care and should be approached in a manner that is lawful, necessary, proportionate, and consistent with the best interests of the child.

Under Rwanda's DPP Law, data controllers remain responsible for ensuring that personal data is processed in compliance with the Law, including where processing activities are carried out by data processors on their behalf.

In the context of children, inappropriate or excessive sharing of personal data may expose children to heightened risks, including:

- unauthorised use of data;
- profiling or commercial exploitation;
- loss of confidentiality;
- exposure to harmful content or environments;
- long-term impacts resulting from wider or uncontrolled dissemination of personal data.

Data controllers should therefore carefully assess whether sharing is genuinely necessary and ensure that appropriate safeguards are in place before any disclosure occurs.

Before sharing children's personal data, controllers should:

- clearly identify the purpose of sharing;
- assess whether sharing is necessary to achieve that purpose;
- limit disclosure to the minimum amount of data required;
- avoid sharing data for purposes that are incompatible with the original reason for collection;
- consider whether the same objective can be achieved through less intrusive means.

Particular care should be taken where:

- sensitive personal data is involved;
- data may be shared with multiple parties or transferred outside Rwanda
- data may be used for commercial, profiling, or marketing purposes.

Children and, where appropriate, their parents or guardians should be informed:

- whether data will be shared;
- with whom it will be shared;
- why sharing is necessary;
- what safeguards apply;
- whether the sharing is optional or required by law.

This information should be presented in a clear and understandable manner, consistent with the child's age and level of understanding.

Where data controllers use processors, they should ensure that the data processor provides sufficient guarantees regarding compliance with the DPP Law, is registered with the DPO as a data processor and data processing is governed by a clear contractual arrangement defining:

- the purpose of processing;
- confidentiality obligations;
- security measures;
- restrictions on further use or disclosure;
- deletion or return of data at the end of the service;
- processors do not reuse children's personal data for their own purposes without a valid legal basis.

For further information, consult the guide on contractual provisions for processing at https://dpo.gov.rw/fileadmin/DPO/ComplianceTools/-_Guide-On-Contractual-Provisions-For-Processing-Of-Personal-Data__2_.pdf

Practical Examples

- A school uses an external digital learning platform to support teaching activities. Before sharing student data, the school ensures that:
  - ✓ the provider applies appropriate security and confidentiality measures;
  - ✓ the contract prohibits reuse of student data for advertising, analytics, or unrelated commercial purposes;
  - ✓ only the data necessary for educational purposes is shared.
- A healthcare provider shares a child's medical information with another authorised healthcare professional involved in treatment. The sharing is limited to information necessary for continuity of care and is carried out under professional confidentiality obligations and applicable legal safeguards.
- A public authority shares children's data with another competent authority as required by law for child protection or social support purposes. Sharing is limited to what is necessary, appropriately documented, and carried out with safeguards to ensure confidentiality and the protection of the child's rights.

15. Cross-Border Transfers of Children's Personal Data

Transfers of children's personal data outside Rwanda require particular care due to potential risks posed by differing data protection levels, reduced oversight, or broader access to personal data in other jurisdictions.

Under the DPP Law, international transfers of personal data should occur only when appropriate safeguards and legal requirements are met. Data controllers should also take into account the guidance issued by DPO on cross-border data transfers and the appropriate safeguards.[3]

In the context of children, data controllers should ensure that transfers outside Rwanda:

- do not undermine the level of protection afforded under the DPP Law;
- are necessary and proportionate;
- include safeguards appropriate to the sensitivity and risks associated with children's data.

[3] E.g. https://dpo.gov.rw/fileadmin/DPO/ComplianceTools/-_Standard_Contractual_Clauses_for_Transfer_Personal_Data_Outside_Rwanda_.pdf

Before transferring children's personal data outside Rwanda, data controllers should:

- identify the destination country and assess whether appropriate safeguards are available;
- identify and document the legal basis and safeguards relied upon for the transfer;
- assess risks associated with the transfer, particularly where sensitive data or large-scale processing is involved;
- ensure that the receiving party applies appropriate data security measures;
- ensure that children and parents are informed, where appropriate, about the transfer, its purposes and applicable safeguards.

Where servers or cloud service providers located outside Rwanda are used, data controllers should ensure that the processing and storage arrangements comply with the requirements of the DPP Law, which generally requires that personal data be stored in Rwanda. Storage of personal data outside Rwanda is permitted only where the data controller or processor holds a valid authorisation issued by the DPO.

In the context of children's personal data, data controllers should apply particular care before using server or cloud infrastructure located outside Rwanda and should ensure that the receiving party applies safeguards that ensure a level of protection consistent with the DPP Law and that processing agreements clearly define:

- the purpose and scope of processing;
- confidentiality and security obligations;
- restrictions on further use or disclosure of data;
- retention, deletion, and return obligations.

Data controllers should also ensure that, where appropriate, children and parents are informed that personal data may be stored outside Rwanda, including the purpose of the storage, the safeguards applied, and any implications for the protection of the data.

Practical Examples

- A school uses a cloud-based learning platform hosted outside Rwanda. Before using the service, the school obtains the required authorisation for storage outside Rwanda, assesses the provider's security and confidentiality measures, and ensures that contractual safeguards prohibit the provider from reusing student data for advertising or unrelated analytics.
- A healthcare provider uses an external laboratory information system hosted abroad. Due to the sensitivity of children's medical data, the provider conducts a risk assessment, ensures that only necessary information is transferred, and verifies that the processor applies strict confidentiality and security measures consistent with Rwanda's legal requirements.

16. Data Subject Rights in the Context of Children

Data subject rights are a core safeguard under the DPP Law and should be implemented in ways that reflect the specific needs and vulnerabilities of children. Under the law, children benefit from the same data subject rights as any other individual, including the rights to:

- information and transparency;
- access;
- rectification;
- erasure;
- objection to certain processing activities;
- restriction of processing;
- data portability, where applicable;
- protection against certain forms of automated decision-making.

In the context of children, these rights require particular attention to ensure that they are not only formally available, but also accessible, understandable, and effective in practice.

Children may face additional barriers in understanding how their data is processed, what rights they have and how to exercise them, and the possible consequences of processing activities. Thus, data controllers and processors should adopt a child-centered approach, ensuring that children and, where appropriate, their parents or guardians can meaningfully exercise their rights.

Data controllers should ensure that rights may be exercised:

- directly by the child, where appropriate, and taking into account the child's age, maturity, and understanding;
- by a parent or legal guardian acting in the child's interest.

Where requests are made by parents or guardians, organisations should apply proportionate measures to verify parental responsibility, while avoiding unnecessary or excessive data collection.

Data controllers should ensure that procedures for exercising rights are:

- simple, accessible, and easy to understand;
- available through appropriate channels (e.g., online, in person, email, or forms);
- adapted, where appropriate, to the age and understanding of the child;
- free from unnecessary complexity or barriers.

Information about rights should:

- use clear and plain language;
- explain what the right means in practice;
- explain how to make a request and what happens afterwards.

Data controllers should:

- respond to requests within the timeframes established under the DPP Law;
- provide responses in a clear and understandable manner;
- explain reasons where a request cannot be fully satisfied;

- ensure that exercising rights does not result in unfair treatment or disadvantage to the child.

Where processing is based on consent, children and/or parents should be able to:

- withdraw consent easily;
- stop optional processing activities;
- request deletion of data processed solely on the basis of consent, where appropriate.

Data controllers should ensure that withdrawal mechanisms are:

- easy to locate and use;
- not misleading or unnecessarily difficult;
- clearly explained.

Where profiling or automated decision-making is used, data controllers should ensure that:

- children and parents are informed about such processing;
- meaningful explanations can be provided;
- requests for review or human intervention can be exercised effectively.

Practical Examples

- A digital platform provides children and parents with accessible tools to review account information, adjust privacy settings, download personal data and delete accounts or specific content. The platform explains these options using child-friendly language and ensures that account deletion requests can be completed without unnecessary obstacles.
- A school provides parents and students with a straightforward process for requesting access to student records, correcting inaccurate information, and obtaining explanations regarding how data is used in educational systems or digital learning platforms. Information is provided in a language understandable to both parents and students.
- A public authority processing children's personal data for social protection or welfare services provides accessible procedures for requesting access to records, correcting inaccurate information, and understanding how decisions are made and what data is used. Information is provided in a way that is understandable to both caregivers and, where appropriate, the child.

Annex 1 – Step-by-Step Approach to Age Assurance and Parental Consent

This Annex provides an illustrative approach to help data controllers and processors determine:

- whether a service is likely to be accessed by children;
- whether parental consent may be required under the DPP Law;
- what level of age assurance or verification may be appropriate.

The approach should always be applied in a risk-based and proportionate manner, considering the nature of the service, the risks associated with processing, the sensitivity of the data involved and the likelihood that children will use the service.

Step 1 – Is the service likely to be accessed or used by children?

Consider:

- the nature of the service;
- the design, language, or marketing of the service;
- whether children are known or reasonably likely users;
- whether the service is accessible to children in practice.

If No

Apply general data protection requirements.

If Yes

Proceed to Step 2.

Step 2 – What type of data and processing is involved?

Assess:

- whether sensitive personal data is processed;
- whether profiling or behavioural tracking is used;
- whether geolocation or public sharing features are enabled;
- whether the service includes interaction with unknown users;
- whether automated decision-making or AI tools are used;
- whether processing may significantly affect children.

Lower-Risk Processing Examples

- basic educational tools;

- limited account management;
- offline registration activities.

Higher-Risk Processing Examples

- social networking features;
- behavioural advertising;
- biometric processing;
- profiling or recommendation systems;
- large-scale monitoring.

Proceed to Step 3.

Step 3 – Is parental consent required under the DPP Law?

Under Article 9 of the DPP Law:

- where the child is under the age of sixteen (16);
- and consent is relied upon as the legal basis;

consent must be obtained from a holder of parental responsibility, unless another lawful basis applies.

Data controllers should first assess:

- whether consent is the appropriate legal basis;
- whether another legal basis under Article 46 applies more appropriately.

Where consent is not freely given or there is a clear imbalance of power, another legal basis may be more appropriate.

Step 4 – What level of age assurance or verification is appropriate?

The level of assurance should reflect the risks associated with the processing.

Lower-Risk Situations

Possible measures may include:

- self-declaration of age;
- basic consistency checks;
- simple parental email confirmation.

Medium-Risk Situations

Possible measures may include:

- verified parental contact confirmation;

- account-based parental approval;
- additional age estimation measures.

Higher-Risk Situations

Additional safeguards may include:

- stronger parental verification;
- enhanced age-assurance measures;
- stricter privacy defaults;
- additional human oversight;
- limitation or disabling of certain features for children.

Step 5 – Ongoing Review

Data controllers should:

- periodically review whether age assurance measures remain effective and proportionate;
- reassess risks where services, technologies, or processing activities change;
- monitor whether children may bypass safeguards;
- ensure that consent withdrawal mechanisms remain accessible and effective.

Annex 2 – Illustrative Examples of High-Risk Processing Involving Children

Certain processing activities involving children's personal data may present heightened risks to children's rights and freedoms and therefore require additional safeguards, enhanced oversight, and, where appropriate, a Data Protection Impact Assessment (DPIA).

This Annex provides non-exhaustive examples of processing activities that may be considered high-risk in the context of children.

A. Profiling and Behavioural Monitoring

Processing activities involving:

- behavioural profiling;
- monitoring of online activity;
- tracking habits, preferences, or interactions;
- prediction or analysis of behaviour.

Examples

- social media platforms analysing engagement patterns;
- gaming platforms tracking behaviour to influence purchases;
- retail services creating behavioural marketing profiles of children.

B. Large-Scale Processing of Sensitive Personal Data

Processing involving:

- health data;
- disability information;
- biometric data;
- welfare or social protection information;
- psychological or behavioural assessments.

Examples

- school systems processing health and counselling records;
- healthcare platforms managing children's medical information;
- child welfare databases.

C. Automated Decision-Making Affecting Children

Use of systems that:

- evaluate;
- rank;
- score;
- categorise;
- recommend;
- or make decisions about children.

Examples

- AI systems assessing student performance;
- automated eligibility assessments for services;
- algorithmic moderation systems affecting children's access or participation.

D. Systematic Monitoring or Surveillance

Monitoring activities involving:

- CCTV;

- geolocation tracking;
- online monitoring;
- device monitoring;
- classroom surveillance technologies.

Examples

- facial recognition attendance systems;
- remote examination monitoring tools;
- continuous tracking of children's movements through wearable devices.

E. Public or Large-Scale Sharing of Children's Data

Processing activities where children's personal data may be:

- publicly visible;
- widely disseminated;
- or shared across multiple entities.

Examples

- public publication of student achievements with identifiable information;
- online platforms enabling unrestricted public profiles for children;
- sharing data across multiple commercial partners.

F. Processing Involving Emerging Technologies or AI

Use of technologies that may:

- infer emotions or behaviour;
- personalise recommendations;
- influence behaviour;
- create persistent digital profiles.

Examples

- AI recommendation systems targeting children;
- emotion-recognition technologies;
- adaptive advertising systems;
- AI-powered educational analytics.

G. Cross-Border Processing and Cloud Infrastructure

Processing involving:

- storage outside Rwanda;
- international transfers;
- multiple subcontractors;
- cloud environments involving children's data.

Examples

- cloud-based educational platforms hosted abroad;
- international social networking services;
- outsourced child welfare or healthcare systems.