ORGANISATIONAL PRIVACY RISK ASSESSMENT

A Single Scored Assessment Form, with a Children's Data Module

This form has been designed by the Open Institute to help organisations assess their privacy risk. The form is built primarily on the Office of the Data Protection Commissioner, Kenya (ODPC) Guidance Note on Data Protection Impact Assessment and Guidance Notes for Processing Children's Data (2025). Full source details are listed in the References at the end of this document.

For a data controller or processor assessing a system, project, or processing activity. Complete Part A for context, then work through every question in Part B. Add up your points and use Part C to find your risk level and required action.

Before You Begin: Please Read

This form is a practical aid for identifying and scoring privacy risk. It is not legal advice and does not replace a lawyer, a qualified Data Protection Officer, or formal legal review.

The point weightings were developed by the Open Institute as a reasonable, structured estimate for prioritising action. They are not derived from a single published legal standard, and your organisation's own risk appetite or sector-specific rules may justify different weights.

This form benchmarks several jurisdictions' frameworks for comparison, but organisations processing data outside Kenya remain fully responsible for complying with the specific laws of every jurisdiction in which they operate.

Where a High or Critical score results, or where children's data is involved, escalate to a Data Protection Officer, legal counsel, or the ODPC (or the relevant supervisory authority) before proceeding.

This document reflects publicly available guidance as of the assessment date. Verify you are working from the current version of any law, regulation, or guidance note cited before relying on it for a compliance decision.

Part A: Processing Activity Overview

Name of project / system / service	
Data controller / processor	
Assessor name and role	
Date of assessment	
Brief description of the processing (what data, how collected, why, who has access, retention, third parties)	
Categories of data subjects (tick all that apply)	□ *General public / adults* □ *Employees* □ *Customers/users* □ *Children (under 18)* □ *Vulnerable adults* □ *Other: _____*
Categories of personal data involved	□ *Basic identifiers (name, contact)* □ *Location/tracking* □ *Financial* □ *Sensitive data (health, biometric, genetic, ethnicity, religion, sex life)* □ *Behavioural / profiling data* □ *Images, audio or video* □ *Other: _____*
Lawful basis relied upon (DPA Act s.30)	
Are children data subjects, or reasonably likely to be?	*Yes, complete Part B.3* *No, skip Part B.3*

Part B: Weighted Risk Questionnaire

Every question below is worded so that answering 'Yes' means a risk or gap is present. For each question: write Yes or No in the third column. If you answered Yes, copy the points value into the Score column. If you answered No, write 0 in the Score column. If you are unsure, or the safeguard is not fully in place yet, treat it as Yes and score the points, since an unresolved gap is itself a risk. At the end of each subsection, add up every number in the Score column into the Subtotal box.

Worked example: *the question 'Is the data unencrypted at rest or in transit?' carries 3 points. If your answer is Yes (some of the data is not encrypted), you write '3' in the Score column. If your answer is No (everything is encrypted), you write '0'.*

Question (answering "Yes" means a risk or gap is present)	Points if Yes	Your answer (Yes/No)	Score
Are you collecting sensitive information, like health, biometric, genetic, ethnicity, religious, or criminal data, from a large number of people?	4		
Does a system regularly analyze people to make decisions that seriously affect them (e.g. approving a loan, screening a job application, setting a price) without a human reviewing it?	4		
Are you continuously watching or tracking people, through cameras in public spaces or by monitoring their behaviour over time?	3		
Are you using new or emerging technology, like AI, facial recognition, or smart/connected devices, in a way not previously tried at your organisation?	2		
Could this processing stop someone from getting a service, signing a contract, or exercising a right if they refuse or cannot provide certain data?	3		
Will you link or merge this data with other datasets to learn more about someone than either dataset shows on its own?	3		
Does the processing involve large-scale processing, cross-border transfer, or a large number of data subjects?	3		
B.1 SUBTOTAL (add up the Score column above)			

B.2 Data Protection Practice Gaps

These check for safeguards a data handler should already have in place. Each question is phrased so that 'Yes' means the safeguard is missing or weak.

Question (answering "Yes" means a risk or gap is present)	Points if Yes	Your answer (Yes/No)	Score
Are you collecting or processing personal data without a clear, documented legal basis?	3		
Is your privacy notice missing, unclear, or not written in plain, accessible language?	2		
If relying on consent, would someone be blocked from the service if they said no?	2		
Are you collecting anything 'just in case' that you do not actually need for the stated purpose?	2		
If you later use this data for a new purpose, would you skip seeking fresh permission?	2		
Would inaccurate data likely go undetected or uncorrected, with no easy way to catch or fix it?	1		
Is this data kept indefinitely by default, with no defined retention schedule?	2		
Does deletion depend on someone remembering, rather than happening automatically at the end of the retention period?	2		
Can people access this data who do not genuinely need it, i.e. no role-based access controls?	2		
Is any of the data unencrypted, either at rest or in transit?	3		
Has the system NOT been independently tested for security weaknesses recently?	2		
Are vendors or partners given this data without checking their own safeguards?	2		
Is data shared with any third party without a signed contract or data-processing agreement?	2		
Does data cross borders without an appropriate transfer safeguard in place?	2		
Could this system make a significant automated decision about someone without a human reviewing it?	3		
Would you be unable to fulfil a request to access or delete someone's data within a reasonable time?	2		
Do you lack a breach response plan, including who to notify and within what deadline?	3		
B.2 SUBTOTAL (add up the Score column above)			

B.3 Children's Data (complete only if Part A indicates children are, or may be, data subjects)

This section reflects ODPC Guidance Notes for Processing Children's Data (2025) and comparable requirements under GDPR Art. 8, the ICO's Age Appropriate Design Code, COPPA, and POPIA s.35. Points are weighted higher, reflecting the heightened protection children are owed. As above, 'Yes' always means a risk or gap is present.

Question (answering "Yes" means a risk or gap is present)	Points if Yes	Your answer (Yes/No)	Score
Has the impact of the processing on the child's safety, dignity, and development NOT been documented, i.e. no best-interests assessment?	3		
Is verifiable parental or guardian consent missing, with no valid exemption identified?	5		
Is there no proportionate age-verification mechanism in place?	3		
Is there no mechanism to verify that the person giving consent is genuinely the child's parent or guardian?	3		
Where the child's sensitive data is involved, is separate explicit parental consent missing?	4		
Does the processing involve profiling a child for direct marketing?	4		
Does the processing involve automated decision-making that affects the child, without human intervention?	4		
Is withdrawing consent harder than giving it?	2		
Is the service a public-facing or social platform accessible to children?	2		
B.3 SUBTOTAL (add up the Score column above, or leave blank if not applicable)			

Part C: Scoring, Risk Level and Required Action

Add B.1 + B.2 (+ B.3 if completed) into the total below, then find your risk level in the matching table.

B.1 subtotal	
B.2 subtotal	
B.3 subtotal (if applicable)	
TOTAL SCORE	

If children are NOT data subjects (Part B.3 not completed): maximum possible score is 59

Score range	Risk level	Required action
0 to 10	**Low**	Document this assessment and proceed. Monitor with a routine review, at least annually or on material change.
11 to 25	**Medium**	Assign an owner to close the gaps identified in Part B within a set timeframe. DPO sign-off required before proceeding. Re-review within 12 months.
26 to 45	**High**	Do not proceed (or pause current processing) until the priority items in Part D are actioned. Requires senior management and DPO sign-off. Review within 6 months.
46 to 59	**Critical**	Do not begin, or continue, processing until these gaps are resolved. Escalate to the Data Protection Officer and consult the ODPC (or equivalent supervisory authority) before proceeding.

If children ARE data subjects (Part B.3 completed): maximum possible score is 89

Score range	Risk level	Required action
0 to 15	**Low**	Document this assessment and proceed. Monitor with a routine review, at least annually or on material change.
16 to 37	**Medium**	Assign an owner to close the gaps identified in Part B within a set timeframe. DPO sign-off required before proceeding. Re-review within 12 months.
38 to 66	**High**	Do not proceed (or pause current processing) until the priority items in Part D are actioned. Requires senior management and DPO sign-off. Review within 6 months.
67 to 89	**Critical**	Do not begin, or continue, processing until these gaps are resolved. Any unmitigated risk to a child must be escalated to the Data Protection Officer, with mandatory prior consultation with the ODPC (or equivalent supervisory authority) before proceeding.

** The children's-data scale carries higher thresholds because its maximum possible score is higher, not because the underlying risk tolerance is looser. Use whichever table matches the sections you completed in Part B.*

Part D: Mitigation and Action Plan

List the specific actions needed to close the gaps you scored in Part B, starting with the highest-point items.

Action / safeguard	Gap addressed (Part B item)	Owner	Target date	Status

Part E: Sign-Off and Record of Outcomes

Adapted from the ODPC Guidance Note on Data Protection Impact Assessment, Part 5.

Item	Officer name / date	Notes / instructions
Measures approved by		Integrate actions into the project plan with owner and completion date.
Residual risk approved by		If accepting residual High or Critical risk, consult the ODPC before proceeding.
DPO advice provided		DPO should advise on compliance, Part D measures, and whether processing may proceed.
DPO advice accepted or overruled by		If overruled, reasons must be recorded.
Consultation with ODPC (or equivalent authority): response		Mandatory where residual risk is Critical or involves unmitigated children's-data risk.
This assessment will be kept under review by		DPO to review at the interval set in Part C, or on material change.

References

California Consumer Privacy Act of 2018, Cal. Civ. Code section 1798.100 et seq., as amended by the California Privacy Rights Act of 2020.

Children's Act, No. 29 of 2022 (Kenya).

Children's Online Privacy Protection Act, 15 U.S.C. sections 6501 to 6506 (1998).

Constitution of Kenya, 2010.

Data Protection Act, No. 24 of 2019 (Kenya).

Data Protection (General) Regulations, 2021 (Kenya).

Federal Trade Commission. (n.d.). Children's Online Privacy Protection Rule (COPPA). https://www.ftc.gov/business-guidance/privacy-security/childrens-privacy

Information Commissioner's Office. (2020). Age appropriate design code: A code of practice for online services. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/

Information Commissioner's Office. (n.d.). Data protection impact assessments. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-impact-assessments/

Office of the Data Protection Commissioner, Kenya. (2025). Guidance notes for processing children's data. https://www.odpc.go.ke

Office of the Data Protection Commissioner, Kenya. (n.d.-a). Complaints management manual. https://www.odpc.go.ke

Office of the Data Protection Commissioner, Kenya. (n.d.-b). Guidance note on data protection impact assessment. https://www.odpc.go.ke

Protection of Personal Information Act 4 of 2013 (South Africa).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L119, 1 to 88.