

Data Breach Response Checklist

AN INCIDENT READINESS & RESPONSE GUIDE

MUCHANGI PATRICK & ASSOCIATES ADVOCATES
Data Privacy • AI Governance • Digital Regulation

EXECUTIVE SUMMARY

Section 43 of the Data Protection Act, 2019 requires a data controller to notify the Office of the Data Protection Commissioner within seventy-two hours of becoming aware of a breach likely to result in risk to the rights and freedoms of data subjects, and to notify affected data subjects without undue delay in appropriate cases.

This checklist has been prepared by Muchangi Patrick & Associates Advocates to assess an organisation's breach readiness and to guide the practical steps to be taken during detection, containment, assessment, notification and post-incident review.

This checklist is a diagnostic tool, not a substitute for legal advice. Organisations identifying material gaps should seek a full compliance audit before relying on the results for governance or regulatory reporting purposes.

HOW TO USE THIS CHECKLIST

For each of the twenty-four requirements below, the assessor should record one of the following four ratings, supported where necessary by a brief explanatory note:

YES — Fully compliant with the requirement.

PARTIAL — Some compliance, but improvements are required.

NO — Not compliant; the requirement is unmet.

N/A — Not applicable to the organisation's current incident.

BREACH READINESS & RESPONSE ASSESSMENT

N O.	RESPONSE REQUIREMENT	YES	PARTIAL	NO	N/A	NOTES
01	Data breach response plan or policy documented	☐	☐	☐	☐	
02	Incident response team identified with defined roles and responsibilities	☐	☐	☐	☐	
03	Breach detection and monitoring mechanisms in place	☐	☐	☐	☐	
04	Employees know how to report a suspected breach internally	☐	☐	☐	☐	
05	Breach reporting channel and contact clearly communicated	☐	☐	☐	☐	
06	Initial assessment of a suspected breach conducted promptly	☐	☐	☐	☐	
07	Breach contained to prevent further unauthorised access or loss	☐	☐	☐	☐	

N O.	RESPONSE REQUIREMENT	YES	PARTIAL	NO	N/A	NOTES
08	Scope and nature of the breach determined (data, subjects and volume affected)	☐	☐	☐	☐	
09	Risk to the rights and freedoms of affected data subjects assessed	☐	☐	☐	☐	
10	Decision on notification to the ODPC made and documented	☐	☐	☐	☐	
11	ODPC notified within seventy-two hours where required	☐	☐	☐	☐	
12	Affected data subjects notified without undue delay where required	☐	☐	☐	☐	
13	Notification includes the nature of the breach, likely consequences and measures taken	☐	☐	☐	☐	
14	Law enforcement notified where criminal conduct is suspected	☐	☐	☐	☐	
15	Evidence relating to the breach preserved	☐	☐	☐	☐	
16	Root cause of the breach investigated	☐	☐	☐	☐	
17	Remedial and corrective measures implemented	☐	☐	☐	☐	
18	Processors' breach notification obligations to the controller confirmed	☐	☐	☐	☐	
19	Insurance provider notified where cyber insurance is in place	☐	☐	☐	☐	
20	Internal breach register or log maintained	☐	☐	☐	☐	
21	Communications with media and stakeholders managed appropriately	☐	☐	☐	☐	
22	Post-incident review conducted	☐	☐	☐	☐	
23	Breach response plan updated based on lessons learned	☐	☐	☐	☐	
24	Staff retrained following the incident where necessary	☐	☐	☐	☐	

COMPLIANCE SCORE

Aggregate the ratings above to determine the organisation's overall compliance posture:

SCORE	RATING
22 - 24	Excellent
17 - 21	Good
10 - 16	Fair
0 - 9	Immediate Remediation Required

PRIORITY ACTIONS

Corrective actions identified during the assessment should be recorded and tracked to closure below:

PRIORITY	ACTION	RESPONSIBLE OFFICER	TARGET DATE
HIGH			
HIGH			
MEDIUM			
MEDIUM			
LOW			

OVERALL ASSESSMENT

Overall Breach Readiness Rating:

☐ EXCELLENT	☐ GOOD	☐ FAIR	☐ POOR
------------------------------------	-------------------------------	-------------------------------	-------------------------------

AUDITOR'S NOTES

--

FACING A SUSPECTED DATA BREACH?

This checklist provides a high-level readiness and response tool only. For active incidents or breach preparedness reviews, Muchangi Patrick & Associates Advocates offers:

- ✦ Data Protection Compliance Audits
- ✦ Data Protection Impact Assessments (DPIAs)
- ✦ AI Governance Assessments
- ✦ Privacy Programme Development
- ✦ Data Breach Response Advisory
- ✦ Virtual Data Protection Officer (vDPO) Services
- ✦ Executive & Board Training

www.dataprivacyadvocates.co.ke