FREE STARTER PACK

The Ghana Data Protection Act Starter Pack

Everything a data controller needs to comply with the Data Protection Act, 2012 (Act 843): registration with the Data Protection Commission, the eight principles as controls, breach notification, people's rights and ready-to-use templates.

Free, and no email required. Checked against the Act and the Commission's compliance guidelines on 17 November 2026.

WHAT'S INSIDE

From registration to renewal.

Act 843 applies to controllers established in Ghana, to controllers elsewhere using equipment or processors in Ghana, and to processing of information that originates in Ghana (s.45). If that's you, you must register before processing.

1

28 controls

Every duty in sections 17 to 58, with the section reference, expected evidence and ISO 27001 mapping.

2

Registration checklist

What to prepare for the Commission, plus renewal every two years and the 14-day change rule.

3

Templates

A record of processing activities (ROPA) layout and a privacy notice checklist built from section 27.

4

Breach and rights

How and when to notify a breach, and how to handle access, correction, marketing and automated-decision requests.

STEP ONE

Register before you process.

A data controller who has not registered must not process personal data (s.53). Processing

without registration is an offence, with a fine of up to 250 penalty units, up to two years' imprisonment, or both (s.56).

What the Commission asks for

- Certificate of incorporation or business registration
- Entity category (for example limited liability company)
- Address and sector
- Description of the services you provide
- Annual turnover in Ghana cedis
- Average number of people whose data you process, and average annual number of records
- Whether you are part of a group with a large data controller or processor
- Reasons for processing
- Countries outside Ghana where you process data

Deadlines to diarise

- Renew every two years (s.50)
- Report changes to your particulars within 14 days (s.55)
- Separate register entries for each purpose (s.47(3))

Data protection supervisor

The Act lets you appoint a certified supervisor (s.58). The Commission's guidelines say medium and large controllers must appoint one. Small controllers are exempt but are advised to get certified support.

Before you renew: the Commission's guidelines ask controllers to appoint and train a supervisor, run a compliance assessment, fix the gaps, document technical and organisational measures and train staff. Supplying false information on an application is an offence (s.47(2)).

TEMPLATES

Two documents every controller needs.

Record of processing activities:

Privacy notice: what people must

one row per activity

1. Processing activity and business owner
2. Purpose (s.22)
3. Lawful basis (s.20)
4. Categories of people and data
5. Special personal data, if any (s.37)
6. Source of the data (s.21)
7. Recipients, including processors (s.29, s.30)
8. Countries outside Ghana
9. Retention period and disposal method (s.24)
10. Security measures (s.28)
11. Automated decisions, if any (s.41)

be told (s.27(2))

1. What data you collect
2. Your name and address
3. Why you need it
4. Whether giving it is mandatory or optional
5. What happens if they don't give it
6. The law that requires or permits it, if any
7. Who you share it with
8. Their right to access and correct it

Give this before collection. If you collect from a third party, give it before or as soon as practicable after (s.27(3)).

BREACHES

Tell the Commission and the people affected.

When there are reasonable grounds to believe personal data has been accessed or acquired by an unauthorised person, notify the Commission and the people affected as soon as reasonably practicable (s.31). Delay the notice to individuals only if security agencies or the Commission say it would impede a criminal investigation.

1

Restore integrity

Take steps to restore the integrity of the information system (s.31(3)).

2

Choose the channel

Registered mail, email, a prominent notice on your website, the media, or as the Commission directs (s.31(5)).

3

Say enough

Give people enough information to protect themselves, including the identity of the unauthorised person if known (s.31(6), (7)).

Other reports may apply: the same incident may also need a report to your sectoral CERT within 24 hours under the Cybersecurity Act (s.47(5)) and, for financial institutions, to Bank of Ghana under the CISD. See our **Act 1038 Compliance Pack**.

THE CONTROL LIST

28 controls across the Act.

Requirements are paraphrased summaries, not the Act's text. The CSV version adds status, owner and notes columns so you can use it as your compliance assessment.

ID	Section	Requirement	Expected evidence	ISO 27001
REGISTRATION				
DPA-01	s.27(1), s.46(3), s.53	Register with the Data Protection Commission before processing personal data. Processing without registration is prohibited.	DPC registration certificate	A.5.31, A.5.34
DPA-02	s.47(1)	Prepare the registration particulars: business details, the personal data and categories of people, any special personal data, purposes, recipients, countries data may go to, and a description of security measures.	Registration application and supporting records	A.5.31
DPA-03	s.47(3)	Where data is kept for two or more purposes, each purpose gets its own entry in the register.	Register entries by purpose	A.5.31
DPA-04	s.50	Renew the registration every two years.	Renewal date in the compliance calendar; renewal certificate	A.5.31
DPA-05	s.55	Notify the Commission of changes to your registered particulars within 14 days.	Change log and notifications	A.5.31
DPA-06	s.45(2)	A data controller not incorporated in Ghana registers as an external company.	External company registration	A.5.31
SUPERVISOR				
DPA-07	s.58; DPC guidelines	Appoint a certified data protection supervisor where the Commission requires it. The DPC's guidelines say medium and large controllers must appoint one; small controllers are exempt but advised to get certified	Appointment letter; supervisor's DPC certification	Clause 5.3, A.5.2, A.5.34

		support.		
PRINCIPLES				
DPA-08	s.17	Apply the eight principles: accountability, lawful processing, purpose specification, compatible further processing, information quality, openness, security safeguards and data subject participation.	Privacy policy mapped to the eight principles	A.5.34
LAWFUL PROCESSING				
DPA-09	s.18, s.19	Process personal data lawfully and reasonably, without infringing privacy, and only where necessary, relevant and not excessive. For foreign data subjects, also respect the law of their country.	Record of processing activities (ROPA)	A.5.34
DPA-10	s.20(1)	Have prior consent, or another justification: a contract with the person, a legal requirement, the person's legitimate interest, a statutory duty, or your or a third party's legitimate interest.	Lawful basis recorded for each processing activity; consent records	A.5.34
DPA-11	s.20(2), (3)	Stop processing when a person objects, unless the law provides otherwise.	Objection handling procedure and log	A.5.34
COLLECTION				
DPA-12	s.21, s.22	Collect data directly from the person unless an exception applies, and only for a specific, explicitly defined and lawful purpose.	Data sources in the ROPA; documented exceptions	A.5.34
DPA-13	s.23, s.27(2), (3)	Tell people, before collection, what is collected, who is collecting it, the purpose, whether supplying it is mandatory and the consequences of not doing so, the legal basis, the recipients and their access and correction rights.	Privacy notices at each collection point	A.5.34
RETENTION				
DPA-14	s.24	Keep data no longer than necessary unless an exception applies, then destroy, delete or de-identify it so it can't be reconstructed.	Retention schedule; disposal records	A.5.33, A.8.10
FURTHER PROCESSING				

DPA-15	s.25	Keep further processing compatible with the original purpose, or within the Act's exceptions.	Compatibility assessments for new uses	A.5.34
QUALITY				
DPA-16	s.26	Keep data complete, accurate, up to date and not misleading.	Data quality checks	A.5.34
SECURITY				
DPA-17	s.28(1), (2)	Secure personal data with technical and organisational measures: identify foreseeable risks, put safeguards in place, check they work and update them as risks change.	Risk assessment covering personal data; safeguard testing	Clauses 6.1, 8.2, A.5.34
DPA-18	s.28(3)	Follow generally accepted information security practice and your industry's own rules.	ISO 27001 or equivalent control set; sector rules mapped	Clauses 4 to 10
PROCESSORS				
DPA-19	s.29, s.30(1) to (3)	Use processors only under a written contract that requires confidentiality and security. Processors act only with your authorisation.	Signed processor contracts	A.5.19, A.5.20
DPA-20	s.30(4)	Where a processor is not based in Ghana, make sure it complies with Ghana's laws.	Contract clauses and checks for foreign processors	A.5.20, A.5.23
BREACHES				
DPA-21	s.31(1), (2)	Where personal data has been accessed or acquired by an unauthorised person, notify the Commission and the people affected as soon as reasonably practicable.	Breach procedure; notification records	A.5.24 to A.5.26
DPA-22	s.31(5) to (7)	Notify people by registered mail, email, a prominent website notice, the media or as the Commission directs, with enough detail for them to protect themselves.	Notice templates by channel	A.5.26
RIGHTS				
DPA-23	s.32, s.35	Answer access requests: confirm whether you hold data, describe it, its purposes, recipients and source, and explain the logic of solely automated decisions.	Request log; response templates	A.5.34

DPA-24	s.33	Correct or delete inaccurate, excessive or unlawfully held data on request, or give evidence supporting it. Tell recipients about corrections.	Correction log	A.5.34
DPA-25	s.37	Process special personal data (children, religion, ethnicity, health, sexual life, political opinion, criminal behaviour and others) only where necessary or with consent.	Special data inventory and justifications	A.5.34
DPA-26	s.40	Get prior written consent for direct marketing, and stop when told to.	Marketing consent records; suppression list	A.5.34
DPA-27	s.41	On written notice, ensure significant decisions are not based solely on automated processing. Where they are, tell the person, who can ask for reconsideration within 21 days.	Automated decision register; reconsideration procedure	A.5.34
ACCOUNTABILITY				
DPA-28	DPC guidelines	Run a data protection compliance assessment, score the gaps by risk and keep an action plan. Train management and staff.	Assessment report; action plan; training records	Clauses 9.2, 10.2, A.6.3

This pack summarises the Data Protection Act, 2012 (Act 843) and the Data Protection Commission's guidelines to help you plan. It is not legal advice. Check the Act and the **Data Protection Commission**'s current guidance and fees for exact requirements. The Commission advises controllers to seek support from institutions and experts it has accredited. Last reviewed 17 November 2026.

Need help putting this into practice? Assurelo runs gap assessments, readiness programmes and internal audits. Email hello@assurelo.com or visit assurelo.com to book a free 30-minute call.