Key contacts

Dorothy Mensah
Partner,
Corporate & Commercial
dorothy.mensah@templars-law.com

Aasiya Sarku Nettey
Senior Associate,
Corporate & Commercial
aasiya.nettey@templars-law.com

Kezia Owusu-Ansah
Principal Associate
Corporate & Commercial
kezia.owusuansah@templars-law.com

Data Protection Compliance in Ghana: Navigating the Regulatory Framework and Emerging Compliance Requirements

Introduction

Today's digital world has made data privacy a crucial concern for businesses all over the world which now have a heightened need to safeguard the privacy of their client and employee data. Like many other nations, Ghana has established a legal framework to regulate the collection, processing, and storage of personal data originating in Ghana to protect the data privacy of individuals. This article will examine Ghana's legal framework for data privacy and how organizations can put practical measures in place to ensure continuing compliance with the applicable data protection law.

Legal Framework of Data Protection in Ghana

The primary legislation governing data protection in Ghana is the Data Protection Act, 2012 (Act 843) (**DPA**) and the Data Protection Commission (**DPC**) is the body tasked by the law to enforce data protection laws. The law controls how personal data is collected, retained and processed and aims to ensure the application of the eight key data protection principles of accountability, lawfulness of processing, specification of purpose, compatibility of further processing with purpose of collection, quality of information, openness, data security safeguards and data subject participation.

Overall, the DPA seeks to strike a balance between the need of businesses to process personal data for legitimate purposes and the protection of the privacy of individuals and therefore provides a comprehensive framework for the regulation of personal data processing and the protection of personal data in Ghana. The key highlights of the Act include the following:

i. Personal data protection

The act defines personal data broadly to include any information which, on its own or in conjunction with other information, makes individuals identifiable such as names, addresses, identification numbers, and biometric data. The law requires data controllers to collect personal data directly from data subjects for specific purposes which are explicitly defined except in limited circumstances where data may be indirectly obtained. Data controllers are further required to process personal

data in a manner that ensures appropriate security and protection against unauthorized access, alteration, disclosure, or destruction. Data controllers must therefore take appropriate technical and organizational measures to ensure the security of personal data, such as encrypting data, restricting access, and implementing access control.

ii. Data controllers and processors

The DPA distinguishes between data controllers and data processors and sets out differing levels of obligations for each party. A data controller is defined under the law as the entity which determines the purposes and the manner in which personal data is processed, while a data processor is any person or entity who processes personal data on behalf of a data controller. The differing levels of compliance prescribed for data controllers and data processors under the DPA makes it necessary for companies to clearly set out the roles of their independent contractors and service providers in respect of processing data shared under an outsourcing or service agreement.

iii. Data subject rights

A key aspect of the data subject rights under the DPA is the requirement for data controllers to obtain the freely given, specific, informed, and unambiguous consent of data subjects before processing their personal data. Such consent must be obtained prior to the collection and processing of personal data, and data subjects must be informed of the purposes for which their data will be processed. In addition to the required consent of data subjects, the Act recognizes the rights of data subjects to access their personal data, request correction or deletion of their personal data, object to the processing of their personal data, and withdraw consent to the processing of their personal data. An individual may exercise their right to access their personal data by submitting a written request to the data controller and the data controller must subsequently provide the requested information within 21 days unless there are legitimate grounds for a longer response time.

iv. Data breaches

Under the law, data controllers must report all data breaches or security comprises to the DPC and to affected data subjects as soon as reasonably practicable upon becoming aware of the breach. Although, there are no express timelines under Ghanaian law for such breach notifications, some companies apply a timeline of 72 hours in their data protection policies for conformity with most international data protection frameworks including the General Data Protection Regulation. The notification to data subjects must contain sufficient information to allow them take protective measures and must include the nature of the breach, the measures taken to address the breach, and the likely consequences of the breach.

v. Cross-border data transfers

The law permits cross-border transfers of personal data, such as the transfer of personal data of employees or customers in Ghana to a data centre or server located in another country. In such an instance, the data controller must obtain the consent of data subjects and must also ensure that appropriate safeguards are in place to protect the personal data during the transfer.

vi. Enforcement:

The DPA provides penalties and sanctions for breaches of its provisions. The DPC is authorised to issue enforcement notices to non-compliant data controllers who may be liable to a fine up to GHS1,500 (approximately US$150) or a term of imprisonment of one year (to be served by directors in the case of non-compliant companies) for failure to comply with a notice. Non-complaint

companies and individuals may also be liable upon summary conviction to fines under the Act including the general liability of up to GHS60,000 (approximately US$5,000). The DPC can also cancel the registration of data controllers for non-compliance and request other regulators to also suspend or revoke licences of regulated entities if they breach the provisions of the Act. Data subjects whose rights have been infringed by a breach of the DPA are also entitled to claim compensation for any resulting damages.

It's worth noting that even though the enforcement of sanctions under the DPA is still evolving, the DPC has recently demonstrated its intention to enforce the law, through its liaison with the Attorney General to appoint a dedicated prosecutor for DPC cases as well as its engagements with the Chief Justice to establish a Fasttrack Court for non-compliance suits.

The Applicability of the General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a comprehensive data protection regulation that was implemented by the European Union (EU) in 2018. While the GDPR is a regulation of the EU, its impact extends far beyond the borders of the EU, and it has had a significant influence on data protection laws around the world, including in Ghana.

Although Ghana's data protection laws were enacted before the GDPR, the DPA mirrors the key definitions for personal data, special categories of personal data, data controllers, and data processors as well as the overarching data protection principles in the GDPR. Thus, multinational organizations operating in Ghana with data protection policies based on the GDPR are very likely to comply with the DPA and may not need to alter their organizational policies or take additional actions in order to meet the requirements of the DPA.

Best Practice for Data Protection Compliance in Ghana

To ensure compliance with Ghana's data protection regulations, organizations in Ghana should consider implementing the following best practices:

i. **Registration and Renewal as Data Controllers with the DPC**

Organizations which are classified as data controllers under the DPA must register with the DPC and renew their registration every 2 years to ensure compliance. For the purpose of registration, data controllers are classified by the DPC into large, medium and small data controllers, depending on their annual turnover and number of staff and/ or customers.[1] Foreign companies which are not incorporated in Ghana but are (a) collecting and processing personal data originating from Ghana or (b) using equipment or data processors in Ghana to process data, are required under the DPA to register an external company (also known as a branch, representative office or liaison office) with the Office of the Registrar of Companies and register as data controllers with the DPC.[2] In practice however, the DPC does not insist on the requirement to register as an external company due to the impracticality of enforcement and may allow such foreign companies to register as data controllers upon fulfilling specified conditions.

ii. **Data protection impact assessments (DPIAs)**:

If an organization's data processing activities are likely to result in a high risk to individuals' privacy, the company may conduct a DPIA to assess the impact of the processing on individuals' privacy rights. A DPIA is a risk assessment tool that helps companies identify and mitigate potential data protection risks. By

[1] Upstream and Midstream Petroleum companies, telecommunications companies or operators, banking and financial institutions, credit bureaus, insurance companies and mining companies are classified as large data processors notwithstanding their annual turnover or number of staff.
[2] Section 45 of the Data Protection Act

conducting a DPIA for their operations and projects, companies can identify areas where they may be at risk of non-compliance and take steps to address these risks.

iii. **Cross-border data transfers:**
Organizations which intend to undertake cross-border data transfers must put in place safeguards to ensure that personal data is adequately protected. These include;

Adequacy decisions: One way to ensure that data is protected is by transferring it to a country that has adequate data protection laws comparable to Ghana. If the country is deemed adequate, the transfer can be made without any additional safeguards.

Standard Contractual Clauses: If the transfer is to a country that is not deemed adequate, standard clauses can be included in outsourcing or other relevant contracts to ensure that personal data is adequately protected in the course of the data transfer.

Binding Corporate Rules (BCRs): BCRs are internal rules that apply to a group of companies, which define the standards and procedures for the transfer of personal data within the group. BCRs are subject to approval by the relevant data protection authorities.

Codes of Conduct: Codes of conduct are sets of rules that organizations can voluntarily adhere to, to demonstrate compliance with the DPA.

iv. **Develop data protection policies and procedures:**

Organisations should develop clear policies and procedures for the collection, processing, and storage of personal data, and ensure that all employees are trained on these policies. Such policies and procedures must include the process of obtaining explicit consent from individuals before collecting, processing, or storing their personal data, and providing clear and transparent information about how their data will be used.

v. **Implement appropriate security measures:**

Organizations should implement appropriate technical and organizational measures to protect personal data, such as encryption, access controls, and regular backups. These security measures will alert an organization if a data breach occurs, and thus enable it take remedial measures. In addition, the organization must ensure that its independent contractors and service providers who will serve as data processors have comparable security measures or implement adequate safeguards specifically as relates to personal data received from the organization.

vi. **Regularly review and update data protection practices:**

Companies should regularly review and update their data protection practices to ensure that they remain compliant with the latest regulations and best practices.

Emerging Compliance Requirements in Ghana

A key requirement for the compliance of organizations with the data protection framework in Ghana has, in recent times, been the appointment of a certified data supervisor or data protection officer. Although the appointment of a data supervisor is not mandated under the DPA, the DPC currently, refuses to register or renew the registration of companies and organisations who have not appointed certified data supervisors. The appointed data supervisor must be trained and certified by data protection institutions accredited by the DPC to qualify for appointment.

The data supervisor may be an employee within the organisation or external persons designated with the responsibility for ensuring the organizations compliance with the DPA.[3] The data supervisor may ensure compliance by:

(i) providing guidance and advice on data protection matters to the organisation and its employees;

(ii) ensuring that the organisation complies with the data protection principles set out in the law, including obtaining the necessary consent from individuals before collecting and processing their personal data;

(iii) ensuring that the organisation has appropriate data protection policies and procedures in place, and that they are adhered to;

(iv) conducting regular audits and risk assessments of the organisation's data processing activities to identify and address any potential breaches of the Act;

(v) handling complaints from data subjects who believe their data privacy has been violated by the organisation, and

(vi) acting as the point of contact between the organisation and the DPC and cooperating with the DPC in the event of an investigation or audit.

Conclusion

Data protection compliance is an important consideration for organizations operating in Ghana. By understanding Ghana's data protection laws and implementing best practices for compliance, companies can protect personal data, minimize the risk of non-compliance, and ensure the long-term success of their business operations in Ghana.

[3] Section 58(5) of the Data Protection Act