Privacy Law Developments Commonwealth of The Bahamas 2026

Brief Overview

- The Data Protection (Privacy of Personal Information) Act, was passed into law in April 2003. It came into force on April 2, 2007.
- It sets the legal framework for the collection, use and disclosure of personal information consistent with internationally recognized principles established by the Council of Europe, The European Union (EU), the OECD and the United Nations – driven by the 1998 directive.

5 most significant Data Breaches between 2024 - 2025

- National Public Data Breach (exposed approx. 2.9B individuals involving sensitive data)
- Discord Data Breach (affected millions stemming from a third party processor being compromised)
- Lexis Nexis Risk Solutions (exposed the personal data of over 300K data subjects)
- Library of Congress (countless individuals were affected leading to unauthorized access and office emails)
- Quantas Data Leak (bad actors gained access and leaked millions of customer records which the actual amount to date is still undetermined)

These beaches involve both the private and public sector reflecting widespread vulnerabilities.

Public Sector Journey to transform services digitally

- Boosting Efficiency and streamlining processes throughout ministries and agencies
- Reducing frustration on the part of its citizens and residents
- Improving transparency and accountability
- Enabling data driven decisions
- Reducing costs and optimizing resources

Examples of Breach at Each Stage

- **Collection** – Artist Arena an operator of fan websites for musicians settled for $1Million in civil penalties for improperly collecting personal information from children under 13.
- **Use** – A few years ago, the Spanish Data Protection Agency ordered Google to pay 900Mil Euros for illegally collecting and using personal data without advising how data was intended to be used.
- **Disclosure** – Wellpoint Inc. paid $1.7million after it was discovered that a software upgrade changed the system's authentication mechanism resulting in unauthorized personal data of +600 thousand health information be leaked.

Examples of Breach at Each Stage Continued

- **Retention** – Financial Services Authority in Switzerland charged Zurich Insurance in excess of 2.2million pounds for having insufficient systems and controls in place after an unencrypted backup tape, containing personal details of 46,000 policy holders went missing during a "routine" transfer to a third party storage facility.
- **Destruction** – Less than 3 years ago, the Brighton and Sussex University Hospital Trust was fined 325,000 pounds after hard drives containing large amounts of patient and staff personal data (ie. HIV patients, criminal convictions) were found for sale on Ebay.
- And by now…..we all know of Social Media nightmares involving billions……

Data Protection Roles

- Data Protection Authority – Supervisory entity chartered to enforce privacy or data protection laws and regulations both public and private sectors
- Data Controller – An organization or individual with the authority to decide how and why information about data subjects is to be processed
- Data Processor – An organization or individual that processes data on behalf of the data controller
- Data Subject – An individual about whom information is being processed

Data Protection Jurisdiction Matters

- Data governance within various jurisdictions involving data sovereignty is becoming an increasingly important issue for global enterprises using cloud services, as data protection laws of their service provider jurisdiction govern the protection and access to data;
- Data Sovereignty too which is off significant interest to our foreign missions; and
- Third Party Adequacy Considerations and Agreement – this ongoing designation is driven by the EU and deemed significant.

Reasons for Implementing Data Protection Laws

- To prevent misuse exploitation of personal data
- To uphold individual freedoms and protect against discrimination based on personal information
- To address the challenges posed by modern data-driven models that collect or somehow use personal information
- To create legal frameworks that require organizations to have a valid basis for processing personal information
- To protect civil liberties by restricting unwarranted access to private information by governments, while safeguarding those among us whom we may deem most vulnerable

Key Challenges Facing DPAs in the region

- Passing Laws which results in harmonization/international standards vs. local expectations
- Establishing an authority to ensure sustainability and perceived independence
- Resources involving resident expertise and reliable research activity
- Compliance and enforcement – lack of case laws, technological challenges and harmonization across industries

Regulators must remain Relevant and Establish Cooperative Approaches

- Adaptable to change
- Ready to act
- Innovative and Strategic
- Business advocate (Economic Model Matters)
- Remain aware of technological advancements
- Broad based understanding of interrelated industries
- Understanding and practical
- Execute MOUs and/or working arrangements with Cyber Crime Unit, Financial Intelligence Unit, Industry Experts, Prosecutors and Civil Society
- Cooperation with Central Banks and other top tier Institutions

Research – inclusive of historical, scientific and statistical purposes

Processing of personal data for research purposes.

Relevant conditions in relation to processing of personal data, means that the conditions that the personal data

1. Is not processed to support measures or decisions with respect to particular identifiable natural persons; and
2. Is not processed in a way that substantial damage or substantial distress is, or is likely to be, caused to a data subject.

Existing Act – Area of non-alignment with GDPR	Draft Data Protection Act (2025)
Definitions	
▪ Ethnic origin and sexual orientation are not included in the definition of "sensitive personal data". ▪ Physical or mental health is included in sensitive personal data but excludes employee's health data kept in the	▪ The definition of "sensitive personal data" includes 'ethnic origin' and 'sexual orientation'. ▪ The exclusion regarding physical or mental health in the definition of 'sensitive personal data' was removed

Existing Act – Area of non-alignment with GDPR	Draft Data Protection Act (2025)
Data Protection Principles	
▪ These are outlined briefly in section 6, however, there is no need for back up data to be kept accurate and there is no principle of accountability, i.e., data controllers are not required to demonstrate compliance with principles	▪ Draft Bill includes a Part devoted to the data protection principles. Personal data is required to be processed according to the principles of lawfulness; fairness; transparency; and accuracy. Personal data must also be processed in a manner to ensure appropriate security of the data and must not be kept for a period of time longer than necessary for the purpose kept. ▪ Provision is included to require data controllers to take appropriate measures to comply with the principles and are required to demonstrate compliance with the principles upon request by the Commissioner.

Existing Act – Area of non-alignment with GDPR	Draft Data Protection Act (2025)
Consent	
▪ No definition is provided for consent and there is no provision regarding consent. ▪ There are no special provisions regarding obtaining consent from children.	▪ Concerning 'consent', the following definition is included in the draft Bill: "consent" in relation to a data subject, means any freely given, specific, informed and unambiguous indication of the data subject's wishes, by which the data subject, in a written statement or by clear affirmative action, confirms his agreement to the processing of his personal data ▪ Special provision is provided for obtaining consent from a child, namely, a child's personal data shall not be processed unless consent is given by the parent or guardian of the child and onus is placed on the data controller to make reasonable efforts to verify that consent is given by the parent or guardian.

Existing Act – Area of non-alignment with GDPR	Draft Data Protection Act (2025)
Obligations of data controllers and data processors	
▪ There is no provision requiring controllers or processors to maintain a record of processing activities. ▪ There is no provision allowing controllers and processors to verify and demonstrate compliance with their obligations.	▪ Provision is included for the processing of personal data to be governed by a contract between the controller and processor. ▪ The data controller and data processor are required to register with the Commissioner and maintain data processing records. ▪ Data controller is required to carry out an assessment of the impact of processing on the protection of personal data in certain instances, such as where the processing uses new technologies. ▪ Data controllers are required to only use data processors who provide sufficient guarantees to implement appropriate security measures.

Existing Act – Area of non-alignment with GDPR	Draft Data Protection Act (2025)
Data breaches	
▪ There is no duty to report or record personal data breaches to the Commissioner or affected data subjects, even where the breach is likely to result in a high risk to their rights and freedoms	▪ Provision is included that requires the data controller to notify the Commissioner within seventy-two hours after having become aware of a personal data breach that is likely to result in a risk to the rights and freedoms of an individual. ▪ Additionally, the data controller is required to communicate personal data breaches to the data subject not later than seventy-two hours after having become aware of it, and that breach is likely to result in a high risk to the rights and freedoms of individuals.

Existing Act – Area of non-alignment with GDPR	Draft Data Protection Act (2025)
Remedies	
▪ There is no time period for which the Commissioner must inform a complainant of the outcome of a complaint. ▪ There is no right to an effective judicial remedy or to compensation for data subjects who have suffered material or non-material damage. ▪ There is no provision for administrative penalties nor provision for factors to be considered to guide the imposition of such penalties.	▪ Provision is included for the Commissioner to receive complaints and investigate them. The Commissioner is also required to keep the data subject informed concerning the progress of the investigation and of the outcome. ▪ Provision is also included for the Commissioner to levy administrative penalties in particular cases and provides for the factors to be considered when levying such penalties. ▪ Data subjects have the right to appeal decisions of the Commissioner to the Appeal Tribunal established under the Bill. ▪ Provision is included for data subjects to have the right to compensation for damage suffered from an infringement of their rights under the Bill.

What can I do to close the gap on my own personal information being exposed?

- Determine where my PI exists
- Understand the attitude or culture of the location
- Make reasonable inquiries as to its safety
- Remain aware of any and all announcements or reports involving data breaches
- Become more vigilant as to safeguarding my PI
- Ensure that both work environment and private interactions have responsible oversight of my PI
- Insist that each custodian or fiduciary relationship in possession of my PI either is a “trusted source” or becomes one

Thank You for your Kind Attention!

Mr. Michael Wright
Data Protection Commissioner

Tel: 242-604-1001

P.O. Box N-3017

Email: dataprotection@bahamas.gov.bs

www.bahamas.gov.bs/dataprotection

Instagram:dataprotection_242