
Welcome

Data Protection Masterclass

Monique N. Morrison, MA, LLB, LEC

876-487-5619

9th Floor, PanJam Building, 60 Knutsford Blvd (5) Jamaica

morrisonlawjamaica@gmail.com

Social: Morrison Law Jamaica

Disclaimer

The information provided is for general informational purposes only and should not be relied upon as legal advice. If you have specific legal questions or concerns, please consult with a licensed attorney. Additionally, any information provided may be subject to updates and omissions, and no guarantees are being made as to its accuracy or completeness.

Use of any information provided is at your own risk, and I disclaim any liability for any damages that may arise from your reliance on any information provided.

WHEN DATA MEETS DISASTER

"ALIGNING DATA PROTECTION AND RISK MANAGEMENT"

MONIQUE MORRISON LAW


WE
HAVE
RIGHTS

Rights of the Data Subject

Right to Access

Right to be Informed

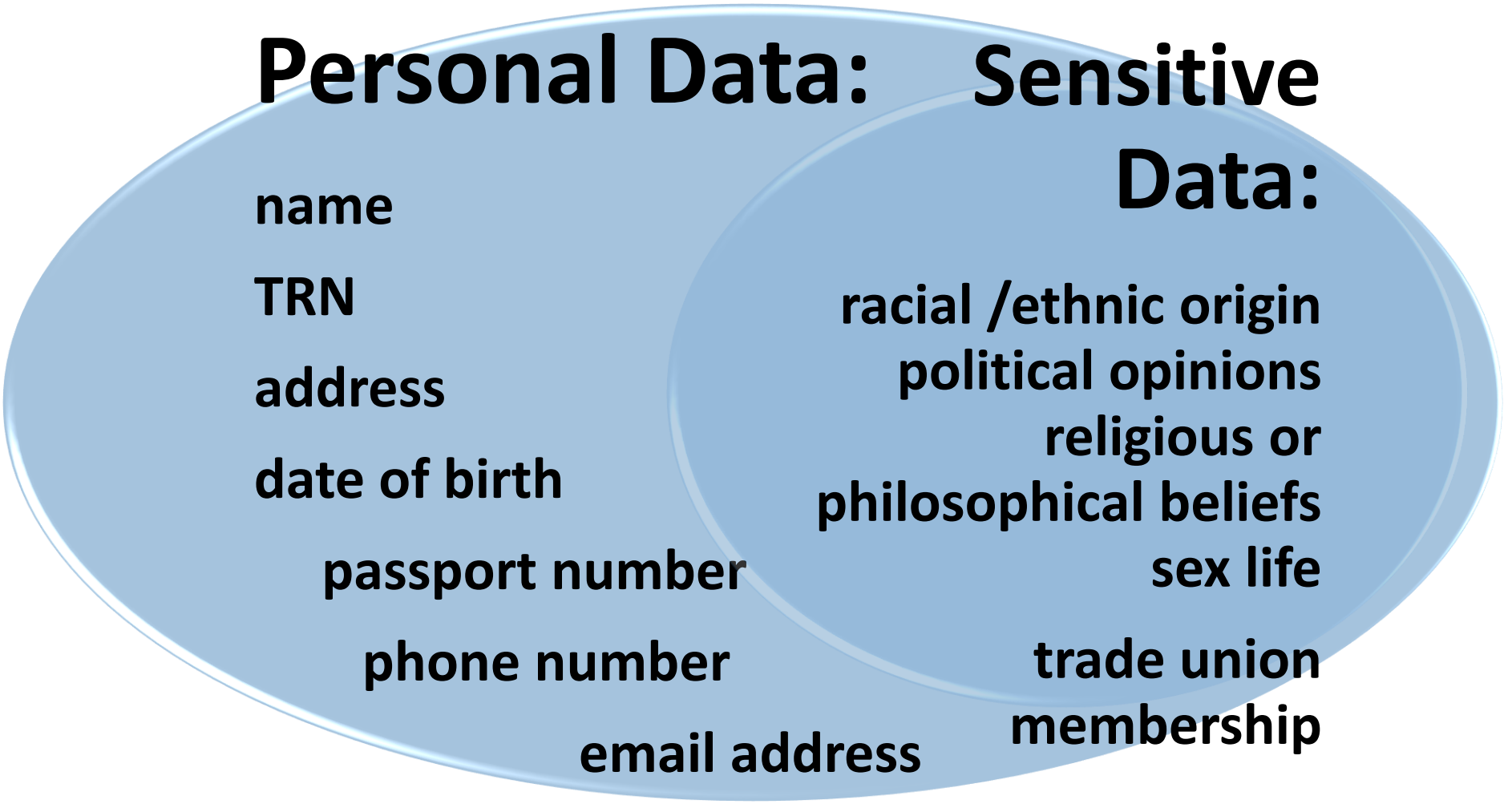
Right to Prevent Processing

Right to Rectification

Rights Related to Automated Decision-Making

Right to Data Portability

Right to Object to Direct Marketing


Personal Data:
name
TRN
address
date of birth
passport number
phone number
email address
Sensitive Data:
racial /ethnic origin
political opinions
religious or philosophical beliefs
sex life
trade union membership

Sensitive Data includes:

Data concerning health (and wellness?)	
RECORDS OF	• illnesses, disabilities, injuries, mental health disorders, disease risk , medical history, family medical history • ALSO: appointments, consultations, and treatments and registration for health services
RECORDS FROM	• doctors, hospitals, labs and other healthcare providers
DATA ON	• alcohol consumption, diet, and exercise levels
INFO FROM Smart Devices	• heart rate, sleep patterns, activity levels, and calorie intake
REPORTS	• Labs :X-rays, MRI scans,
INFO ON	• Causes of death
GROUP DATA	• Studies and statistics on public health, disease prevalence, and health outcomes

Sensitive Data includes:

Biometric Data
Facial images used for recognition
Fingerprints
Iris Scans
Retina Scans
Hand geometry
Gait analysis
Keystroke dynamics
Signature dynamics
Voice scans

Registration Opens Dec. 1 each year



Office of the Information Commissioner

The DPA provides for the establishment of a Data Protection Commission to:

- oversee compliance with the Act
- **investigate complaints** related to data protection.

Data Protection as a Pillar of Risk Management in a Pre- and Post-Hurricane World

Executive Context

- Data is both a strategic asset and a significant liability
- Jamaica's Data Protection Act (2020) reframes data protection as enterprise risk
- Climate-driven disasters amplify data protection failures
- GDPR provides a mature, risk-based benchmark

Why Data Protection Is Risk Management

- Regulatory non-compliance creates financial and legal exposure
- Data breaches damage trust and reputation
- Operational disruption increases likelihood of failure
- Accountability principles require proactive risk controls

Legal Foundations

- Jamaica Data Protection Act, 2020
- Security safeguards and accountability obligations
- Mandatory breach notification
- GDPR alignment: risk-based, proportional safeguards

Personal Data as a Risk Multiplier

- High value to cybercriminals
- Emotionally sensitive to individuals
- Triggers regulatory scrutiny
- Amplifies reputational harm during crises

The Risk-Based Approach

Assess likelihood and severity of harm

Apply safeguards proportional to risk

Document decisions and controls

Demonstrate accountability at all times

Pre-Hurricane World

- Stable infrastructure and predictable operations
- Centralized IT systems
- Routine compliance activities
- Hidden and underestimated vulnerabilities

Pre-Hurricane Data Protection Risks

- Incomplete data mapping
- Inadequate backups and testing
- Weak vendor oversight
- BCPs that ignore data protection realities

DPIAs and Disaster Preparedness

- Foreseeable risks must be assessed
- Hurricanes are predictable Caribbean risks
- Emergency access and manual processing must be planned
- Best practice even where not explicitly mandated

Business Continuity and Data Protection

- BCPs often focus only on system restoration
- Data protection obligations continue during crises
- Lawful processing and access controls still apply
- Misalignment creates major risk exposure

Post-Hurricane Reality

- Power and connectivity disruptions
- Manual and improvised processes
- Staff displacement and stress
- Heavy reliance on third parties

Elevated Post-Hurricane Data Protection Risks

- Loss or theft of physical records
- Use of personal devices and insecure channels
- Unlogged emergency access
- Increased fraud and phishing attacks

Data Breaches in a Disaster Context

- Emergency conditions do not suspend legal duties
- Breach notification remains mandatory
- Preparedness reduces regulatory penalties
- Documentation is critical

Trust and Reputation Risk

- Customers and citizens are vulnerable post-disaster
- Data failures feel exploitative
- Reputational harm may exceed fines
- Transparency preserves trust

Strategic Lessons from GDPR

- Accountability is continuous
- Risk multiplies in emergencies
- Preparedness mitigates penalties
- Resilience depends on data governance maturity

Key Recommendations: Pre-Hurricane

- Embed data protection into enterprise risk management
- Conduct disaster-focused data mapping
- Encrypt and geographically diversify backups
- Update BCPs with data protection scenarios

Key Recommendations: Pre-Hurricane (Continued)

Train

- Train staff on crisis data handling

Clarify

- Clarify emergency access procedures

Assess

- Assess vendor disaster resilience

Document

- Document decision-making processes

Key Recommendations: Post-Hurricane

01

Activate breach and incident response teams

02

Apply proportional safeguards

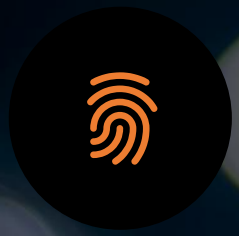
03

Assess and notify breaches promptly

04

Communicate transparently with stakeholders

Post-Incident Review and Improvement



CONDUCT LESSONS-LEARNED ASSESSMENTS

UPDATE POLICIES AND CONTROLS

STRENGTHEN RESILIENCE GAPS

PREPARE FOR THE NEXT EVENT

Final Consultant Insight

- Data protection is not a compliance cost
- It is a resilience and trust investment
- Alignment with risk management ensures continuity
- Prepared organizations emerge stronger

MONIQUE MORRISON LAW

This Act is currently in force.

Data Controllers are encouraged to open an account with the Office of the Information Commissioner (OIC) at https://oic.gov.jm/




Compliance

Penalties for failure to comply are both Civil and Criminal.

They include:

Failure to comply with the requirements under the Act can result in a company being liable to **fine not exceeding ten million dollars or 4% of its annual gross worldwide income.**

Failure to comply with the requirements under the **Act can result in imprisonment for a period of up to 10 years**.

Keep your profits!

Thank You!

Thank You

MONIQUE MORRISON LAW
ATTORNEY AT LAW

Monique Morrison
Attorney-at-Law

876-487-5619

9th Floor, PanJam Building, 60 Knutsford Blvd Kgn. 5 Jamaica

morrisonlawjamaica@gmail.com

Facebook: Morrison Law Jamaica

Instagram: Morrison Law Jamaica