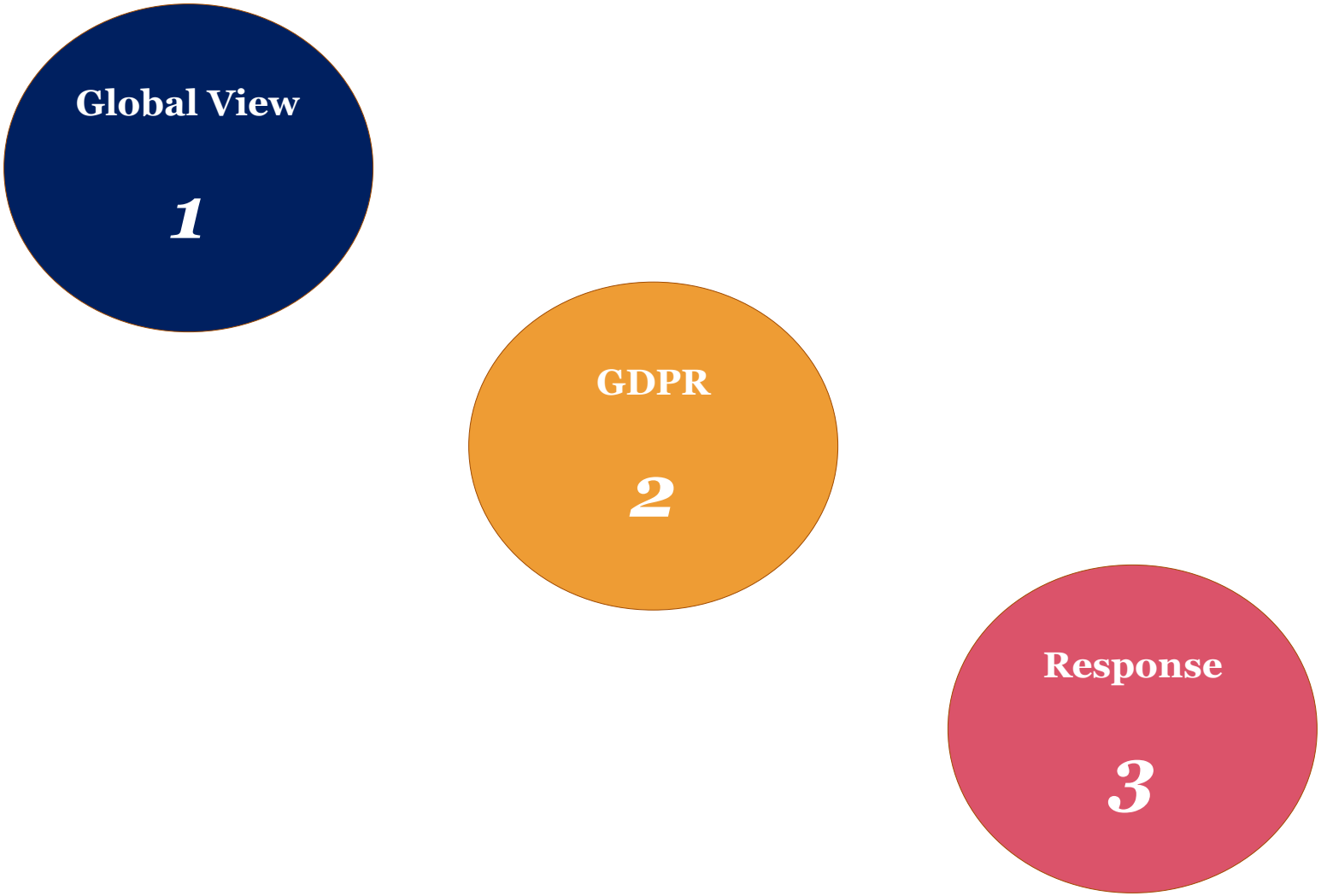
Caribbean Telecommunications Union

EU General Data Protection Regulation (GDPR)

May 2018

Contents



Global View

Privacy & Security Regulation is Global

USA: *~ National breach notification*

CISA breach data sharing (2015)

Sector & State privacy regulation

EU: GDPR (2018)
NISD (2018)

India: IT Rules for Security & Sensitive Data (2011)

Japan: National APPI (2017) based. Similar to GDPR

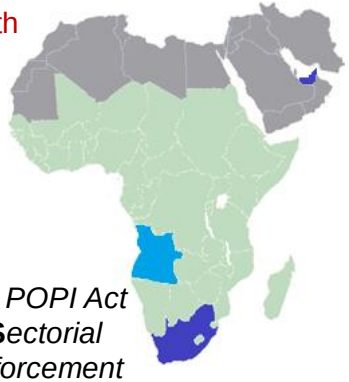
Singapore: Full PDPA passed. (2013). Same essentially as GDPR

Uruguay: EU equivalent national privacy law (2009). Extensive notifications.

Brazil: Extensive sectorial framework (1990) National law in proposed (NA)

Argentina: EU equivalent national law with active DPA (2000)

MEA: Several markets with regulations



South Africa: *POPI Act (2013)* **UAE:** **S***ectorial with active enforcement actions*

Australia: EU equivalent federal Privacy Act & State laws (1988). Updated law enforced (2014)

The importance of a robust compliance program

CTU is Accountable

- To members/regulators in all markets served
- To colleagues, partners and customers that are sensitive to data privacy and share personal data with you

The business landscape is evolving and uses more and more personal data

Organizations need a global data privacy response

- Personal data is regulated on a local, national and international level in many countries and may require different protection depending on the location or type of data:
  - Individual state Privacy and communication regulations in the US require special handling of a resident and customer data incl. ID Numbers, contacts, financial details and treatment details;
  - The US Federal health & communications regulation also covers individual records as well as electronic communications and marketing information; and
  - Various EU, Canadian and other emerging markets regulations cover the above as well as additional items such as employment and educational history and political or religious views

Data Privacy Terms

Personal Information ("Personal Data" or "PI") is information that can be used to uniquely identify, contact, or locate an individual or can be combined with other sources to uniquely identify a single individual

Personal Data Processing means any operation performed on personal data, whether or not by automatic means, such as collection, recording, storage, transmission, dissemination or otherwise making available, blocking or erasure

Right of Access/ Subject Access Request is the right of an individual to request access to or copies of any and all personal information an entity may have about them, *subject to some exceptions*

Data Controllers are the entities that alone or jointly with others determines the purposes and means of the processing of personal data; while **Data Processors** are separate entities that process personal data on behalf of and as instructed by Controllers

Data Breach ("Security Breach") is unauthorized acquisition, access, use, disclosure, modification or destruction of Personal Information which may reasonably compromise the security or privacy of Personal Information

Data Subject usually the living person to which personal data pertains and can be Consumers, Customers, Employees or Suppliers

Opt-in/ Opt-out is a statement to the data subject on how their data will be used requesting active agreement (opt-in) (e.g. signature/ check a box) or passive agreement (opt-out) to such use (e.g. uncheck a pre-checked box)

It's about the Personal Data

- Personal data as any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly…[by or through combination of certain data]
- A data set need not include the name of an individual to be covered data. A combination of certain data may allow an individual to become identifiable

- National or Tax ID Number
- License /State ID No.
- Financial Account/ Policy No.
- Contact data (incl. email)
- Family/ Dependents
- Criminal history
- Compensation data
- Performance data
- ***Location data***

- ***Online identifiers*** (e.g. IP address)
- Employment history
- ***Biometric/ Genetic data***
- Physical/ mental health
- Racial or ethnic origin
- Religion/ philosophy
- Sexual orientation
- Political orientation
- Trade-union membership

Special Categories ("Sensitive") personal data

GDPR additions to the original Directive

Where could we find it?

- Employee Applications, Onboarding & payroll
- Vendor Contracts & Background Checks
- Marketing Databases/ CRM
- Customer account enrollment & analytics data
- Consumer enrollment & education services data

Data Processing Principles

Lawful Basis – Sometimes Enterprise is required to process PI; Other times it's optional

- ✓ We **NOTIFY** data subjects in instances of **Mandatory** data processing or it's in our **Legitimate Interests** and we gather **CONSENT** for **where necessary**

Data Limitation – only collect the minimum data necessary for our legitimate purposes

- ✓ Critical to apply data classification procedures for easier data identification and tracking across Enterprise and over time

Data Security – is how we protect our PI technically and administratively

- ✓ Data Security evolves constantly and is not "set it and forget it". Enterprise IT Security and operations teams must monitor changes in security risk for new ways to protect PI

Transparency & Access – All communications (e.g. email/ websites, individual contracts) must include: (i) what data is collected; (ii) how/why it is used; (iii) who and where it will be accessed; (iv) how to contact us about changes or to opt-out of processing

- ✓ Enterprise IT & Affiliates collaborate to update online notices, marketing messages & enrollment forms

Data Transfer – is subject to the consent of the individual or "adequate protection" where personal data is to be sent

- ✓ Adequacy protection includes (i) local law; (ii) Data Transfer Agreements (DTA) or Binding Corporate Rules; (iii) government guarantee (e.g. Privacy Shield);

EU General Data Protection Regulation (GDPR)

2

GDPR Scope

Numerous changes to the existing privacy landscape in the EU, along with new concepts (e.g. *RtbF; PbD)*

Increased administrative and compliance obligations for those entities operating in or processing any data from country of origin. The following are the top changes and modifications the GDPR makes to the Data Protection Directive (DPD).

Jurisdiction	• GDPR covers entities established in the EU and those offering goods/ services in EU. ***Extraterritoriality*** • **Does not** apply to Citizenship
Personal & Sensitive Data	• Personal Data includes location, online identifiers; • Sensitive Data expands to ***genetic*** and ***biometric*** data • Introduction of "pseudonymized" and SAR's
Governance & Accountability	• Must appoint a Data Protection Officer; • Embed privacy by design (PbD); • Conduct PIA's for high risk/large scale processing
Consent	• New restrictions on consents and child data • Consent must be informed and explicit
Individual Rights	• Right to be forgotten and restrict processing • Entities must comply with Data Subject Portability requests
Transparency & Integrity	• New Notice specifications and consolidated across jurisdictions • Data Subject right to access & rectify and receive details of processing without delay
Security & Breach Notification	• Required regular assessment of technical controls • Mandatory notification to DPA within 72 hours of Personal Data breaches
International Transfers	• Recognition of Binding Corporate Rules; standard contracts; codes of conduct; and certifications • US/EU transfers by Privacy Shield
Data Processors	• Penalties and GDPR requirements apply directly to Processors • Required terms for contracts with Controllers with restrictions on sub-contracting
Remedies	• Individuals have greater judicial remedies and DPAs may impose sanctions including fines up to 4% of global annual turnover

Enterprise Compliance Risks

GDPR compliance risk is not only financial, but can also result in operational distress or litigation.

GDPR is enforced primarily by ***Supervisory Authorities*** (DPAs) as independent agencies in each Member State. DPAs have investigatory and corrective powers, including the explicit power to fine organizations found to have violated GDPR.

Public Right of Action: Individual Data Subjects can bring suit (incl. Class actions)

Corrective Powers: warnings, order compliance, and impose a limitation on processing

Administrative Fines: Max fine greater of EUR 20 million, or up to 4% of the annual worldwide revenue

Litigation Risk	*Operational Risk*	*Financial Risk*
• DPAs are required to investigate all valid complains of GDPR violations. This may lead to significantly more reviews and enquiries from DPAs, or directly from employees or customers for organization to respond • DPA court actions may increase significantly • The GDPR introduces US-style class action consumer lawsuits. Organizations must ensure comprehensive response and monitoring of processes to avoid legal escalation	• DPAs access any data processing equipment or premises without notice, and issue injunctions on all data processing – *organizations cease to operate* • DPAs can order immediate *destruction of vital business data* pursuant to unlawful collection or Right of Erasure/Right of Access request • DPAs can review the nature of personal data transfers in corporate transactions (mergers etc.). *Transaction delayed by DPA ordered individual consent or notification*	• Companies can be fined up to **2% of global annual revenue, or EUR 10 million**, *whichever is greater*, for failing to conduct impact assessments, breach notification to Supervising Authorities, and not having their records in order • Companies can be fined up to **4% of global annual revenue or EUR 20 million (GDPR)**, for non-compliance with basic principles, including conditions for consent, Data Subjects' rights, transfers of Personal Data to a 3rd country

How Does GDPR Impact Organizations?

GDPR replaces EC Directive 95/46 ("Data Protection Directive") which has been in force since 1995 but has been unable to respond to globalization of data, multi-stream technology innovation and explosive business growth.

As a replacement, GDPR will present seismic changes to all aspects of personal data processing:

Scope
- More Entities Covered
- Data Processors Covered
- Non-EU Coverage
- New Privacy Principles

Subject Rights
- Explicit Consent
- Rectification & Restriction
- Right to be Forgotten
- Portability

Legal Risks
- DPA Enforcement Powers
- Fines & Sanctions
- Compensation Claims
- Class Actions

Security & Ops
- Privacy Policies & Notices
- Accountability
- Breach Response
- Data Protection Officer
- PIAs & PbD & D

Key Operational Impacts

- *Lawful Data Collection & Consent*
- *Right of Access & Erasure*
- *Customer Profiling & Big Data*
- *Data Security & "Accountability"*
- *Breach Response & Notification*
- *Cross-border Data Transfer*
- *Dedicated Resourcing & the Data Protection Officer*

Key Topics GDPR on security & Data Breach

Security of processing (Art. 32)

- Risk-based approach (nature of data, scope and level security)
  - E.g., pseudonymization, encryption
- Can be based on code of conduct
- Continued reference to the State of the Art

Data breach notification (Arts. 33-34)

- Definitions
  - Unauthorized or unlawful use, destruction, loss, alteration processing
- Triggers
  - Any breach UNLESS unlikely to result in "harm"
- Modalities and timeframes
  - Report to DPA(s) without "undue delay"/72 hours
  - If "high risk" tell data subjects – clear and plain language

Key Topics ***State Of the Art***

- Sustained governance structure, senior leadership sponsors and appropriate mandate
- Keeping pace with changing threat vectors and advancing technologies – to remain ***appropriate to risk*** and ***adequate***

[Not] *the most sophisticated control and security program for every process, all the time*

GDPR requires Controllers maintain security practices with regard to the State of the Art

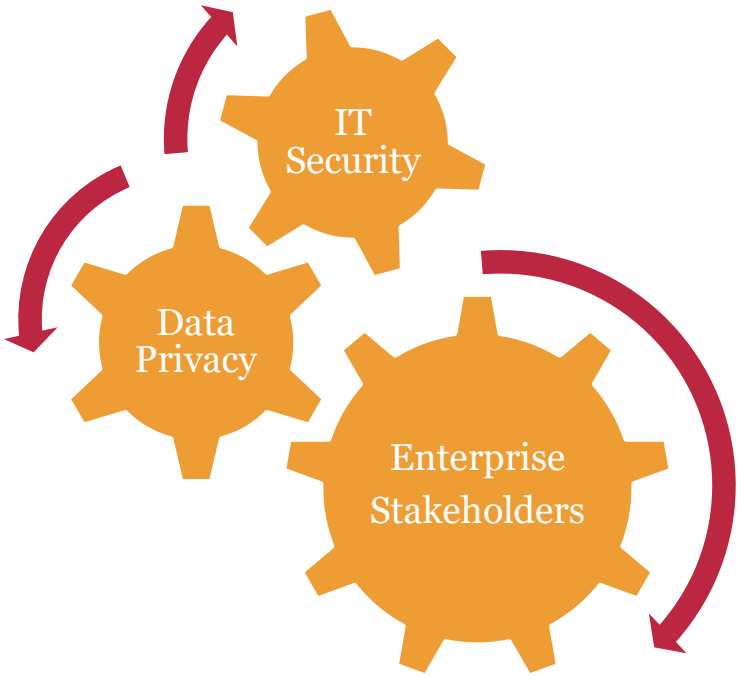
It's not only about EU regulation

FTC & FFIEC require risk-aware security practices and ongoing enhancement appropriate to risk and evolving threats

Response

3

Collaboration & Synergy



Includes:

- Planning Committees
- Communications
- Policies & Procedures
- Training
- Risk Assessments
- Incidence Response
- Monitoring & Reporting

Implementation Framework

Domain	Requirement	Tasks
Accountability & Governance	• An Accountability Governance framework to govern the processing of personal data • Regular business appropriate training program to develop a culture of privacy	• Establish Governance framework • Leadership Awareness program • Design appropriate training programs
PIA & Privacy by Design	• PIA must be performed for 'special' data (e.g., background check) • PbD concepts must be integrated into the PIA process and applied to new processing	• Implement PIA process business-wide • Integrate PbD procedures into PIA and train accordingly
Breach Response	• Ensure procedures in place to detect, respond to data breaches; Must DPAs within max 72 hrs. • Conduct regular cyber security reviews to ensure ongoing adequate protection measures	• Implement adequate breach response & notification program • Design ongoing Cyber Security review program
Data Processors	• Suppliers must implement appropriate technical and organizational measures to meet GDPR requirements • 3rd parties must be contractually committed to support your GDPR compliance and be regularly monitored depending on risk	• ID and risk assess all 3rd parties • Re-contract all suppliers according to risk • Implement ongoing 3rd party monitoring program
Records of Processing Activities	• Records are required data processing activities, covering purposes of the processing, categories of data, categories of recipients (sharing) of data, where it came from and retention periods	• Develop a sustainable Personal Data processing inventory
Data Subject Rights	• Procedures must cover all SARs • Response must be possible electronically and in commonly used format • Not all SARs are absolute rights	• Assess likelihood & impact of all SAR scenarios • Design appropriate, risk-based procedures for SAR scenarios

Additional Considerations

- Policies and procedures hygiene
- Process realignment
- Tools and Automation
- Training

Questions