Data Privacy

What is the purpose of the Data Privacy Function in a company?

- The purpose of the unit is to ensure corporate level standards including compliance with in-country Data Privacy Regulations are complied with, by specifying the Control Objectives and ensuring design and operating effectiveness

- Examples of Regulation:

- UAE : Consumer Protection Regulation and Standards, Proposed Data Privacy Law for Financial Transactions

- UK / FR : General data Protection Regulation

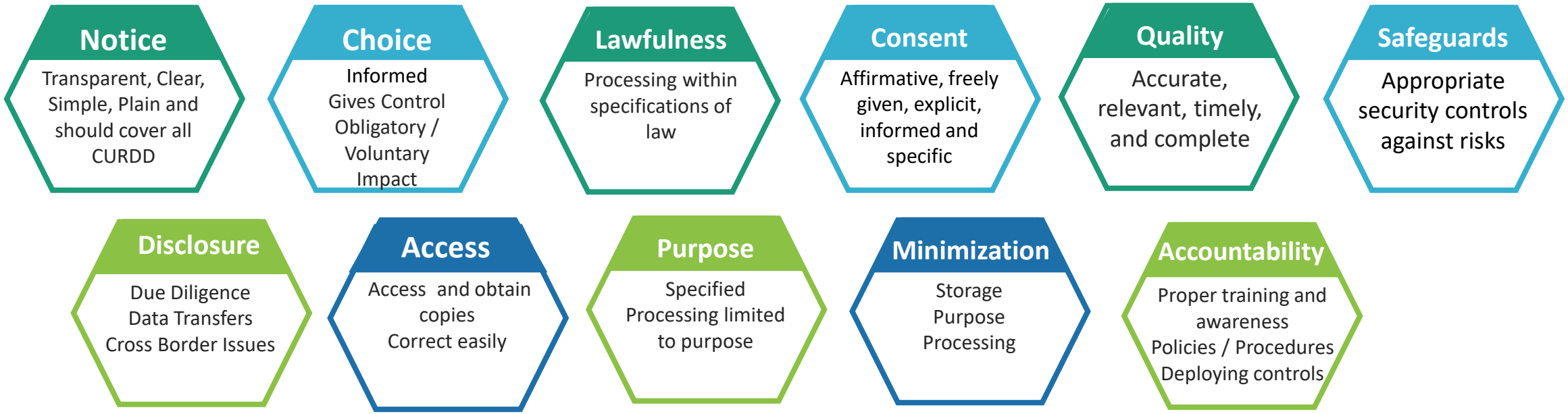
- HK : Personal Data Protection Ordinance

- SG : Personal Data Protection Act

What are the Key Principles of Data Privacy ?

ISO defines Data privacy as the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information.

11 Principles that determine the obligations as follows



Background to Data Privacy

What is the need for Data Protection or Data Privacy for Consumers?

- Organisation for Economic Cooperation and Development has evolved a set of Data Privacy principles while US has Fair Information Practices. The General Data Protection Regulation (GDPR) of the European Union contains detailed requirements.
- In addition to Information Security requirement to protect personal data, laws in various countries have recognized Data Subject rights and have specified legal obligations or have other mandates
- Central Bank UAE has published the Consumer Protection Regulation and Standards. These specify a number of protections for Consumers in their life cycle of products and services including Data Management and Protection.
- Information Security assures Confidentiality, Integrity and Availability.
- Data Privacy = Information Security for Personal Data + Right of Data Subjects + Other Legal Obligations
- In many organizations, the Group Data Privacy Office is part of Group Security Office

Understanding Data Privacy Elements

Personal Data

Any information relating to an identified or identifiable natural person, identified directly or indirectly.

This includes factors of biometric, health, economic, social identity., all account details

Data Subject

Natural person, to whom the data refers. Subject of Personally Identifiable Information

(Customers, Employees, Authorized representatives of corporates)

Data Controller

The entity, who determines the processing means and purposes

(Business Units, Support Units, Chief Data Officer)

Data Processor

Performs operations on the data on behalf of the controller

(Head Office in regard to branches, Cloud Providers, Agents, Vendors)

Regulatory Authority

Public authority responsible for monitoring compliance to privacy legislation

(CB UAE, In-Country Regulators)

Data Subject Rights

Regulatory requirements protecting Data Subject Rights such as consent, access, retention, notification

(Violation of rights leads to fines)

Data Privacy Lifecycle Management

Appropriate collection of data

Relevant use of data

Managed disclosure

Appropriate retention and disposal

Review privacy due diligence

What are Data Subject Rights?

01 **Right to be Informed**

provide any information and any communication relating to processing to the data subject in a transparent, intelligible and easily accessible form, using clear and plain language.

02 **Right to Access**

obtain confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and other relevant info

03 **Right to Rectification**

obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.

04 **Right to erasure / to be forgotten**

obtain the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay.

Right to restriction of processing 05

Obtain restriction of processing where: a)accuracy is contested by the data subject; b) the processing is unlawful; c) no longer needs the personal data for the purposes of the processing.

Right to Data Portability 06

receive the personal data in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance.

Right to object 07

object on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, including profiling based on those provisions.

Right not to be subject to a decision based on exclusive automated processing 08

right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him/her.

What are some Important Legal Obligations?

Consent -1

Ensure that Data Subject 'Opt-in' for various products, services, contacts.

They are considered 'opted-out' by default.

Consent -2

A record of Consent, notices and disclosures is maintained for a specified period

3rd Parties

Sharing of Information with 3rd Party is highly controlled and processing is limited

Limitation

All Personal data Processing is limited to the agreed purposes only

Records

Records are maintained until the purpose is served and not beyond what is legally necessary

Access Rights

Ensuring that Data correction requests are promptly addressed.

Any complaints are fully resolved

Breach

Breaches are fully prevented.

If these happen, these should be properly handled and reported

Controls

Ensure a proper environment of protection

Perform the requires risk assessments and monitor compliance

What are the functions of Data Privacy in a company?

Design

1. They design Control Objectives relating to Data Privacy.

2. They also design how IT and Business Units handle the Risks and Controls as a part of their Risk Control Self Assessments requirements (RCSA)

Review

1. They perform a number of reviews upon receipts of requests.

2. They also carry out Privacy Impact Assessments to assess conformance of number of Business Initiatives, to Data Privacy laws and requirements

3. This can cover Business Unit Legal Agreements, SOPs, New Products or Services or tools or new system features

Monitoring

1. They monitor risks under RCSA. They also offer Consulting support to Business Units.

2. They track the risks and monitor the progress of remedial actions

3. They also monitor the environment for ad hoc regulatory requirements

Reporting

1. Dashboard based System for International Locations- reports on key Data Privacy aspects

2. A number of reports are made out on risks and status at Management Committee meetings, for CISO and as well as Chief Risk Officer

Understanding Group Data Privacy Office more deeply

What is a Privacy Impact Assessment?

A Privacy Impact Assessment systematically understands a new initiative that handles personal data. All aspects of the processing are then studied for compliance with regulations and other requirements.

How is a Privacy Impact Assessment done?

- This is done by collaborating with respective Business Unit on filling a Processing Description Form.
- Once the form is filled by the Business Unit, relevant aspects are reviewed. A Processing Assessment Questionnaire then checks compliance with respective specific regulations.

Why is Privacy Impact Assessment required?

- This Assessment is required to determine if all the requirements of Regulations are complied with.
- If there are any gaps these should be addressed.
- If there are gaps that present a High Risk to Data Subject Rights, then a more detailed Data Protection Impact Assessment is required in some countries.
- In other cases, it is important to demonstrate adequate due diligence over Data Subject rights and legal requirements

What does a Typical Risk Report look like?

Ref	Key Risk Areas	UAE	UK	FR	HK	SG	KW
1	Areas having High potential for regulatory action	0	0	0	0	0	0
2	Areas having Medium potential for regulatory action	0	0	0	0	0	0
3	Material Regulator orders or enquiries on non-compliance	0	0	0	0	0	0
4	Data Privacy Breaches arising from Technology, Process or Human Failures	0	0	0	0	0	0
5	Material Data Processor(Vendor) compliance issues	0	0	0	0	0	0
6	Open Integration / Migration Data Privacy Issues , (Open Audit Issues or other material Review issues)	0	1	1	0	3	0
7	Any other material compliance issues with Bank's Obligations including DPO tasks related support	0	0	0	0	0	0

- In addition, Company level Risk Issues re reported, with the Status and progress of remedial actions.