DATA PROTECTION BASIC

Data Protection Authority

Commonly Asked Questions about the Basics of Data Protection

DATA PROTECTION BASICS

1. **What is the Data Protection Authority in Somalia?**

(DPA) is the national independent authority responsible for protecting personal privacy and monitoring that all organizations are compliant with the Data Protection Act (no. 005 which was passed in March 2023).

2.What is the role of the Data Protection Authority DPA)?

The role of DPA is to implement the Data Protection Act, as well as providing services that facilitate protection of personal data, such as; awareness campaigns, registration, trainings, creating and passing regulations specific to storing and processing data.

3. when does data protection low apply and what does it cover?

Data protection laws are crucial for safeguarding personal information in our increasingly digital world. These laws apply to the collection, processing, storage, and sharing of personal data, typically focusing on data belonging to individuals or "data subjects." The specifics can vary by jurisdiction, but here are general principles and coverage areas common to many data protection laws:

When Data Protection Law Applies

Geographical Scope: Data protection laws typically apply based on:

Territoriality: If the data processing occurs within the jurisdiction, regardless of the nationality or residence of the data subject.

Extraterritoriality: If the data subjects are residents of the jurisdiction, regardless of where the data processor or controller is located. This means companies outside the jurisdiction may still need to comply if they are handling data from individuals within that jurisdiction (e.g., GDPR).

Types of Data: Most data protection laws apply to personal data, which is any information relating to an identified or identifiable natural person. Some laws also specifically address the handling of sensitive personal data, such as health information, political opinions, or racial and ethnic data.

Activities Covered: These laws apply to all major activities involving personal data, including:

Collection

Storage

Use

Processing

Transmission

Disclosure

What Data Protection Law Covers

- **Rights of Data Subjects:** Data protection laws typically grant individuals certain rights regarding their personal data, such as:
    - Right to Access: Individuals can request access to their personal data to understand how and why it is being processed.
    - Right to Rectification: Individuals can request correction of inaccurate personal data.
    - Right to Erasure: Often referred to as the "right to be forgotten," allowing individuals to request the deletion of their data under certain conditions.
    - Right to Restrict Processing: Individuals can request that the processing of their data be restricted.
    - Right to Data Portability: Allows individuals to receive their data in a structured, commonly used format, and to transfer it to another data controller.
    - Right to Object: Individuals can object to certain types of data processing, such as processing for direct marketing purposes.

Obligations of Data Controllers and Processors: Entities that handle personal data are required to:

Protect data using appropriate technical and organizational measures.

Ensure transparency about data processing activities.

Obtain consent for processing data in certain situations, particularly when handling sensitive data.

Report data breaches to relevant authorities and, in some cases, to the affected individuals.

Appoint a Data Protection Officer (DPO) in certain circumstances.

Regulatory and Compliance Requirements: Depending on the jurisdiction, there may be requirements for:

Conducting impact assessments for high-risk processing.

Registering data processing activities with a supervisory authority.

Adhering to specific principles of data processing, such as minimizing the collection of data, limiting the purpose for which data is collected, and ensuring data accuracy.

Examples of Data Protection Laws

- General Data Protection Regulation (GDPR): Applies across the European Union and to entities outside the EU that process data of EU residents.
- California Consumer Privacy Act (CCPA): Applies to certain businesses that collect the personal data of California residents.
- Personal Data Protection Act (PDPA) in Singapore: Applies to data controllers and processors in Singapore handling personal data.

- Each jurisdiction has its own nuances and additional requirements, so it's important to consult specific laws relevant to your location or the locations where your data subjects reside.

4. what is personal data? when are they processed

Personal data refers to any information that relates to an identified or identifiable individual. This could include direct identifiers like a person's name, identification number, location data, online identifier, or factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity.

Here are some common categories and examples of personal data:

1. Identifiers: These are pieces of information that directly identify an individual. Examples include:

- Name
- Social Security number
- Passport number
- Driver's license number
- Employee identification number

2. Contact Information: This includes information that allows for communication with the individual. Examples are:

- Email address
- Phone number
- Mailing address

3. Biographical Information: This refers to details about an individual's life. Examples include:

- Date of birth
- Age
- Gender
- Marital status

4. Financial Information: This includes data related to an individual's financial status or transactions. Examples include:

- Bank account number
- Credit card number
- Salary details
- Tax identification number

5.Location Data: Information about an individual's physical location. Examples include

- GPS coordinates
- IP address
- Mobile device location data

6.Online Identifiers: These are identifiers specific to an individual's online presence. Examples include:

- Usernames
- Social media handles
- Cookies
- Device identifiers

7.Health and Medical Information: Data related to an individual's health or medical history. Examples include:

- Medical records
- Health insurance information
- Genetic data
- Biometric data (e.g., fingerprints, facial recognition data)

8.Biometric Data: Unique physical characteristics used for identification. Examples include:

- Fingerprints
- Retina scans
- Voiceprints
- Facial recognition data

9.Ethnicity or Race: Information about an individual's racial or ethnic origin.

10.Criminal Records: Information related to an individual's criminal history or legal proceedings.

- Personal data can be processed in various situations and for a multitude of purposes. Here are some common scenarios in which personal data may be processed

  . **Consent**: When someone agrees to their data being used, like opting in for marketing emails.

  . **Contractual Obligations**: Processing data to fulfill a contract, such as providing a product or service after a purchase.

  . **Legal Obligations**: Processing data to meet legal or regulatory requirements, like tax purposes or responding to lawful requests.

  . **Legitimate Interests**: When it's necessary for legitimate interests, such as fraud prevention or security, balancing against individuals' rights.

  . **Vital Interests**: Processing data to protect someone's or others' vital interests, like emergency medical treatment.

  . **Public Interest**: Processing data for tasks in the public interest or exercising official authority, like public health or national security.

  . **Contractual Necessity**: Processing data necessary for a contract or steps before entering into one, such as assessing eligibility for a service.

5. what is data controller?

A data controller, as defined by data protection authorities, is an entity or individual that determines the purposes and means of processing personal data. In simpler terms, it's the party responsible for deciding why and how personal data is processed.

Responsibilities of a Data Controller:

1. Compliance with Data Protection Principles: Data Controllers must ensure all data processing activities adhere to legal requirements of lawfulness, fairness, transparency, data minimization, accuracy, integrity, and confidentiality.

2. Implementing Protective Measures: They are required to establish and maintain security measures to protect personal data from unauthorized access and other risks.

3. Managing Consent: Data Controllers must obtain and manage the consent of data subjects for data processing, ensuring it is clear and explicit, and allowing subjects to withdraw consent.

4. Data Subject Rights: They must facilitate the rights of data subjects, including access to data, corrections, erasure, portability, and the right to object to data processing.

5. Record Keeping: Data Controllers need to keep detailed records of all data processing activities and present these records to supervisory authorities upon request.

6. Data Protection Impact Assessments (DPIA): They are responsible for conducting assessments to evaluate the risks of data processing operations on the protection of personal data.

7. Notification of Data Breaches: Data Controllers must notify the relevant authority and possibly the affected data subjects about data breaches within 72 hours of awareness.

8.Appointment of a Data Protection Officer (DPO): If required, Data Controllers must

Data controllers have legal responsibilities under data protection laws to ensure that personal data is processed lawfully, fairly, and transparently. They must also take steps to protect the rights and freedoms of individuals whose data they process, including ensuring the security and confidentiality of the data.

In many cases, organizations or businesses are the primary data controllers for the personal data they collect and process. However, individuals acting in a personal capacity, such as sole traders or freelance professionals, can also be considered data controllers if they determine the purposes and means of processing personal data.

6. what is data processor?

A data processor, according to data protection authorities, is an entity or individual that processes personal data on behalf of a data controller. Unlike the data controller, which determines the purposes and means of processing personal data, the data processor only acts on the instructions of the data controller.

Here are some key points:

1. **Acting on Instructions**: The data processor processes personal data based on the instructions provided by the data controller. They don't decide on the purposes or methods of processing; rather, they carry out the processing activities as directed.
2. **Contractual Relationship**: There's typically a contractual relationship between the data controller and the data processor. This contract outlines the terms and conditions for the processing of personal data, including the obligations and responsibilities of both parties.
3. **Examples of Data Processors**: Data processors can include a wide range of entities or individuals, such as cloud service providers, IT support companies, payment processors, marketing agencies, and third-party vendors that handle personal data on behalf of a business or organization.
4. **Legal Responsibilities**: While data processors don't have the same level of control over personal data as data controllers, they still have legal responsibilities under data protection laws. They must process personal data securely, maintain confidentiality, and comply with the instructions provided by the data controller.
5. **Data Protection Agreements**: Data controllers often put in place data protection agreements or data processing agreements with data processors to ensure compliance with data protection laws. These agreements outline the specific requirements and obligations regarding the processing of personal data.

Overall, data processors play a crucial role in the processing of personal data on behalf of data controllers, and their actions can significantly impact the privacy and security of

individuals' data. Therefore, it's essential for data controllers to carefully select and manage data processors to ensure compliance with data protection regulations.

7. what is data protection officer (DPO)?

A Data Protection Officer (DPO) is an individual designated by an organization to oversee and ensure compliance with data protection laws and regulations. The role of the DPO is particularly crucial in organizations that process large amounts of personal data or engage in sensitive data processing activities.

Responsibilities of a DPO:

1. **Monitoring Compliance**: The primary responsibility of the DPO is to monitor the organization's compliance with data protection laws, regulations, and internal data protection policies. This involves staying up-to-date with relevant laws, conducting audits, and assessing data processing activities for compliance.

2. **Advising on Data Protection Matters**: The DPO serves as a knowledgeable resource within the organization, providing guidance and advice on data protection matters to management and staff. They may offer recommendations on best practices, risk assessments, and strategies for ensuring compliance.
3. **Handling Data Subjects' Requests**: The DPO is often responsible for managing data subjects' requests regarding their rights under data protection laws, such as access requests, rectification requests, and requests for erasure (the right to be forgotten).
4. **Cooperating with Regulatory Authorities**: The DPO serves as the point of contact for regulatory authorities regarding data protection matters. They may liaise with supervisory authorities, respond to inquiries or complaints, and facilitate communication during regulatory inspections or investigations.
5. **Data Protection Impact Assessments (DPIAs)**: The DPO may oversee the process of conducting Data Protection Impact Assessments, which are systematic assessments of the potential impact of data processing activities on individuals' privacy rights. DPIAs help identify and mitigate privacy risks associated with data processing activities.
6. **Training and Awareness**: The DPO may be involved in developing and delivering data protection training and awareness programs for staff members to ensure that they understand their responsibilities and obligations regarding data protection.