GDPR

Shweta A. Chawla
Founder & Investigator
SC Cyber Solutions

SC
Cyber Solutions

- The General Data Protection Regulation is a law that applies within the European Union (EU) and the European Economic Area (EEA)
  - European Economic Area (EEA) = European Union (EU) + Iceland + Liechtenstein + Norway + UK
- The law went into effect on May 25, 2018
- Governs the type of notice that must be provided to people regarding how their identifiable data is used
- Governs how companies are allowed to use and process identifiable data
- Has stricter requirements for using and processing sensitive data

shweta@sccybersolutions.com

SC
Cyber Solutions

Aim of GDPR

- Protection of personal data and privacy of EU citizens
- Restriction on export of personal data outside of EU

shweta@sccybersolutions.com

SC
Cyber Solutions

Who does GDPR apply to?

- Those who offer goods or services to persons in the EU and/or the EEA
- Those who control and process data about persons in the EU/EEA

shweta@sccybersolutions.com

SC
Cyber Solutions

Data protected by GDPR

- Personally identifiable information (PII)
  - Any data that can specifically used to identify an individual
  - Basic identity information – name, age, address, email address, phone number, identity numbers
  - Web data – login info, social media posts, images, geolocation, IP address, cookies, RFID tags, browsing and behavioural data
  - Health, medical data
  - Biometric data
  - Genetic, racial, ethnic data
  - Political opinions, religious affiliations, union memberships
  - Sexual orientation

shweta@sccybersolutions.com

SC
Cyber Solutions

Controllers vs Processors

- A distinction is made recognizing the fact that not all organisations processing identifiable data have the same resoponsibilites
- Controller
  - The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
  - Make decisions about processing activities
  - Responsible for complying under GDPR
  - Need to demonstrate compliance with the data protection principles
  - Deploy adequate technical and organizational measures

shweta@sccybersolutions.com

SC
Cyber Solutions

- Processor
  - A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
  - Serve the controller's interests
  - Limited compliance requirements

shweta@sccybersolutions.com

SC
Cyber Solutions

Data Processing

- Processing of data involves one or more of the following
  - Adapting
  - Altering
  - Collecting
  - Combining
  - Consulting
  - Destroying
  - Disclosing
  - Erasing
  - Organizing
  - Recording
  - Retrieving
  - Storing
  - Structuring
  - Using

shweta@sccybersolutions.com

SC
Cyber Solutions

Principles of GDPR

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

shweta@sccybersolutions.com

SC
Cyber Solutions

Consent under GDPR

- Consent must be freely given, specific, informed and unambiguous
- It must be given on a voluntary basis
- Other bases for processing personal data
  - Contract
  - Legal obligations
  - Vital interests of the data subject
  - Public interest
  - Legitimate interest as stated in Article 6(1) GDPR

shweta@sccybersolutions.com

SC
Cyber Solutions

Steps to Ensure GDPR Compliance

- Appoint a data protection officer
- Classify all data
- Complete a privacy impact assessment
- Document, maintain and enforce privacy policies, procedures and processes
- Train employees in GDPR
- Test data breach response procedures
- Monitor and audit GDPR compliance

shweta@sccybersolutions.com

SC
Cyber Solutions

Rights of an Individual under GDPR

- The right to be informed
  - Need to be informed of the data being collected, its purpose, retention policy, data sharing policy
- The right of access
  - Can ask to know what data about them is held by a company, its origin, its usage, who used it
- The right to rectification
  - Incorrect personal data can be rectified or completed
- The right to erasure
  - Ask for all records and traces of the individual to be removed
  - Applies when
    - The personal data is no longer necessary in relation to the purpose for which it was collected
    - The individual specifically withdraws consent to processing
    - Personal data has been unlawfully processed
  - The data must be erased within a fixed period of time as stated in legal obligations

shweta@sccybersolutions.com

SC
Cyber Solutions

- The right to restrict processing
  - Can request restriction or suppression of data
  - Its not an absolute right
- The right to data portability
  - Allows individuals to obtain and reuse their personal data
- The right to object
  - Users can object to their data being processed under certain circumstances
  - Users can stop their data from being used for direct marketing
- Rights in relation to automated decision making and profiling
  - Provides information about processing
  - Provides ways to request human intervention
  - Provides ways to challenge a decision

shweta@sccybersolutions.com

Contact details:
Mob: +91 98230 80864
shweta@sccybersolutions.com
www.sccybersolutions.com
@sccs1300