GDPR

Overview & Scope

- Enacted May 2018 (EU Regulation 2016/679)
- Applies to EU/EEA Organizations
- Extra-territorial Scope (non-EU firms serving EU residents)
- Replaces Data Protection Directive 95/46/EC
- Enforced by National DPAs

7 Core Principles (Article 5)

1. Lawfulness, Fairness & Transparency
2. Purpose Limitation
3. Data Minimisation
4. Accuracy
5. Storage Limitation
6. Integrity & Confidentiality
7. Accountability

Lawful Bases for Processing (Article 6)

- Consent
- Contractual Necessity
- Legal Obligation
- Vital Interests
- Public Task
- Legitimate Interests

Data Subject Rights

- Art. 15 – Right of Access
- Art. 16 – Right to Rectification
- Art. 17 – Right to Erasure ('Right to be Forgotten')
- Art. 18 – Right to Restriction of Processing
- Art. 20 – Right to Data Portability
- Art. 21 – Right to Object
- Art. 22 – Rights re. Automated Decision Making & Profiling

Key Roles

- Data Controller
  - Determines purpose & means of processing
  - Primary accountability to DPA
- Data Processor
  - Processes on behalf of controller
  - Bound by Data Processing Agreement
- Data Protection Officer (DPO)
  - Mandatory for public bodies & large-scale processors
  - Independent advisory & compliance role
- Data Subject (Individual)
- Supervisory Authority (DPA)

Special Categories of Data (Article 9)

- Racial / Ethnic Origin
- Political Opinions
- Religious / Philosophical Beliefs
- Trade Union Membership
- Genetic & Biometric Data
- Health Data
- Sex Life / Sexual Orientation

Consent Requirements

- Freely Given
- Specific
- Informed
- Unambiguous (clear affirmative action)
- Withdrawable at any time
- No pre-ticked boxes / bundling

Key Obligations for Organizations

- Privacy by Design & by Default (Art. 25)
- Records of Processing Activities – ROPA (Art. 30)
- Data Protection Impact Assessment – DPIA (Art. 35)
- Data Processing Agreements – DPA (Art. 28)
- Appoint DPO where required (Art. 37)
- Privacy Notice / Transparency (Art. 13-14)
- Security Measures (Art. 32)

Breach Notification

- Notify DPA within 72 hours (Art. 33)
- Notify Data Subjects without undue delay (Art. 34)
- Only if likely to result in high risk
- Processor notifies Controller promptly
- Document all breaches internally

Related Regulations & Frameworks

- UK GDPR (post-Brexit)
- ePrivacy Directive (Cookie Law)
- NIS2 Directive (Cybersecurity)
- EU AI Act (AI & profiling)
- ISO/IEC 27701 (Privacy ISO standard)
- CCPA / CPRA (California, US)

Penalties & Enforcement

- Tier 1 – Lower Fine
  - Up to €10M or 2% global turnover
- Tier 2 – Higher Fine
  - Up to €20M or 4% global turnover
- Corrective Powers (ban processing, etc.)
- Right to Compensation (Art. 82)
- One-Stop-Shop Mechanism (lead DPA)

International Data Transfers

- Adequacy Decisions (e.g. UK, Japan, Canada)
- Standard Contractual Clauses (SCCs)
- Binding Corporate Rules (BCRs)
- EU-US Data Privacy Framework (2023)
- Derogations (explicit consent, vital interests, etc.)

www.hackingarticles.in

@hackinarticles
https://github.com/Ignitetechnologies
https://in.linkedin.com/company/hackingarticles