**1️⃣ What is GDPR?**

* **Full name:** General Data Protection Regulation (EU) 2016/679)
* **Enforced:** 25 May 2018
* **Purpose:** Protect natural persons in the EU regarding processing of **personal data** and free movement of such data.
* **Scope:**
  + **Material:** Any operation on personal data (collection, storage, use, disclosure, deletion, etc.).
  + **Territorial:** Applies to controllers/processors in the EU **and** outside the EU if offering goods/services to, or monitoring, EU data subjects.

**2️⃣ Key GDPR Terms to Know**

| **Term** | **Meaning** | **Example** |
| --- | --- | --- |
| **Personal Data** | Any info relating to identified or identifiable person | Name, email, IP, device ID |
| **Special Category Data** | Sensitive data with extra protection | Health, biometrics, race, religion |
| **Processing** | Any operation performed on personal data | Collecting, storing, deleting |
| **Controller** | Entity determining purposes & means of processing | An e-commerce site |
| **Processor** | Processes data on behalf of controller | Cloud hosting provider |
| **Data Subject** | The individual whose data is processed | A customer |
| **DPO (Data Protection Officer)** | Oversees compliance, reports to top mgmt | Appointed in high-risk orgs |
| **Supervisory Authority** | National authority monitoring GDPR compliance | CNIL in France |

**3️⃣ GDPR Principles (Art. 5)**

1. **Lawfulness, fairness, transparency**
2. **Purpose limitation**
3. **Data minimization**
4. **Accuracy**
5. **Storage limitation**
6. **Integrity and confidentiality**
7. **Accountability**

**4️⃣ Lawful Bases for Processing (Art. 6)**

* Consent
* Contract
* Legal obligation
* Vital interests
* Public task
* Legitimate interests

**5️⃣ Data Subject Rights (Arts. 12–22)**

* Right to information (privacy notice)
* Right of access
* Right to rectification
* Right to erasure (right to be forgotten)
* Right to restrict processing
* Right to data portability
* Right to object
* Rights related to automated decision-making & profiling

**6️⃣ Key Processes to Understand for Interview**

**A. Data Mapping & Records of Processing (RoPA)**

* Maintain Article 30 records (who, what, why, how long, with whom shared).

**B. DPIA (Data Protection Impact Assessment)**

* Required when high risk to individuals (e.g., large-scale profiling, biometrics).

**C. Consent Management**

* Freely given, specific, informed, unambiguous, easy to withdraw.

**D. Breach Notification**

* Notify supervisory authority within **72 hours** of becoming aware, unless unlikely to risk rights/freedoms.
* Notify data subjects without undue delay if high risk.

**E. International Transfers**

* Only if adequate safeguards:
  + Adequacy decision
  + SCCs (Standard Contractual Clauses)
  + BCRs (Binding Corporate Rules)

**F. Vendor (Processor) Management**

* Contracts must have Art. 28 clauses: processing only on instructions, confidentiality, security, subprocessor approval, deletion/return of data, audits.

**7️⃣ Penalties**

* Up to **€20M or 4% of global annual turnover** (whichever higher) for severe infringements.
* Lower tier: €10M or 2% turnover.

**8️⃣ Implementer vs Auditor View**

**Implementer Perspective:**

* Build a GDPR register of processing.
* Implement consent management system.
* Establish data retention & deletion policy.
* Create breach response process (with 72h clock).
* Ensure vendor contracts are GDPR-compliant.

**Auditor Perspective:**

* Check RoPA completeness.
* Verify privacy notices match actual processing.
* Sample test consent records & withdrawal process.
* Review DPIA for high-risk projects.
* Verify breach notifications met timing & content.
* Examine international transfer safeguards.

**9️⃣ Interview Hot Questions**

* “Walk me through GDPR principles and how you ensure compliance.”
* “What’s the difference between controller and processor obligations?”
* “How do you handle a personal data breach under GDPR?”
* “What are the lawful bases for processing, and which one is most flexible?”
* “What’s a DPIA and when do you need one?”
* “How do you handle cross-border data transfers post-Schrems II?”

If you want, I can make you a **GDPR One-Page Study Sheet** with:

* All Articles to remember for audit
* Breach workflow (72h process)
* Lawful bases table
* Rights table
* Implementer/Auditor checklist