GDPR CHEAT SHEET

Curated By: tsaaro

GDPR OVERVIEW

A comprehensive data protection regulation enacted by the European Union (EU)

It aims to safeguard personal data and privacy rights of individuals within the EU

GDPR applies to businesses and organizations that process personal data of EU residents

RIGHTS OF DATA SUBJECTS

RIGHT TO BE INFORMED

Individuals have the right to know how their data is collected, processed, and used

RIGHT OF ACCESS

Individuals can request access to their personal data held by organizations

RIGHT TO RECTIFICATION

Individuals can request correction of inaccurate or incomplete data

RIGHT TO ERASURE

Individuals can request the deletion of their data under certain circumstances

RIGHT TO RESTRICT PROCESSING

Individuals can limit or restrict the processing of their data

RIGHT TO DATA PORTABILITY

Individuals can request their data to be provided in a structured, commonly used format

RIGHT TO OBJECT

Individuals can object to the processing of their data in certain situations

RIGHTS RELATED TO AUTOMATED DECISION-MAKING AND PROFILING

Individuals have the right to know if decisions are made solely based on automated processing

HOW TO BECOME GDPR COMPLIANT

DATA PROTECTION OFFICER (DPO)	RECORD KEEPING	CONSENT MANAGEMENT
Appoint a DPO if your organization's core activities involve regular and systematic monitoring of individuals on a large scale or processing special categories of data	Maintain records of data processing activities, including the purposes of processing, categories of personal data, recipients of data, and retention periods	Obtain explicit consent for processing personal data, providing clear information about the purposes and rights associated with the processing

DISCOVER → **DEFINE** → **DEVELOP** → **DEPLOY** → **SUSTAIN**

- *Understand the GDPR Requirements & the data setup & flow*
- *Evaluate the gap & define the Compliance Strategies*
- *Set up the Compliance PMO & the Data Governance Policies*
- *Implement the Corrective Strategies*
- *Ensure an ongoing compliance*

GDPR COMPLIANCE JOURNEY

COMPLIANCE IN DATA BREACH

ASSESS THE BREACH	CONTAIN THE BREACH	RESTORE DATA SECURITY
Determine the breach scope and data compromised and Evaluate risks and potential harm	Stop the Breach and Engage in Security Teams for investigation	Take necessary steps for the restoration of Data Security

72 HOURS TO REPORT

NOTIFY AFFECTED INDIVIDUALS	NOTIFY RELEVANT PARTIES
Notify Data Subjects if Breach likely to result in high risk to the rights and freedoms	Notify Internal Team, Legal Team and Supervisory authority within 72 hours of Data Breach Discovery

PENALTIES UNDER GDPR

ADMINISTRATIVE FINES

Supervisory authorities can impose fines for GDPR violations

€20 MILLION
€10 MILLION

MAXIMUM FINES

Up to €20 million or 4% of worldwide annual turnover for severe violations, and up to €10 million or 2% of worldwide annual turnover for less severe infringements

Fines are determined based on the nature, gravity, duration of the infringement, and mitigation measures taken

KEY GDPR PRINCIPLES

PURPOSE LIMITATION

Collect and process personal data only for specified, explicit, and legitimate purposes

LAWFULNESS, FAIRNESS, AND TRANSPARENCY

Ensure that data processing is done lawfully, fairly, and transparently

DATA MINIMIZATION

Collect and process only the necessary personal data for the intended purpose

ACCURACY

Maintain accurate and up-to-date personal data

STORAGE LIMITATION

Retain personal data for only as long as necessary

INTEGRITY & CONFIDENTIALITY

Implement appropriate security measures to protect personal data

TYPES OF VIOLATIONS

Non-compliance with data protection principles

Failure to uphold individual rights

Inadequate security measures leading to data breaches

Improper data transfers to countries without adequate protection

OTHER ENFORCEMENT MEASURES

Authorities can issue warnings, reprimands, and orders to comply

Limitations on data processing or suspension of data transfers may be imposed

DATA SECURITY & PRIVACY MEASURES

- **DATA ENCRYPTION**
- **ACCESS CONTROLS**
- **REGULAR DATA BACKUPS**
- **DATA BREACH NOTIFICATION**
- **PRIVACY BY DESIGN**