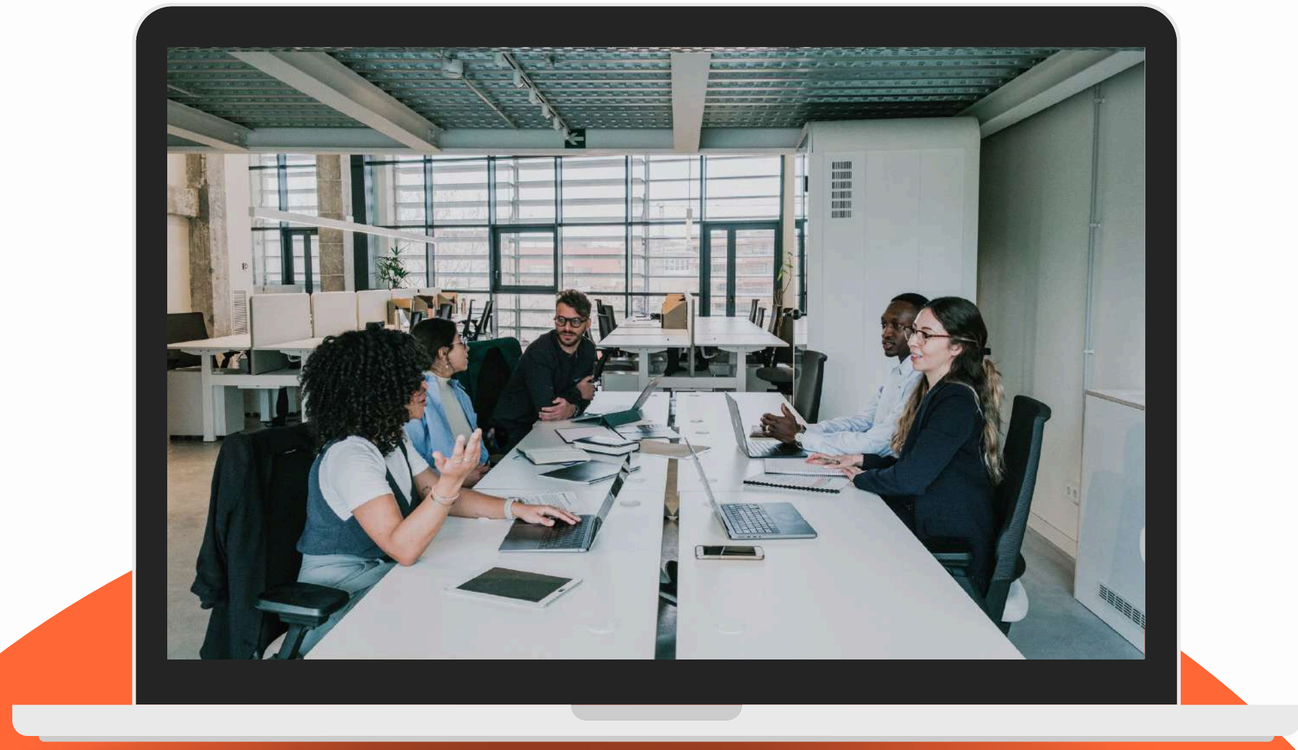
SALOT & SHAH ASSOCIATES

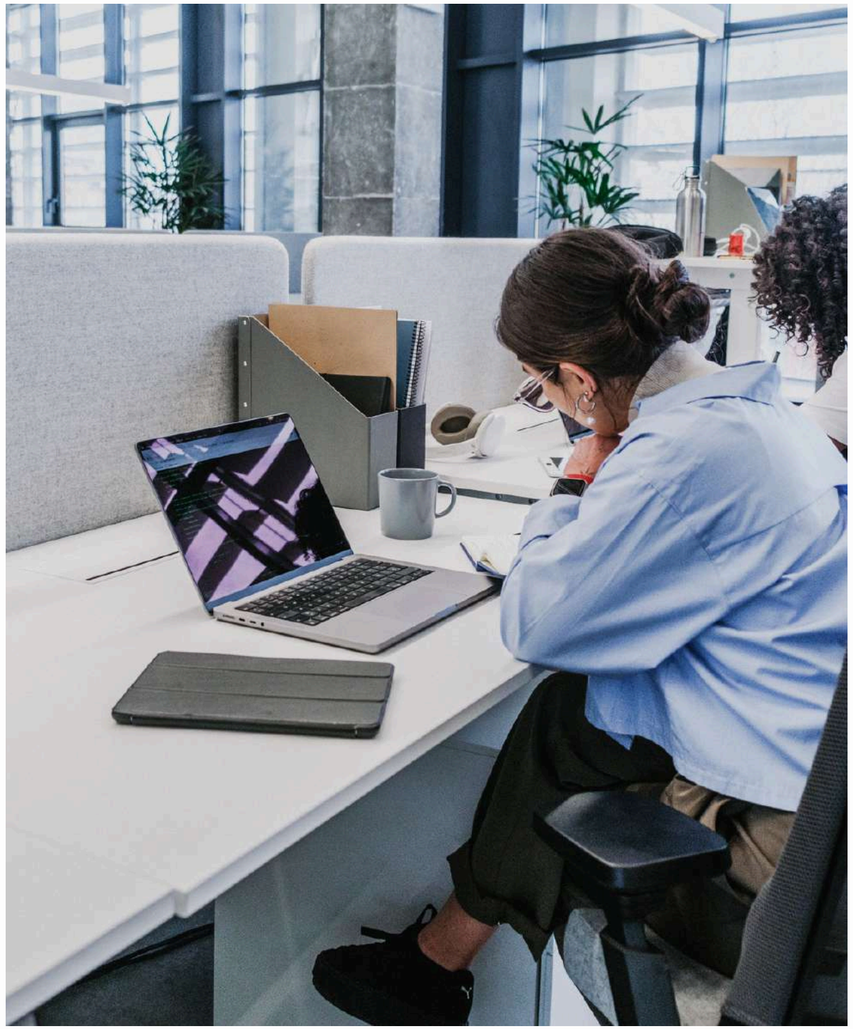
GENERAL DATA PROTECTION ACT (GDPR)

By: Salot and Shah Associates



Overview

- Introduction
- Need of GDPR
- Key Definitions
- Applicability and Scope
- Overview of GDPR Framework
- Core Principles of GDPR (Article 5)
- Rights of Data Subjects
- Obligations of Controllers & Processors
- Consent Framework under GDPR
- Governance Structure
- Penalties



Introduction

As digital technologies have become a part of everyday life, organizations now collect and use large amounts of personal information. This increased use of data has also raised concerns about privacy and misuse of personal information. To address these concerns and ensure better protection of individuals' data across the European Union, the General Data Protection Regulation (GDPR) was introduced. GDPR provides a clear framework for responsible, fair, and secure handling of personal data.

1995
Directive (95/46/EC) 1st EU Data Protection Law introduced

2012
GDPR formally proposed by the European Commission

2014-15
Debates on: Consent standards, Enforcement, Role of national authorities

Apr 2016
GDPR formally adopted by the EU Parliament and Council
EU Regulation 2016/679

May 2016
GDPR entered into force 2 Year transition period provided to organizations for compliance

2018
GDPR became fully applicable and enforceable

SALOT & SHAH ASSOCIATES

Need of GDPR Act

Obligations and Rights: To grant individuals clear rights over their personal data and impose obligations on organizations that collect and process such data, in accordance with the GDPR.

Processing of Data: Provides guiding principles on how data can be collected and on which legal basis the processing can take place.

Digital Economy and Data Usage: The rapid growth of the digital economy has transformed both economic activities and social interactions. As a result, the collection and use of personal data have become an integral part of digital transactions.

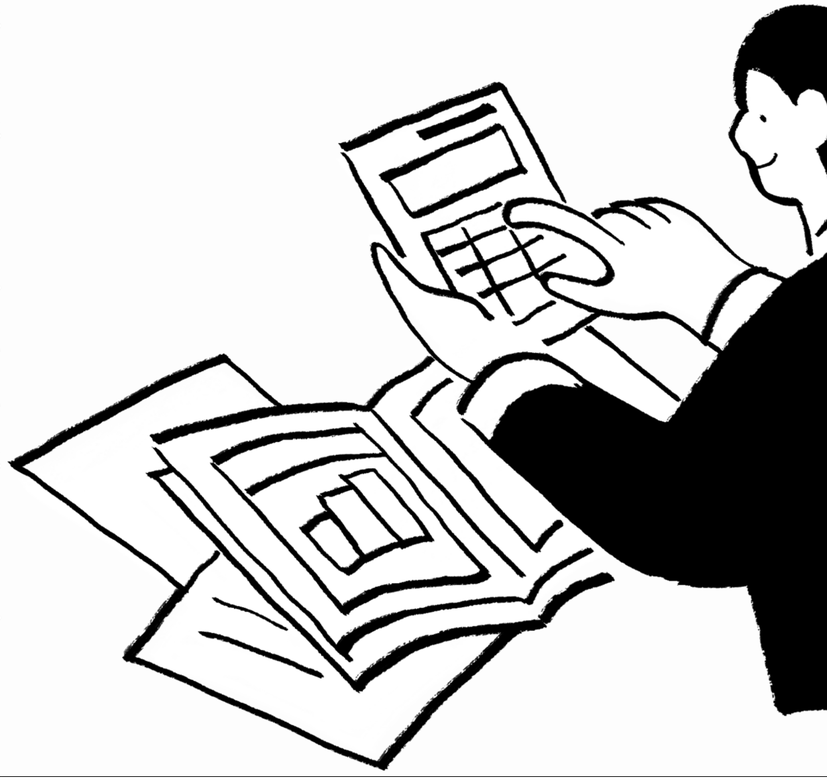
Cross-Border Data Transfers: Increasing international data flows required a structured framework to ensure personal data remains protected when transferred across borders.

Imposing Penalties: To impose strict penalties on organizations for unlawful or non-compliant processing of personal data, ensuring effective enforcement of the GDPR.

SALOT & SHAH ASSOCIATES

Key Definitions

Data Subject: An identifiable person is one who can be recognized, directly or indirectly, through identifiers such as a name, ID number, location data, or factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity. Essentially, the data subject is any living individual whose information is being collected, stored, or processed.



Data 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data Processor: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Personal Data: means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Key Definitions (Cont..)

Consent: Freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

Personal Data Breach: Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Cross Border Processing: Refers to data activities occurring across a company's establishments in multiple EU Member States, or activities at a single EU location that substantially affect individuals in more than one Member State.

Sensitive Personal Data (Special Categories): Data revealing racial/ethnic origin, political opinions, religious/philosophical beliefs, trade union membership, genetic/biometric data, health data, or data concerning a person's sex life or sexual orientation.

Pseudonymisation: Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

SALOT & SHAH ASSOCIATES

Applicability and Scope

01 Applies to organizations within the EU and those outside the EU that offer goods or services to, or monitor the behavior of, individuals located in the EU.

02 Governs the processing of "personal data" (any information relating to an identified or identifiable natural person) by fully or partially automated means or manual filing systems.

03 The regulation does not apply to data processing carried out by an individual for purely personal or household activities with no connection to professional or commercial activity.

04 Specifically excludes processing related to national security, common foreign and security policy, and activities by competent authorities for the prevention or prosecution of criminal offenses.

GDPR REQUIREMENTS FOR ORGANIZATIONS

SALOT & SHAH ASSOCIATES

Data Protection Impact Evaluation

A Data Protection Impact Evaluation is conducted to evaluate the impact of new or changed data processing activities on the protection of personal data. It involves assessing potential risks to individuals' rights and freedoms and may require the creation of new procedures or modification of existing processes.

1

2

Data Transfers

GDPR requires data controllers to ensure that personal data is adequately protected when it is shared or transferred to third parties. Controllers must ensure that such transfers are carried out only for lawful purposes, with appropriate safeguards in place, and in compliance with GDPR requirements, including contractual protections and security measures, to prevent unauthorized access or misuse of personal data.

Data Protection Officer

The DPO is responsible for informing and advising the organization and its employees about compliance with GDPR obligations, monitoring adherence to data protection requirements, and acting as a point of contact for supervisory authorities and data subjects.

Data Security

Organizations must implement appropriate technical and organizational safeguards to protect personal data from unauthorized access, misuse, or breaches, including those resulting from deliberate actions, as required under the GDPR.

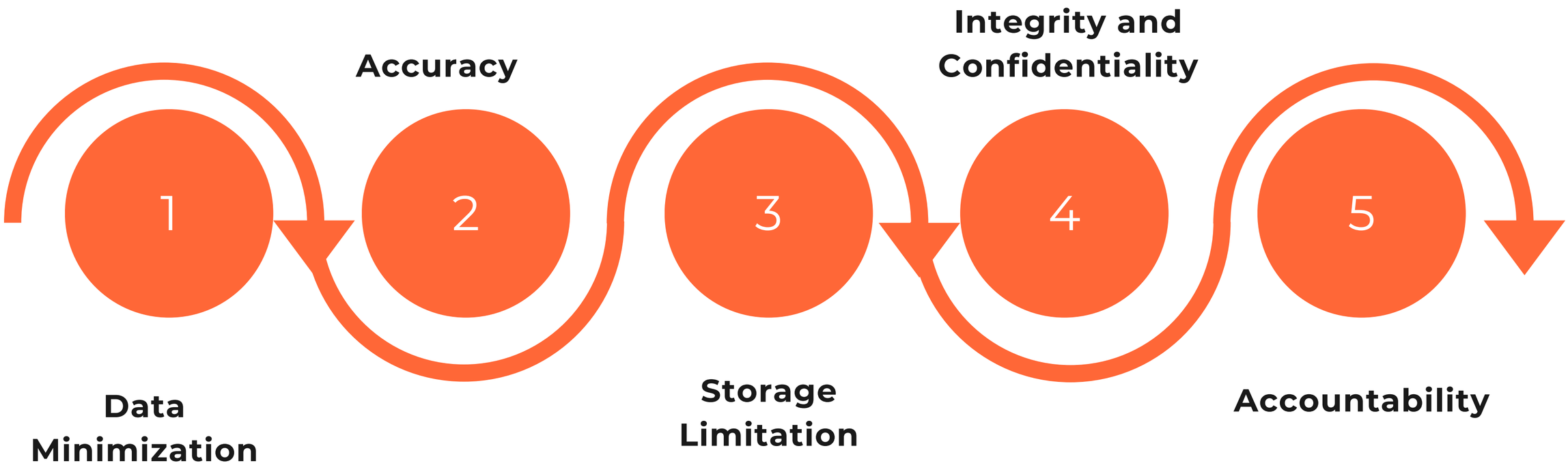
3

Awareness and Training

Organizations must ensure that staff members are adequately informed about essential GDPR requirements and their responsibilities in handling personal data. Regular training and awareness programs should be conducted to educate employees on the protection of personal data, secure data handling practices, and the importance of prompt identification and reporting of personal data breaches in accordance with GDPR obligations.

SALOT & SHAH ASSOCIATES

Core Principles



Rights of Data Subject

SALOT & SHAH ASSOCIATES

The General Data Protection Regulation (GDPR) grants several rights to data subjects, enabling them to exercise control over the collection, use, and processing of their personal data.

Section 1 Transparency and modalities

Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject

Section 2 Information and access to personal data

Article 13: Information to be provided where personal data are collected from the data subject
Article 14: Information to be provided where personal data have not been obtained from the data subject
Article 15: Right of access by the data subject

Section 3 Rectification and erasure

Article 16: Right to rectification
Article 17: Right to erasure (‘right to be forgotten’)
Article 18: Right to restriction of processing
Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing
Article 20: Right to data portability

Section 4 Right to object and automated individual decision-making

Article 21: Right to object
Article 22: Automated individual decision-making, including profiling

Section 5 Restrictions

Article 23: Restrictions

SALOT & SHAH ASSOCIATES

Obligations of Data Controller

Controllers must implement appropriate technical and organisational measures to ensure GDPR-compliant processing of personal data.

The measures implemented must take into account the nature, scope, context, and purpose of the personal data processing, as well as the potential risks of varying likelihood and severity to the rights and freedoms of individuals.

Controllers must be able to demonstrate compliance with GDPR (accountability principle).

Data Controllers are required to process personal data lawfully, fairly, and transparently. They must ensure that personal data is accurate, secure, and used only for specified and legitimate purposes. Controllers are obligated to obtain valid consent where required, respect the rights of data subjects, and implement appropriate technical and organisational measures to protect personal data from misuse, unauthorized access, loss, or data breaches.

Compliance may be demonstrated by adhering to approved codes of conduct (Article 40) or through approved certification mechanisms (Article 42).

Implemented measures should be regularly reviewed and updated where necessary.

Where proportionate, controllers should adopt data protection policies covering processing activities.

SALOT & SHAH ASSOCIATES

Consent Framework

Valid Consent

- Consent must be free, specific, informed, unconditional, and unambiguous.
- Given through a clear affirmative action (No pre-ticked boxes).
- Must relate to a specified purpose.
- Data Subject has the right to withdraw consent at any time.

Example: An individual manually opting-in to receive specific marketing newsletters by clicking a confirmation link sent to their email.

Consent Manager

- An authorized, independent platform for individuals to manage, review, and withdraw consent.
- Acts as a single-window interface for data subjects.
- Must be accountable and transparent in operations.
- Ensures compliance with technical standards.

Example: A corporate data portal where an employee can view all active data-sharing permissions granted to HR and Payroll systems.

Deemed Consent for legitimate use

- Voluntary data sharing
- Government Subsidies & Benefits
- National Security & State Functions
- Legal Obligations
- Judicial or Legal Compliance
- Medical Emergencies
- Public health response such as pandemic
- Disaster & Public order response

Example: First responders accessing blood group data during an accident rescue.

European Data Protection Board

The European Data Protection Board (EDPB) is an independent EU body with full legal personality under **Article 68** of the GDPR. It possesses the legal capacity to acquire or dispose of property, enter into contracts, and be a party to legal proceedings, acting through its Chair to ensure the unified enforcement of data laws across the Union.

The European Data Protection Board (EDPB) is an independent European body, established under the General Data Protection Regulation (GDPR), that serves as the central pillar of data privacy governance within the European Union. Its primary mission is to ensure that the GDPR is interpreted and enforced consistently across all Member States, preventing a fragmented legal landscape. Composed of the heads of national Data Protection Authorities (DPAs) and the European Data Protection Supervisor (EDPS), the Board acts as a collaborative hub where national regulators align their strategies. It is supported by a dedicated Secretariat that provides legal and administrative backing, ensuring the Board remains independent from any political or commercial influence.

Functionally, the EDPB plays a critical role through its Consistency Mechanism, which is triggered when data processing activities cross national borders. The Board is responsible for issuing binding decisions to resolve disputes between national authorities, ensuring that a company operating in multiple countries is not subject to conflicting rulings. Beyond dispute resolution, the EDPB is the primary source of official guidance, publishing comprehensive papers on topics such as the "Right to be Forgotten," data breach notifications, and international data transfers. For businesses, the EDPB represents the "Gold Standard" of compliance; by following its guidelines, organizations can achieve legal certainty and benefit from the One-Stop-Shop principle, which allows them to deal primarily with a single lead regulator while operating across the entire European Economic Area.

Independent Supervisory Authority

Each Independent Supervisory Authority is a public body established under **Article 51** of the GDPR, endowed with the legal personality and capacity required by national law to act as an independent enforcer. It possesses the authority to manage its own resources, enter into legal contracts, and be a party to judicial proceedings, acting through its head or board to ensure that data protection rights are upheld and enforced within its specific territory.

An Independent Supervisory Authority is a public body established by each EU Member State to monitor the application of the GDPR and protect the fundamental rights of individuals regarding their personal data. Central to their role is the principle of absolute independence; these authorities must remain free from any external political or commercial influence and cannot seek or take instructions from any government or outside entity. To support this independence, Member States are legally obligated to provide each authority with the necessary human, technical, and financial resources to perform their tasks effectively, which include promoting public awareness, advising national governments, and handling complaints from data subjects.

Beyond their advisory role, Supervisory Authorities possess extensive investigative and corrective powers to ensure strict legal compliance. They have the authority to conduct data protection audits, gain access to all personal data and premises, and issue formal warnings or reprimands to organizations. In cases of serious infringement, an authority can impose a temporary or permanent ban on data processing and levy significant administrative fines—reaching up to €20 million or 4% of a company's total global annual turnover. By collaborating through the European Data Protection Board, these national authorities ensure that while they operate locally, their enforcement remains consistent across the entire European Union.

SALOT & SHAH ASSOCIATES

- **Meta (Facebook): The Record Breaker (2023):** €1.2 Billion (The largest fine in GDPR history). Forced a complete overhaul of how transatlantic data flows are handled and accelerated the creation of the new EU-U.S. Data Privacy Framework.
- **Schrems II: International Data Transfers (2020):** The Court of Justice of the EU (CJEU) invalidated the "Privacy Shield" (the mechanism used to transfer data to the US). This led to the mandatory use of Transfer Impact Assessments (TIAs) for global businesses.
- **Amazon: Behavioral Advertising (2021):** Led to a €746 Million Fine. Clarified that even if there is no "data breach" (leak), the misuse or non-transparent processing of data is enough to trigger massive penalties.
- **H&M: Employee Privacy (2020):** €35.3 Million fine. Illegal surveillance of employees. Management recorded "Welcome Back Talks" after sick leave, capturing sensitive details about employees' family issues, religious beliefs, and medical diagnoses. A landmark case for Employee Rights, proving that GDPR protects individuals from intrusive monitoring by their employers.
- **Google: Transparency & Consent (2019):** Lack of transparency and valid consent for ad personalization. Information was "hidden" across too many menus, and consent boxes were pre-checked by default, led to €50 Million fine. Established that consent must be "unambiguous" and "affirmative." It ended the era of "silence equals consent" for digital tracking.

SALOT & SHAH ASSOCIATES

Penalties
Administrative Fines 2 Tiered System

Tier 1: Standard Maximum (Less Severe)

Fine: Up to €10 million or 2% of the organization's total global annual turnover of the preceding financial year, whichever is higher.

Applies to: Administrative and procedural failures, such as failing to integrate data protection "by design," not appointing a Data Protection Officer (DPO) when required, or failing to maintain records of processing activities.

Tier 2: Higher Maximum (Most Severe)

Fine: Up to €20 million or 4% of the organization's total global annual turnover of the preceding financial year, whichever is higher.

Applies to: Violations of core principles, such as processing data without a legal basis, violating data subjects' rights (e.g., right to erasure), or transferring personal data to countries outside the EU without adequate safeguards.

SALOT & SHAH
ASSOCIATES

THANK YOU!

Salot and Shah Associates

9328669060

www.salotandshah.com

503, 5th Floor, Phoenix Complex,
Opp New Girish Cold Drinks, Vijay X Roads,
to, Commerce Six Road, Navrangpura,
Ahmedabad, Gujarat 380009.

info@salotandshah.com