Introduction to PRIVACY

Data privacy outlines how we handle certain pieces of information/data while defining its relative importance. The need for comprehensive data security and privacy guidelines has never been more important than it is now. These guidelines have developed and evolved from the days where data was stored in file cabinets and physical folders primarily to today’s digital age that majorly uses electronic, online and cloud as storage platforms. Vital personal data that can be divided further into Personally Identifiable and Personal Health information (PII and PHI), includes financial data, social security numbers, credit card details, addresses, full names, medical records, etc. When data that’s meant to be private is leaked, misused or falls in the wrong hands, there can be dire consequences. Hence, it is all the more important for individuals and businesses to protect important related information and follow globally set principles to ensure data accuracy, safety and security.
The European Union General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) came into full force in May 2018 to strengthen and unify the protection of personal data.

The primary objective of this regulation is to allow for citizens to regain the rights and control of their personal data while simplifying the regulatory environment for international business by unifying regulations in the EU.
Preparation is Key

This new GDPR requirement will transform the methods in which data and technologies are designed and managed. The impact can involve storage, processing, access, transfer, and disclosure of an individual’s data records.

If the GDPR is not complied with, organizations will face significant reputational damage and fines that can be up to 4% of global turnover.
Why it Matters

GDPR is a step forward in harmonizing data and privacy regulations.

It gives personal data a broader definition and gives data subjects stronger rights.

It enhances transparency on data management and processing.

There will be higher penalties for non-compliance and organizations will be held accountable.

It has the potential to become the global standard for data governance.
The **Solution**

The goal is to create a secure and harmonized space for data, allowing users to become more aware of their personal data usage within the platform — where they can be educated about their data rights, how their data is being used and managed within the platform, and how users can manage their own personal data.

Users should be able to manage - **subscriptions, account removal, data transparency, downloadable data, and more...**
What You Need to Know

TO WHOSE DATA DOES THIS APPLY?

- Individuals
- Employees
- Company Owners

WHAT TYPE OF DATA?

- Sensitive Personal Data
  - Data which reveals: race, ethnic origin, political opinions, religion, health, sexual orientation
- Non-sensitive Personal Data
  - Data related to: name, date of birth, location data, identification number, transaction data
Data Processing

Data processing will become an even more critical task where any operation that involves personal data will need a governance process in place to keep the organization accountable for this data.

Apart from data collection, related operations will include - recording, collating, structuring, storing, adaptation or editing, retrieval, consultation and data usage. It also will include disclosure by transmission, dissemination or any other forms in which data can be made available.
Privacy Compliance
Data **Compliance**

**FRAMEWORK**

Prevent > Detect > Respond

**COMPLIANCE**

- Rules
- Standards
- Policies
- Requirements
- Regulations
- Transparency
- Law
Key Requirements of **Compliance**

- Consent
- Access
- Erase
- Security and Protection
Pillars of Compliance

**T**
- **Transparent Policies**
  - Notify users of data collection
  - Allow users to understand data is being processed
  - Provide processing details
  - Inform users of data retention and deletion

**I**
- **IT and Training**
  - Invest in privacy personnel and employee training
  - Enhance data policies
  - Secure a Data Protection Officer if the organization holds 250+ employees
  - Invest in a processor/vendor contract

**P**
- **Personal Privacy**
  - Users have the right to access all their data and manage it
  - Users can modify or remove data, if desired
  - Users can choose to opt-out of data processing
  - Users can export their personal data

**C**
- **Controls & Notifications**
  - Strict security requirements
  - Breach notification obligation
  - Appropriate consents for data processing
  - Confidentiality
  - Recordkeeping
Privacy Solutions
Defining Personal Data

Personal data is any information relating to an individual — private, professional or public.

It can be a name, home address, photo, email address, bank details, social network, medical information, or a computer’s IP address, browsing history, record logs, etc.
Data Accountability

Data controllers/data protection officers will now hold the responsibility to take every technical and organizational measure that is appropriate to ensure and demonstrate compliance.

MOVING FORWARD...

Analyze existing policies surrounding data security and protection as well as understand their effectiveness by monitoring and documenting policy implementation methods and using the right data lineage tools.

The goal is to establish unified management of data.
Platforms should aim to **provide and ensure data security as a priority** when data is acquired and ensure that it is **built into the core architecture and functionality** of the platform.

**MOVING FORWARD...**
Apply end-to-end encryption to reduce risk of data breach or loss.

When data is prompted within the platform, ensure users understand why the requested data is required and how it will be used.
Privacy by **Default**

GDPR and privacy management are complementary — privacy is not something that is added to an existing application, but it is built into the core architecture and functionality.

The platform will be accountable for the **protection** of the data the platform acquires.

**MOVING FORWARD...**

Establish a consistent and strong foundation of **data management and security** that will translate well over time.
Privacy Design
Personal Data & Data Management

Create legitimacy and bring awareness of personal data rights to users of the platform:
Design a destination for users to develop a better understanding of GDPR and their data by adopting a privacy-by-design approach across platform.

Creating transparency between users and the platform:
Educating users about the need and purpose of the data they share within the platform and why certain data is required, etc.

Allowing users to manage and exert their personal data rights:
Designing a destination for users to manage and have the choice to opt-out of certain personal details and data under account management.

Create a streamlined and consistent approach to data management:
By collecting data in the same manner through robust workflow and monitoring capabilities, potential personal data breaches are minimized.
Privacy Notices and **Consent**

Carefully consider how to construct privacy policies to provide more information about data management and protection as well as demonstrate that the GDPR requirements have been met.

- Provide detailed, clear, accessible and timely information to the client about the processing of personal data.
- Accountability principle must evidently be the guiding principle when it comes to organizing personal data.
- Demonstrate and ensure that consent was given by the user. For use of sensitive data consent must be explicit.
- Incorporate Privacy Impact Assessment within the overall framework and adjust policies to reflect the new regulatory requirements.

The goal is to provide education and clarity to the user.
Data FAQ

- Gives opportunity to build customer relationship.
- Brings awareness by educating users about GDPR and their data rights.
- Creates transparency between the user and the platform by explaining how data is used in the platform both for the user’s benefit and the product’s.
- Brings better understanding of how data security and management is executed.
- Establishes clear and concise data policies that will translate seamlessly to users as well as give them insight to the GDPR compliancy.
Security Notifications

Organizations should be prepared to notify users if suspicious activity has occurred that threatens personal data or if it has been breached.

By constructing and sending out a precautionary notification, users will be able to stay connected and understand what is happening to and with their data and can be involved with how to protect and prevent a security breach.

This creates transparency between users and the platform, allowing users to exert their personal data rights.
Manage **Profile**

**Users will have the ability to...**

- Manage general profile information
- Change password
- Manage notifications and subscriptions
- View, edit, and remove payment information and history
- Request to download and delete personal data and content
Data Privacy
Rules for Handling Data

Handle User Consent
Database Handling
Processing Confidential Data
Handling Consent

Platform will handle consent by following the below steps:

- Create consent database

- Platform will create an audit log of when consent was given and withdrawn and this will improve system accountability

- Platform will use a routine which purges data when consents are revoked

- Platform will share list of users to the partner who opted out of consent shall be provided to partners to purge the data

Expectations with Partners

- Review approach toward consent and accountability with data sharing partners

- Make sure each party has same level of compliance

- Partner must use the shared data for the same purpose for which the subscriber gave consent
Handling Consent

Platform will handle consent by following below steps:

**Individual / data subject / account owner:**
Person who authorized data flow with consent

**Data operator:**
Provides related services and enables digital consent management

**Data sources and data using services:**
Data source provides data about the Individual to the services that use this data (Data Sink). Same actor can be working as both Data Source and Data Sink

![Consent Flow](image)
Handling **Database**

- Platform will save private and sensitive data in restricted database and all other data can go in an unrestricted database. This will improve system accountability.

- Platform will perform anonymization or pseudonymization on the data in an unrestricted database and thus cannot be correlated with personal identifiers.

- Platform Infrastructure will provide access to individuals who are authorized to access restricted (private) data.
Handling Personal Data - PII

Personal data should be processed following the defined rules:

<table>
<thead>
<tr>
<th>Data Entry</th>
<th>Action</th>
<th>Type</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Anonymize (Hash)</td>
<td>String</td>
<td>ID shall be anonymized. Stored separately</td>
</tr>
<tr>
<td></td>
<td>Pseudomize (token)</td>
<td>Int</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Encrypt</td>
<td>Int</td>
<td>Shall be stored separately</td>
</tr>
<tr>
<td>Email</td>
<td>Encrypt</td>
<td>Int</td>
<td>Shall be stored separately</td>
</tr>
<tr>
<td>IP Address</td>
<td>Encrypt</td>
<td>Int</td>
<td>Add consent to keep IP addresses, stored separately</td>
</tr>
<tr>
<td>Physical Address</td>
<td>Encrypt</td>
<td>Int</td>
<td>Shall be stored separately</td>
</tr>
</tbody>
</table>

**Data Access:**

Analysis or work related to confidential data should be role based

**Data Purge:**

When subscriber revokes the content, data in the conditional access database is removed and consent database is updated
**Handling Personal Data - SPI**

Sensitive personal information should be processed following the defined rules:

<table>
<thead>
<tr>
<th>Data Entry</th>
<th>Action</th>
<th>Type</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethnicity / Race</td>
<td>Encrypt</td>
<td>String</td>
<td>Stored Separately</td>
</tr>
<tr>
<td>Health information (Physical/ Mental)</td>
<td>Encrypt</td>
<td>String</td>
<td>Stored Separately</td>
</tr>
<tr>
<td>Genetic Information</td>
<td>Encrypt</td>
<td>String</td>
<td>Stored Separately</td>
</tr>
<tr>
<td>Criminal Information</td>
<td>Encrypt</td>
<td>String</td>
<td>Stored Separately</td>
</tr>
<tr>
<td>Political Preferences</td>
<td>Encrypt</td>
<td>String</td>
<td>Stored Separately</td>
</tr>
<tr>
<td>Trade Union Membership</td>
<td>Encrypt</td>
<td>String</td>
<td>Stored Separately</td>
</tr>
<tr>
<td>Religion(s) or philosophical beliefs</td>
<td>Encrypt</td>
<td>String</td>
<td>Stored Separately</td>
</tr>
<tr>
<td>Sexual Preference</td>
<td>Encrypt</td>
<td>String</td>
<td>Stored Separately</td>
</tr>
<tr>
<td>Personal Photo and / or Video Data (including copies of Identity Cards / Driving License / Passports and equivalent that carry a picture of the individual(s))</td>
<td>Encrypt</td>
<td>String</td>
<td>Stored Separately</td>
</tr>
</tbody>
</table>
## Handling Personal Data - SFI

Sensitive financial information should be processed following the defined rules:

<table>
<thead>
<tr>
<th>Data Entry</th>
<th>Action</th>
<th>Type</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Balance on the account</td>
<td>Encrypt</td>
<td>String</td>
<td>Stored Separately</td>
</tr>
<tr>
<td>Transactional Information</td>
<td>Encrypt</td>
<td>String</td>
<td>Stored Separately</td>
</tr>
<tr>
<td>Financial Profile (Credit Rating)</td>
<td>Encrypt</td>
<td>String</td>
<td>Stored Separately</td>
</tr>
<tr>
<td>Salary / Income</td>
<td>Encrypt</td>
<td>String</td>
<td>Stored Separately</td>
</tr>
<tr>
<td>Credit Card Number / Direct Debit Card</td>
<td>Encrypt</td>
<td>String</td>
<td>Stored Separately</td>
</tr>
</tbody>
</table>
Handling Personal Data - SSI

Sensitive security information should be processed following the defined rules:

<table>
<thead>
<tr>
<th>Data Entry</th>
<th>Action</th>
<th>Type</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pin codes</td>
<td>Encrypt</td>
<td>String</td>
<td>Stored Separately</td>
</tr>
<tr>
<td>Private (Cryptographic) Keys</td>
<td>Encrypt</td>
<td>String</td>
<td>Stored Separately</td>
</tr>
<tr>
<td>User Authentication Questions</td>
<td>Encrypt</td>
<td>String</td>
<td>Stored Separately</td>
</tr>
<tr>
<td>User Biometric data (finger print, face, etc.)</td>
<td>Encrypt</td>
<td>String</td>
<td>Stored Separately</td>
</tr>
<tr>
<td>used to authenticate users</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal Signatures (of individuals) + Public</td>
<td>Encrypt</td>
<td>String</td>
<td>Stored Separately</td>
</tr>
<tr>
<td>Keys</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Case Studies for GDPR
GDPR @ Facebook

Transparency
Facebook’s upgraded Data Policies have been modified to include how personal data will be processed and will educate users as to when and how it happens. They plan to do this through in-product notifications and consumer education campaigns.

Control
Facebook will continue to allow users to control how their data is used and have launched a new user-friendly control center that will contribute to an easier and understandable experience for users.

Accountability
Facebook’s Privacy Policies explain their process on privacy and data protection. There is a team that solely works on this and assists in ensuring that compliance is documented. They also work on constantly improving the protection of personal information.
With the GDPR in place, Facebook has implemented some changes in their platform via the Settings page, where the user can go and modify their privacy settings. They also are shown the kind of data Facebook captures for them, with an option to download that information.

Facebook also has added the option for permanently deleting the account in that section under the user profile settings.
GDPR @ Google

Policy Updates
Google’s upgraded policies have been modified to include responsibilities held by Google Service users. Additionally, Google has clearly provided illustrations on how it collects, collates and stores user data and how can users access or delete it. The objective is to ensure users keep having granular control over their shared information while using Google’s services.

Contract Changes
Google has included a GDPR terms page to support and educate users about the contract changes applied to services such as AdWords, DoubleClick, and the Analytics suite. Users of such services must review and accept before continuing with the service.

Product Changes
To comply with GDPR, Google has implemented product changes across their publisher sites — giving publishers customization abilities including displaying and personalization or non-personalization.
GDPR @ Google

Google has taken the steps to implement GDPR by first introducing a privacy reminder to its users — known as the “Google GDPR popup” that would lead users to their privacy dashboard.

Within this privacy dashboard — users have the ability to manage multiple settings. Google has taken a strict consent-based approach to the GDPR implementation and risks.

They also provide the users with a list of various data elements that they collect and store.

Google’s Privacy Dashboard includes a variety of information that allows users to better understand their data, how it is used, and how they want it to be used.
**Policies & Compliance**

Banks have begun implementing GDPR by understanding what the basics are, by embarking on large data discovery projects and examining legal basis for holding data. These initiatives will contribute to their commitment in continually improving their policies and contracts — ensuring that data is properly protected, collected, and processed.

**Control**

Banks will return to their customers so that they can re-confirm consent to hold their data. By doing this, banks are educating and giving control to their users/customers.

**Data Processing**

Data processing activities are under review and are enroute for improvements to adjust to the GDPR requirements. By including a data processing officer — data can be more efficiently stored and secured in line with the GDPR Policy to ensure a sustainable compliance.
Key steps taken by the bank:
The bank has taken initiatives that demonstrate its commitment toward personal data protection. Going forward (as per GDPR guidelines), the collected/processed data will be held and used appropriately and this will be ensured through strict policies, checks, and compliance audits.

It has also established an organization-wide GDPR program that aims to cover its affiliates and subsidiaries. Subsequently, the bank is also looking at leveraging a system that will include multiple country compliance officers along with a global team of legal/privacy and compliance experts that will assure sustainable compliance with GDPR regulations.

How will it affect you as a client of the bank?
Under these regulations, customers can expect updates to certain data privacy provisions that will reflect the required changes. The bank will directly contact its customers in cases of revisions, updates or changes related to documentation that may be required to comply with GDPR norms.
<table>
<thead>
<tr>
<th></th>
<th>GDPR Checklist</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Have you done Data Privacy Impact Assessment?</td>
</tr>
<tr>
<td>2</td>
<td>Does your business have updated information along with a process that keeps data up-to-date?</td>
</tr>
<tr>
<td>3</td>
<td>Does your business need to appoint a Data Protection Officer?</td>
</tr>
<tr>
<td>4</td>
<td>Do you have details of all personal information, its source, what are doing with it and with whom is this data shared?</td>
</tr>
<tr>
<td>5</td>
<td>Do you hold any piece of personal data longer than necessary?</td>
</tr>
<tr>
<td>6</td>
<td>Do we have a defined policy on retention periods for all items of personal data, from customer, prospect and vendor data to employee data? Is it compliant with the GDPR?</td>
</tr>
<tr>
<td>7</td>
<td>Do you have a set plan and process in terms of data repository/stored location and data flow?</td>
</tr>
<tr>
<td>8</td>
<td>Do you have a data privacy policy (that now complies with GDPR norms) that is easily accessible for employees and related stakeholders?</td>
</tr>
<tr>
<td>9</td>
<td>Is your staff trained on data privacy to ensure proper compliance when it comes to handling data?</td>
</tr>
<tr>
<td>10</td>
<td>Does your plan include management/decision-maker education that helps them create awareness across all levels/verticals?</td>
</tr>
</tbody>
</table>
### GDPR Checklist (Continued)

<table>
<thead>
<tr>
<th></th>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>Don't Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>You have a formal agreement/contract with all partners, vendors, data processors and other related groups (with whom data is shared) outlining your data protection policies?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Have you updated your contracts with the above mentioned stakeholders as per GDPR regulations?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Do you regularly audit/review the data that you hold?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Do you adequately document internal processes?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Can your employees/customers/stakeholders easily request or gain access to their personal information?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Your customers/employees/stakeholders have control regarding edits, updates, profiling, processing rights and deletion of data that is related to them?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Can your customers/employees/stakeholders provide and/or revoke consent easily (under your data privacy policy)?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Are all policy updates are informed and communicated to existing customers/stakeholders/employees?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Your business regularly checks and reviews data policies for effectiveness, changes, updates in data handling and governance norms of countries/geographies where that data flows to?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>You report data leaks and breaches related to personal data (in case it happens) to concerned authorities and individuals involved?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
REFERENCES

Authors & Contributors

Diana Kearns-Manolatos
Sr. Director - Marketing

Ashish Nangla
Sr. Director - Software

Kapil Wadhawan
Asst. Specialist - Technology & UX

Ajay Sharma
Asst. Specialist - Technology

Sam Yeung
Jr. Associate

Nikhil Deshkar
Sr. Specialist - Technology

Aditya Seolikar
Sr. Manager - InsurTech Marketing

Saumen Das
Manager - UI/UX

Rakesh Patil
Sr. Manager - UI/UX