Repeat the pen-tester exercise done for the original design.

As our drive-sharing company decides to sell user data to advertisers, it's crucial to reevaluate our privacy and security measures. Using Imperva's penetration testing framework, we will evaluate the new risks introduced by this change and identify vulnerabilities that could lead to data breaches affecting not only app users, but drivers as well.

Therefore, for this analysis they will be based on regulations from The Council of the European Union, the General Data Protection Regulation (GDPR) this is a legislation to replace the Data Protection Directive. This has important repercussions for organizations dealing with personal data. In addition to enforcing one implementation for all EU member states and any organizations operating in them, it introduces substantial fines for violations.

Within this regulatory framework, certain privacy patterns are fundamental to compliance and ethical data management. These patterns, categorized into creation, maintenance, and upholding, form the backbone of our revised privacy strategy. They ensure not only adherence to European Union laws but also reinforce our commitment to protecting the personal data of our users and drivers.

CREATE

Creating Privacy Policy: Develop a legal document that clearly outlines privacy risks and the steps taken to mitigate them. For example, detailing how user data will be anonymized before being shared with advertisers.

Fair Information Practices: Implement principles like notice, choice, access, and integrity to ensure transparency and user control over personal data, aligning with FTC guidelines.

Respecting Social Organizations: Involve users in privacy policy creation through surveys or feedback sessions to better understand their privacy concerns and expectations.

MAINTAIN

Appropriate Privacy Feedback: Set up mechanisms like periodic privacy statements or alerts to inform users about data usage and collection practices.

Maintaining Privacy Policy: Regularly review and update privacy policies to reflect changes in data handling practices or legal requirements.

Privacy Management System: Implement a system where users can personalize their privacy settings, like choosing what data can be shared and opting out of certain data uses.

UPHOLD

Usage Control Infrastructure: Employ systems that track data flow and enforce policies on how data is used and shared, including real-time monitoring tools.

Distributed Usage Control: Implement controls that maintain data usage rules across various systems, ensuring consistent privacy protection even in complex environments.

Sticky Policies: Ensure that data shared with third parties adhere to the privacy policies under which they were collected, using contractual agreements and regular audits to prevent violations.

Likewise, for the pentesting analysis we will use the Imperva Penetration testing framework, so that it is also related to the data laws and regulations of the European Union (GDPR).

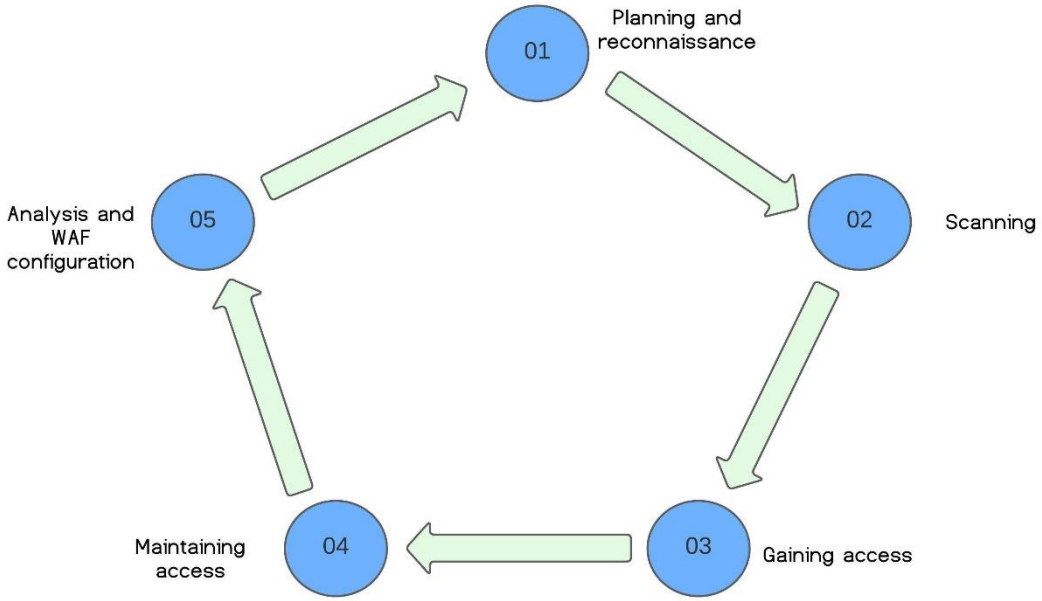

Image 1. Imperva Penetration testing framework

1. **Planning and Reconnaissance:**

   Include systems that manage data sharing with advertisers.

   Assess how user consent is obtained and managed, in line with GDPR requirements.

2. **Scanning:**

   Identify vulnerabilities in systems handling user and driver data for advertisers.

   Check API endpoints for compliance with GDPR's data protection principles.

3. **Gaining Access:**

   Test for GDPR compliance in access controls and data processing methods.

   Simulate attacks to evaluate the robustness of systems against unauthorized data access.

4. **Maintaining Access:**

   Examine the potential for sustained unauthorized access, a significant concern under GDPR.

   Assess systems' capabilities to detect and respond to prolonged breaches.

5. **Analysis:**

Evaluate the impact of breaches on GDPR compliance, particularly in terms of data sensitivity and unauthorized third-party access.

Strategies by Data Subject, Controller, and Authority

A subject control their personal data through the controller, who informs them about that data. The controller is involved in all strategies, including enforcing policies on any processors, also represented as the controller. It demonstrates compliance to the authority and applies data-oriented privacy risk mitigation strategies. These interactions are somewhat cyclic, as only the controller and or processor use them.

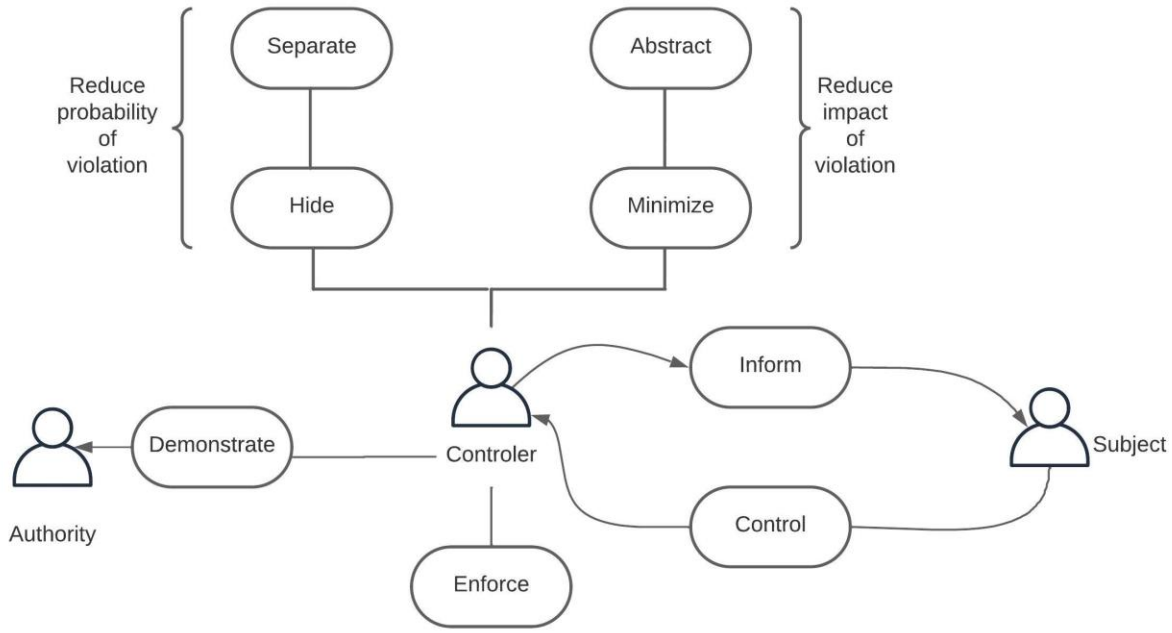

Image 2. Strategies by data protection legislation actors

Reduce Probability of Violation

Hide: This strategy involves techniques like data anonymization to prevent unauthorized parties from seeing or accessing personal data.

Separate: This strategy is about keeping personal data compartmentalized to prevent aggregation that could lead to privacy breaches.

Reduce Impact of Violation

Abstract: By presenting data in less detailed forms, such as aggregates or summaries, the strategy lessens the potential harm of data exposure.

Minimize: This ensures that only the necessary data for a specific purpose is used, reducing the amount of data that could be compromised.

Authority-Controller-Subject Interactions:

Demonstrate: The controller shows the authority that they are following the rules through audits and logs, ensuring accountability.

Enforce: The controller applies policies and controls to process personal data, upholding privacy standards.

Inform: The subject is kept informed about their data, enhancing transparency.

Control: The subject has control over their data, including consent and data management.

Risks Under the Role of User:

Unauthorized Access to Sensitive Data: GDPR categorizes certain data as sensitive. If an attacker gains user access, they could potentially obtain information about travel habits, personal preferences, and real-time location data.

Identity Theft (Phishing): Attackers could deceive users into giving away their credentials, breaching the GDPR's principle of integrity and confidentiality.

Risks Under the Role of Administrator:

Mass Data Exfiltration: An attacker with administrator privileges could extract vast amounts of data, violating the GDPR's data minimization principle.

Alteration of Privacy Controls: Malicious changes to privacy settings could facilitate unauthorized access or improper data processing.

Risks Under the Role of Developer:

Injection of Vulnerabilities: Developers may intentionally introduce vulnerabilities that can later be exploited to compromise the app.

Backdoors and Hidden Functionalities: Implementing features that bypass normal security controls, allowing future unauthorized access.

Methods of Attack to Provoke a Privacy Breach:

Brute Force and Password Spraying Attacks: Repeated login attempts to guess passwords, which can violate GDPR if it results in unauthorized access.

SQL Injection and Cross-Site Scripting (XSS): These attacks aim to exploit vulnerabilities in the app to access or manipulate data, potentially resulting in a GDPR violation due to inadequate protection of personal data.

Phishing and Social Engineering: Tricking users or employees into revealing credentials or confidential information, which could lead to a lack of data integrity and confidentiality.

Write an ethical analysis of the consequences of selling this data to adverstisers

Selling user data to advertisers involves a complex array of ethical considerations. Ethically, such actions could be seen as a breach of trust, as users typically do not expect their personal information to be commoditized. This is particularly sensitive when considering the principles of the GDPR, which prioritize user privacy and control over personal data.

GDPR Compliance:

Legality of Processing: The GDPR requires data processing to be lawful, fair, and transparent. The sale of data to advertisers must be based on a clear legal basis, such as the explicit consent of the users.

Principle of Minimization: The company should only sell the data necessary for the agreed purpose, avoiding the overexposure of personal data.

Right to be Forgotten: Users have the right to request the deletion of their data, which should be feasible even after the data has been shared with advertisers.

International Transfers: When selling data outside the EU, the company must ensure that advertisers comply with protections equivalent to those of the GDPR.

Ethical Obligations and Impact on Trust and Reputation:

In terms of trust and reputation, the way users and the public perceive the company can be significantly affected. Compliance with the GDPR and ethics in the management of personal data are essential to maintain user trust. Privacy violations and data misuse can lead to irreparable damage to a company's reputation and significant GDPR penalties.

User Autonomy: Selling data can undermine user autonomy, as users may not have real choice or control over how their data is used, especially if consent is not obtained transparently.

Data Misuse: There is also a risk that advertisers will misuse data, resulting in unwanted or intrusive targeting of people.

Discrimination: The potential for discriminatory practices may occur if data is used to select or exclude individuals from certain opportunities based on their data profile, demographic location, etc.

Transparency and Consent: The principles of the GDPR mandate that organizations collect data in a transparent manner and with the explicit consent of individuals, solely for specific, stated purposes. While not always mandatory, obtaining consent is the preferred method, as it empowers customers with actual oversight of their personal information.

Confidentiality and Anonymity: Customers often participate in data collection under the assumption that their information remains confidential. Organizations are advised to avoid collecting personally identifiable information (PII) whenever possible and to design data collection methods that protect the anonymity of the people and users.

Purpose Limitation and Data Minimization: GDPR supports the practice of purpose limitation, meaning organizations should not collect data with the intention of using it for undefined purposes at an undetermined point in the future. The principle of minimum viable collection encourages only gathering the data necessary to achieve the intended results or understand a trend, reflecting the data minimization principle.