MAPPING GUIDE

Imprivata FairWarning Mapping to GDPR

What is GDPR?

The General Data Protection Regulation (GDPR) is a set of European Union (EU) laws that change the way organizations collect, store, and transmit personal data of EU citizens. It gives control of personal data back to EU Citizens and applies to any company processing or handling EU citizen data, even if it is located outside of the EU. So, don't think of the GDPR as a fortress, but rather a network towards data privacy. It is now being enforced since May 25th, 2018. https://gdpr-info.eu

What is the purpose of GDPR?

GDPR should make it easier for EU citizens to understand how their data is being used, and also raise any complaints, even if they are not in the country where it is located. Thus, EU citizens have more control over their data.
What are the Penalties of Noncompliance?

What are the penalties of noncompliance?

- Fines up to €20 million or 4% of annual turnover, whichever is higher

What are key takeaways of GDPR?

- **Protect Personal Data at Rest or in Transit –** The GDPR defines personal data as anything that can be used to identify someone directly or indirectly; This includes identification numbers, location data, online identifiers, physical, physiological, genetic, mental, economic, or cultural/ social data of a person
- **Enable Data Breach Notification Requirement –** If personal data has been breached or compromised, organizations will be required to notify the Data Protection Authority within 72 hours
- **Fulfill on Rights of Data Subject –** The various rights data subjects (any person whose personal data is being collected, held, or processed) gain or maintain under the GDPR in regards to their data – organizations may have an obligation to fulfill such requests from data subjects

What are specific rights given to data subjects?

- **Right of Access –** Data subjects have the right to obtain electronic records as to how and where their data is being processed
- **The Right of Erasure or The Right to be Forgotten –** Data Subjects will have the right to request the erasure of their data, but only under the circumstances that it is no longer needed for its original purpose- you will have one month to respond to a request
- **The Right of Portability –** Individuals have the right to obtain and move/transfer data from one environment to another
- **The Right to Consent –** Consent must be given by the data subject to the controller in a lawful manner. It must be given in an explicit statement with free choice

How can I begin my journey to GDPR compliance?

- **First, conduct a Risk Assessment** to gain a comprehensive view of where your organization currently stands in relation to GDPR compliance
- **Appoint a Data Protection Officer** to drive the vision of your privacy posture and take ownership of communicating and organizing your new strategy
- **Identify and classify your current data.** You cannot adapt and govern your data if you don't know where and what it is
- **Prepare to fulfill the Rights of Data Subjects.** Implement a process for handling requests in regards to the right of erasure, data portability, etc
- **Implement privacy into your design and culture.** Not only will you need to advance and secure your existing technological systems, but you will also need to create a security-centric culture for team members

What are some questions I should ask myself while preparing?

- Will fines and consequences be worse if we don't properly protect our data?
- Do I have a proper security team in place?
- Where is all my data stored?
- Who has access to my data?
- How can I secure my IT Infrastructure?
- Do I have the tools in place to track access to data in the case of e-discovery, lawsuit or forensic investigation?
- Do I have the ability to locate the source and identify the scope of a data breach within the required 72 hour notification window?
- Do we have a system for reporting and proving compliance?

How does Imprivata FairWarning assist with GDPR compliance?

Imprivata FairWarning fulfills or partially fulfills upon the following articles for the General Data Protection Regulation:

Article 25	Article 32	Article 33	Article 34
Data Privacy by Design and by Default	Security of Processing	Notification of Personal Data Breach to the Supervisory Authority	Communication of a Personal Data Breach to the Data Subject

Section	Requirement	Control	Imprivata FairWarning Platform	Imprivata FairWarning Full or Partial Support
Article 25	Data Privacy by Design and by Default	Article 25 requires that data processing be limited to what is necessary given the purpose for which data is initially collected and be limited to those who need to access the data. It also requires the ongoing confidentiality and integrity of processing data processing systems and services.	Imprivata FairWarning assists its customers in regularly monitoring what information their users are accessing in each application. The Imprivata FairWarning platform can aid in determining who has accessed what (documenting) and provide evidence to support establishing and changing access control policies.	Full
Article 32	Security of Processing	Article 32 requires that Data Controllers and Data Processors implement technical and organizational measures that ensure data security presented by processing personal data. It also requires that they take steps to ensure that any natural person with access to personal data does not process data without instruction from controller, processer, EU Union law, or member state law.	Imprivata FairWarning assists its customers to regularly monitor what information their users are accessing. The Imprivata FairWarning platform can aid in determining who is currently accessing what, documenting and providing evidence to support establishing and changing of access control policies.	Partial
Article 33	Notification of a personal data breach to the supervisory authority	Article 33 requires that in the event of a personal data breach, data controllers notify the appropriate supervisory authority without undue delay and, where, feasible, not later than 72 hours after having become aware of it.	Imprivata FairWarning's platform provides monitoring for potential data breaches, incident response tracking and management. This assists customers in the prompt and orderly documentation of post-incident analysis, resolution mitigation and other activities.	Full
Article 34	Communication of a personal data breach to the data subject	Article 34 requires that if a data breach risks the rights and freedoms of affected data subjects then the data controller must, without undue delay, notify each affected person. The notification must be clear and in plain language to communicate the same information required in article 33	Imprivata FairWarning's platform helps in the investigation and determination regarding the scope of a data breach and identification of those affected. Imprivata FairWarning's platform also provides incident response tracking and management. This assists customers in the prompt and appropriate reporting and management of their security incidents.	Partial