YOUR GDPR COMPLIANCE JOURNEY WITH SALESFORCE SHIELD

This document contains information about certain EU General Data Protection Regulation (GDPR) provisions and does not provide legal advice. We urge you to consult with your own legal counsel to familiarize yourself with the requirements that govern your specific situation.

WHAT IS SHIELD?

Salesforce Shield (or "Shield") is a premium set of integrated security services offered at an additional cost and built natively on the Salesforce Platform. Shield lets customers see who is doing what with their confidential data, know the state and value of their data going back 10 years, and encrypt data at rest, while still preserving business functionality. It is declarative and can be set up through the standard administrative interface with point-and-click tools.

Shield can be added as a security enhancement to the "Salesforce Services," including Force.com (or Lightning), Sales Cloud, Service Cloud, and Community Cloud, along with Financial Services Cloud, Health Cloud, and Salesforce CPQ.

How can Shield assist customers in their journey toward GDPR compliance?*

While Shield is not required for customers to comply with the GDPR as part of their use of the Salesforce Services, Shield can be used to help a customer's overall compliance journey.

One of the key principles under the GDPR is that organizations must implement appropriate organizational and technical security measures to protect personal data (Article 5(1)(f), Article 32).

Organizational measures include training programs, policies, and procedures. Technical measures include user authentication and logical access controls.

Salesforce provides comprehensive security measures in our delivery of services, as described in our Security, Privacy, and Architecture documentation, such as incident management procedures and disaster recovery plans.

Additionally, Salesforce makes available to customers a comprehensive array of customer-controlled security features that can be used to heighten a customer's Salesforce deployment, such as multifactor identification and IP address whitelisting. Shield is an additional step customers may take to further heighten the protection of customer data.

* Please note that definitions used in this document are based on those included in the GDPR. For more information about the GDPR, please review Salesforce's GDPR website, which features a Trailhead providing a basic overview of European privacy laws and several white papers.

THERE ARE THREE KEY FEATURES OF SHIELD:

- PLATFORM ENCRYPTION
- EVENT MONITORING
- FIELD AUDIT TRAIL

These features allow Shield to assist customers with their obligations under the GDPR in several ways.

PLATFORM ENCRYPTION

What is it?

Platform Encryption lets customers encrypt sensitive data at rest while maintaining important application functionality. At its most basic level, encryption scrambles information so that only those people with the right decoder key can unscramble it. This offers an additional layer of security to the standard Salesforce Services offering (see Trust and Compliance Documentation). Because the Platform Encryption service is integrated in the application layer, key Salesforce application functionality can be made "encryption aware" and work with limited functional impact despite the data being encrypted (for further details, please see the Implementation Guide). Some partner applications on the AppExchange can (with permission) also include and use data that a customer chooses to encrypt within their organization. Platform Encryption is built natively into the Salesforce Platform and can easily be set up through the standard administrative graphical user interface (GUI) or through the application programming interface (API).

How can Platform Encryption help with GDPR requirements?

- Security Measures:
  While the GDPR is not prescriptive in stating what "appropriate" technical measures are, one example it does provide is encryption (Article 32(1)(a)). Salesforce offers encryption while data is in transit for most of its services at no additional cost to the customer. The addition of Shield offers the option of encrypting data while at rest, meaning that data is encrypted when it's inactive or being stored within Salesforce using an advanced key derivation system. Platform Encryption may be particularly beneficial in assisting with compliance under the GDPR for sensitive personal data (including personal data related to race, sexual orientation, health, etc.), which is likely to require a higher level of security due to the nature of the data secured.

- Personal Data Breach:
  Platform Encryption may be helpful in the event of a personal data breach where customer data is exfiltrated, no matter how big or small in scale. Under the GDPR, the controller may be required to notify the data protection authority and/or the individuals affected if the breach is likely to result in "a risk to the rights and freedoms" of the people involved (Articles 33 and 34). If the personal data involved in the breach is encrypted, it is less likely that the personal data will become visible to someone who shouldn't be seeing it, thus limiting the impact of the breach. Furthermore, the GDPR notes that communication to the data subjects will not be required if the controller has implemented appropriate technical and organizational measures, such as encryption, which render the personal data unintelligible to any person who is not authorized to access it (Article 34(3)(a)). As a result, encryption may further limit the scope of any potential embarrassment or further investigation into the incident.

salesforce

EVENT MONITORING

What is it?

Event Monitoring gives customers broad visibility into their Salesforce apps, letting them easily see what data users are accessing, from what IP address, and what actions they take with regard to that data. Features include tracking when a user changes ownership, refreshes a list, or exports valuable sensitive data. Customers simply access daily logs showing the activity for the past 30 days via APIs. In the event of a data leakage incident, customers will be able to access a series of logs that allow them to easily identify suspicious activity through analytics instead of manually going through thousands of rows of log data to spot the threat. In addition, Transaction Security, a customizable Event Monitoring feature, detects user actions, whether they involve logging into Salesforce from a second device or attempting to export a number of records. These actions can be evaluated in real time, based on predefined rules, allowing IT to detect unusual behavior and take immediate action.

How can Event Monitoring help with GDPR requirements?

- Security and Data Integrity:
  As described above, adequate security is important for ensuring that personal data is properly protected under the GDPR. In addition to encryption, the GDPR provides further examples of measures which may be "appropriate," including those which allow for "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and service" (Article 32(1)(b)). Event Monitoring allows customers to monitor log data and to quickly identify suspicious activity, assisting them in preserving the integrity of the personal data and their systems.
- Personal Data Breach:
  By being able to observe and quickly respond to any threats, Event Monitoring assists customers by allowing them to minimize damage and rapidly remediate the threat, thus limiting the scope of the impact on the data subjects. The Transaction Security feature allows customers to tailor their security profile to respond in real time to certain threats commonly faced by their organization. This helps customers to better enforce their policies, for example, by blocking the activity or by notifying a designated user of the unwanted activity.

FIELD AUDIT TRAIL

What is it?

Field Audit Trail gives customers a time machine so they can go back in time and see the changes to their data on any date, at any time. It expands what is currently available with Field History Retention, giving customers up to 10 years of audit trail data for up to 60 fields per object. Field Audit Trail is built for massive scalability and letting customers access audit data. Customers can also use this data to establish any relevant data retention policies.

How can Field Audit Trail help with GDPR requirements?

- Retention:
  Under the GDPR, one of the key principles is that personal data must only be retained for "no longer than is necessary" for the purpose of the processing, otherwise known as the "data retention" principle (Article 5(1)(e)). Field Audit Trail can assist customers with their data retention obligations by enabling them to develop data retention policies to ensure that personal data is not stored for excessive periods of time.
- Security and Data Integrity:
  As mentioned, the GDPR highlights that measures that allow "the ability to ensure the ongoing confidentiality, integrity, availability and resilience" of processing systems may be "appropriate" to secure certain personal data. In the event personal data is incorrectly modified or is lost, Field Audit Trail allows customers to retrieve a recent historical copy, thereby assisting them in ensuring the availability and resilience of their personal data.
- Accountability:
  The GDPR requires that organizations are able to demonstrate that they treat personal data in compliance with the law (Article 24). Field Audit Trail helps customers to achieve this by allowing them to confirm exactly what data the organization has held on the Salesforce Platform, and for how long.

HOW DO CUSTOMERS KNOW IF THEY NEED SHIELD?

Customers are responsible for determining how they will comply with the security and compliance obligations under the GDPR based on their individual circumstances.

While most Salesforce customers effectively secure their data using Salesforce's standard security features, some customers may decide they need to heighten their protection of data by using Shield. This analysis will depend on factors such as the customer's industry, regulatory requirements, internal compliance policies, and the nature of the data they process in Salesforce's services.