The European Union’s General Data Protection Regulation (GDPR), which went into effect on 25 May 2018, has significantly impacted legal requirements for organizations that control or process data, with major changes regarding the handling of personal data. These frequently asked questions and answers will help you understand **how SAP and SAP® Ariba® solutions can support your company in complying** with the new laws.

1. **Overview**

2. **SAP Commitment to Compliance**

3. **GDPR Definitions and Roles**

4. **SAP Ariba Compliance and Support**

5. **Personal Data Protection in SAP Ariba Solutions**

6. **SAP Data Protection Approach**
OVERVIEW

What is the GDPR?
In May 2016, the European Union (EU) adopted a harmonized data protection law called the General Data Protection Regulation (GDPR). On 25 May 2018, the GDPR went into force throughout all EU member states and in the European Economic Area (EEA). While the GDPR has not introduced many substantially new concepts, it has increased the compliance requirements for the handling of personal data substantially.

How does this impact your business? Where does the GDPR apply?
The GDPR applies not only to companies located in the EU, but also in situations where processing activities are related to goods and services offered to individuals located in the EU or where the behavior of individuals located in the EU is monitored, regardless of whether the processing activities take place in the EU or whether the individual is a EU citizen.

What are the penalties for noncompliance?
Organizations can be fined up to 4% of annual global revenue or €20 million for breaching the GDPR, whichever is higher. This is the maximum fine that can be imposed for the most serious infringements, such as not having sufficient customer consent to process data or violating the core of privacy by design concepts. There is a tiered approach to fines; for example, a company can be fined 2% for not having its records in order (GDPR Article 28) plus not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors, which means that cloud businesses like SAP Ariba that act as data processors for their customers are not exempt from GDPR enforcement.

SAP COMMITMENT TO COMPLIANCE

What stance does SAP take on the GDPR?
SAP is committed to complying with the GDPR as a company, and is also supplying technologies that support customers in GDPR compliance. SAP has been consistent in its approach to data protection as part of its general product standards, and this is now being extended to reflect the new requirements of the GDPR.
What are the roles of customers, suppliers, and SAP Ariba according to the GDPR?

**Data controllers:** GDPR Article 4(7) states: “‘controller’ means the natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data” (emphasis added). In general, the controller assumes responsibility for all personal data collected and must ensure that rights of the data subject and the controller’s own legal obligations are also covered by the processor.

- SAP Ariba customers are data controllers when they use SAP Ariba applications. SAP Ariba acts as data processor on behalf of the customer by means of the contract (such as the data protection agreement, service description, or statement of work).
- SAP Ariba suppliers are data controllers as they are fully responsible for the personal data entered in Ariba Network, for example by self-registration.

**Data processors:** GDPR Article 4(8) states: “‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller” (emphasis added). In general, this refers to data processing based on the instructions of the data controller as contracted.

- SAP Ariba as the cloud solution provider for customers and suppliers is the data processor for customers and suppliers (who are data controllers).

**Who is involved?**

Rights of the data subject...always applicable

The controller assumes responsibility for personal data collected, and must ensure that rights of the data subject and the controller’s own legal obligations are also covered by the processor.

- Data controller: SAP Ariba customer
  - Collection
  - Processing
  - Use

- Data processor: Supplier or service provider
  - Processing as contracted

- Data subject: Customer’s employee
  - Notification
  - Correction
  - Information
  - Erasure

- Rights: DP Agreement
  - Customer’s employee

- Subprocessor: Supplier or service provider

Data processors now have direct obligations, like controllers.
Controllers must maintain a record of processing activities, categories of data subjects, and categories of personal data.
Data processors must maintain a record of the processing categories on behalf of each controller.

Source: GDPR Article 30
What features and services does SAP Ariba provide to support compliance with GDPR?

<table>
<thead>
<tr>
<th>GDPR Aspect</th>
<th>Product Functionality or Technical Feature</th>
</tr>
</thead>
</table>
| Information/ Transparency    | • Display of personal data is available.  
• Records of processing activities are aligned to GDPR requirements.  
• Privacy impact assessments (PIAs) are conducted for new products/services (innovations) and product/service changes in the release cycle.  
• Changes to personal data and privacy settings are logged. |
| Access to data                | Personal data can be accessed only by a user who has been authorized by the SAP Ariba central authentication and authorization mechanisms.                                                                                             |
| Rectification of data         | Personal data can be corrected by an authorized user, such as the customer’s administrator.                                                                                                                                               |
| Erasure of data               | Data will typically be erased at contract termination; individual personal data deletion is implemented by using anonymization/obfuscation.                                                                                                   |
| Restriction of processing     | Restriction of data processing at the transaction level is not currently implemented; user-level deactivation is available to customer administrators.                                                                                         |
| Data portability              | Data portability via export to comma-separated values (CSV) files is available to customer administrators.                                                                                                                               |
| Data breach notification      | Notification is currently implemented by utilizing the existing security incident process.                                                                                                                                                 |
| Privacy by design and by default | SAP Ariba product development follows the SAP guiding product standard security requirements. Additional privacy principles are applied in the design phase, such as the practice of minimized personally identifiable information (PII) data collection. Default settings are set to the maximum restriction. |
| Consent                       | Consent is given by actively accepting the SAP Ariba Privacy Statement (which includes the purpose, the categories of personal data, and other relevant considerations).                                                                     |
Which technical and organizational measures (TOMs) for security are in place?

SAP Ariba as a data processor supports appropriate TOMs in terms of accountability and technology by maintaining records of processing activities, conducting privacy impact assessments, and incorporating privacy by design and default within product cycles.

<table>
<thead>
<tr>
<th>Security Goal</th>
<th>Product Functionality or Technical Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical access control</td>
<td>SAP Ariba policies and controls are in place that are regularly assessed in audits.</td>
</tr>
<tr>
<td>Authentication and authorization</td>
<td>Industry-standard authentication and authorization features are implemented that are regularly assessed in audits.</td>
</tr>
<tr>
<td>Disclosure control</td>
<td>Access to PII can be regulated by the customer and is role based.</td>
</tr>
<tr>
<td>Change control</td>
<td>Logging of changes to personal data is implemented in most parts of the product.</td>
</tr>
<tr>
<td>Transmission control</td>
<td>All internal and external communication is encrypted. A data transmission policy is in place.</td>
</tr>
</tbody>
</table>
| Job control                  | • Customer facing: data is processed according to clear regulations in the customer contract (such as the data protection agreement and service descriptions).  
  • Subprocessor facing: standard corporate master data protection agreement (MDPA) and data protection questionnaire (DPQ) are used, plus service-specific statements of work (SOWs) that regulate data processing. |
| Availability control         | Accidental destruction or loss is avoided by established backup, disaster recovery, and business-continuity mechanisms that are regularly audited.                                      |
| Data separation              | SAP Ariba only collects personal data for the purpose specified in the SAP Ariba Privacy Statement. Customer data is strictly separated in the SAP Ariba data and application architecture. |
PERSONAL DATA PROTECTION IN SAP ARIBA SOLUTIONS

What type of personal data is processed within SAP Ariba solutions? Are special categories of personal data involved?

SAP Ariba products and services support the business-to-business market sector. As such, when SAP Ariba collects information about an individual (that is, personal information), it is generally only related to that person’s role at their company, and is not related to them as a private person or as an individual consumer. SAP Ariba solutions contain simple business contact information about individuals, such as:

- E-mail address
- Employee number
- Employee name
- Business phone
- Business fax
- Alternate e-mail addresses
- Business postal address

The SAP Ariba Privacy Statement prohibits the use of SAP Ariba solutions for processing special categories of personal data (often called “sensitive data”).

Where is personal data stored, and what are the SAP Ariba safeguards?

SAP Ariba has 13 data centers across the world that offer the following support:

- Customers have the option to run applications, such as those in the SAP Ariba Procurement portfolio, in several regional data centers.
- Personal data of the customer’s users is administered in the selected application data center.
- Supplier profiles are stored in the Ariba Network data center operated in the United States (US).
- Most SAP Ariba applications exchange data with Ariba Network to facilitate communication with suppliers; the exchange can include personal data, such as contact information on a purchase order.
- The data exchange between regional data centers and Ariba Network is provided exclusively over industry-standard encrypted connections.

What security measures are used for data transfer between the US and EU?

Transfers of personal data between the US and EU are based on the EU standard contractual clauses (SCCs) that according to the GDPR are approved as appropriate safeguards. This provides for a lawful mechanism of transferring personal data outside the EEA and forms a legally binding agreement between the SAP global entities establishing requirements for a baseline protection of personal data.
SAP DATA PROTECTION APPROACH

SAP has unified the approach for all SAP Cloud solutions with the data protection agreement (DPA):

• The DPA goes beyond SCCs in providing privacy assurances.
• The DPA incorporates an unmodified version of SCCs which controls in case of conflict with the rest of the DPA.
• The DPA defines specific terms – for example, SAP as “processor” and “importer,” the customer as “controller” and “exporter.”
• Customer headquarters (HQ) can sign the amendment on behalf of their EU affiliates; affiliates may sign an accession document with HQ and be considered parties to the clauses.
• SAP has intercompany agreements with SAP affiliates and data processing agreements with partners (subprocessors).
• The DPA lists data protection policies, procedures, standards, and certifications.
• The DPA describes rights and obligations with respect to technical and organizational measures (such as monitoring, incidents, and notifications).
• SAP Ariba data privacy measures are aligned with the SAP Data Protection and Privacy office.

Does SAP have a data privacy officer? Yes; SAP has a designated data privacy officer representing the company according to GDPR requirements.

Learn more

For additional information about the GDPR, you can access the SAP Trust Center, explore GDPR-related documents on the European Commission web site, or review the handbook on European data protection law. For specific questions relating to your account and any existing SAP Ariba agreements or contracts, please contact your representative.