Meeting the GDPR Mandate
How SAP and SAP® Ariba® Solutions Can Support Your Organization’s Compliance with the GDPR
Table of Contents

4 Introduction
5 Objectives
5 Material Scope
5 Territorial Scope
6 Key Provisions
8 Role of SAP Ariba Solutions and Services
The General Data Protection Regulation (GDPR) adopted by the European Union has introduced a wide array of new legal requirements for organizations that control or process data, with the most significant changes impacting the handling of personal data. With the launch of this legislation, companies worldwide are focused on ensuring that they meet the requirements.

This paper is designed to help you better understand the overall implications of the GDPR, how the changes it mandates affect your business, and what support you can expect from SAP and SAP® Ariba® solutions to help your business maintain compliance.
I. Introduction

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. While the GDPR has not introduced many substantially new concepts, it has increased the compliance requirements of data controllers and processors substantially regarding their handling of personal data.

As a company, SAP is committed to ensuring compliance with the GDPR. SAP has been consistent in its approach to data protection as part of its general product standards, and this has now been extended to reflect the new requirements of the GDPR.

To assist customers’ compliance efforts, SAP has set out a summary of the changes introduced by the GDPR, the implications of these changes, and how SAP product features can help customers to meet GDPR requirements.

As part of SAP, SAP Ariba is taking a proactive approach to assist customers in complying with the GDPR, and the second half of this white paper outlines specific SAP Ariba solution capabilities and support available to help them do this.

The information contained in this paper is for general guidance only and provided on the understanding that SAP is not herein engaged in rendering legal advice. The responsibility to adopt appropriate measures to achieve GDPR compliance rests with the customers as controllers in terms of the GDPR, and SAP accepts no liability for any actions taken as response to this white paper. As such, it shall not be used as a substitute for legal or professional consultation.
II. Objectives

The GDPR aims to harmonize data protection requirements across Europe into one single regulation. It addresses corporate bodies governed by public and private law in their capacity of either controller or processor. The new law aims to protect the rights and freedoms of natural persons, to enhance data subjects’ confidence in organizations that hold or process their personal data, and to strengthen the EU’s internal market. To this end, the GDPR provides a uniform set of rules to govern the processing of personal data throughout the EU. The degree of EU-wide harmonization achievable by the GDPR is, however, restricted to the extent that the regulation contains so-called opening clauses that allow EU member states to set out country-specific laws and requirements for specific data processing activities. These opening clauses therefore may result in applying additional rules and obligations for data controllers and processors, but not changing or altering the original regulation.

III. Material Scope

The GDPR has a broad material scope covering the processing of personal data by automated means or in other structured form, including those intended for part of a filing system. This distinction becomes clear as the GDPR states that it does not apply where natural persons process personal data exclusively during a purely personal, private, or household activity.

IV. Territorial Scope

Likewise, the GDPR has a broad territorial scope and applies to any activities of a data controller or processor in the EU that comprise the processing of an individual’s personal data. Central to this is whether the controller or processor is located in the EU. The GDPR also applies to controllers or processors located outside the EU where the processing serves to offer goods or services to data subjects who reside in the EU or to monitor the behavior of data subjects who reside in the EU.
V. Key Provisions

The GDPR has introduced several new legal requirements that may substantially affect a controller’s or processor’s business. Therefore, each controller or processor must verify which GDPR obligations apply to them and must also ascertain how to implement them accordingly.

GENERAL PRINCIPLES
In accordance with its general processing principles, the GDPR requires the processing of personal data to be lawful, proportionate, transparent, adequate, accurate, secure, confidential, limited in time and to designated purposes, and conducted in a responsible and accountable manner (which means applying appropriate security – including technical and organizational measures – to ensure integrity and confidentiality).

PERSONAL DATA
The GDPR explicitly defines what it means by the term personal data: any data that relates to an identified or identifiable individual. GDPR Article 4(1) states: “an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.” The term clearly includes metadata or other associated data such as IP addresses, cookies, or other identifiers – also a combination of such data – that may trace back to an individual. The GDPR has broadened the known catalog of special categories of personal data to include genetic data, biometric data if used to uniquely identify a natural person, and data related to criminal convictions and offenses.

LAWFULNESS
Processing personal data is lawful only if one of the criteria for permission, as set forth in the GDPR, is met. In the absence of direct legal allowance, organizations need consent from individuals whose data is to be processed. This consent must cover all purposes for which the organizations (intending to process the data) collect and process the data and must allow for the individual’s right to withdraw consent at any time. This means that blanket consent or global consent for various unspecified purposes is not valid for the processing of personal data.

ACCOUNTABILITY
The GDPR aims to improve accountability of those processing personal data and increase transparency of the data being processed. Despite its similarity in substance and structure to the previous EU Directive, the GDPR takes a much tougher line in helping enforcement. Penalties for noncompliance are remarkably high, including administrative fines of up to 4% of annual global revenue or €20 million, whichever is greater, and with potential damage claims and other legal liability risks designed to incentivize companies to enhance internal structures and processes to comply with the regulation.

DATA PROTECTION BY DESIGN AND BY DEFAULT
Under the terms of the GDPR, privacy must be built in deliberately and be adopted by default in both systems and processes. Organizations are obliged to ensure that the processing of personal data is for a specific purpose, and organizations must demonstrate that data protection is at the heart of their IT framework and solution design.
TECHNICAL AND ORGANIZATIONAL SECURITY
These bodies are also obligated to implement all necessary technical and organizational measures (TOMS) to ensure a level of security appropriate to the risk of the processing for the data subjects. It is therefore necessary to analyze the organization’s internal IT asset and process landscape to identify and map data flows that include personal data. This helps to ascertain the appropriateness of the security framework.

DATA SUBJECT RIGHTS
Guided by the concept that the individual should know and always be able to identify what personal data is processed, by whom, for what purposes, and over what time period, data controllers need to actively provide certain general and specific information; this is in accordance with the GDPR’s revised concepts of data portability and the individual’s rights to access, to refuse/object, or to be forgotten. Organizations involved in processing personal data therefore require robust internal processes with designated roles.

DATA GOVERNANCE
Organizations must implement a host of systemic measures to reduce the risk of violation – as data controllers, customers must demonstrate to the data subject and to regulators that they comply with the applicable regulation, and as data processor, SAP must demonstrate the same to customers. Complexity grows when bodies need to keep track of every purpose for which personal data is being processed and when they need to ensure that all individuals have given their consent for each data processing use case. These measures must be built into existing IT infrastructures. Depending on the outcome of a company’s data protection risk assessment, measures such as the appointment of a dedicated data protection officer, the execution of privacy impact assessments, and the adoption of regular audit procedures help to maintain compliance.

BREACH NOTIFICATION
This is when something goes wrong – when the internal organizational measures have not prevented a data breach, or the processing of personal data has been found to be outside lawful purpose. In the event of a data breach, data controllers need to notify the supervisory authority and the affected individuals within 72 hours of becoming aware of the situation. Data processors need to inform data controllers without undue delay after becoming aware of a personal data breach.

Organizations are obligated to ensure that the processing of personal data is for a specific purpose, and they must demonstrate that data protection is at the heart of their IT framework and solution design.
VI. Role of SAP Ariba Solutions and Services

SAP Ariba solutions help customers to achieve GDPR compliance in multiple ways. For example:
• SAP Ariba solutions support managing and protecting employee and supplier data, including data accessibility and visibility, so the customer’s procurement and supply chain teams can focus on getting business done.
• With SAP Ariba, the customer can strengthen and protect critical collaboration with their suppliers, managing everything from sourcing to financing.
• SAP Ariba supports the organization’s accountability, security, and data protection demands.

Data controller: GDPR Article 4(7) states: “‘controller’ means the natural or legal person, public authority, agency or any other body which determine the purposes and means of the processing of personal data” (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).

Data processor: 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 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 SOLUTIONS AND PERSONAL DATA
• Categories of personal data: SAP Ariba solutions only process simple business contact information of individuals as users or business contacts, such as their e-mail address, employee number, employee name, business phone, and postal address.
• Special categories of personal data: The SAP Ariba Privacy Statement prohibits use of the solutions for processing special categories of personal data.
• Cross-border data transfer: SAP Ariba maintains data transfer agreements with SAP/SAP Ariba affiliates and subprocessors that comply with the EU requirements for cross-border personal data transfer. These agreements are based on the EU standard contractual clauses that are equally compliant under the GDPR to ensure an adequate level of data protection in case of data transfers to third countries outside the EU.
• Encryption: Personal data is encrypted on the storage level, all external communication is encrypted, and the corresponding security policies are in place.

GDPR ROLES AND DEFINITIONS RELATING TO SAP ARIBA SERVICES

Data controller: GDPR Article 4(7) states: “‘controller’ means the natural or legal person, public authority, agency or any other body which determine 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 the 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.
HOW SAP ARIBA SUPPORTS CUSTOMERS AS A DATA PROCESSOR

• SAP Ariba implements 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.

• SAP Ariba adheres to SAP’s unified approach for all cloud solutions by applying the data protection agreement as a substantial part of the customer contract, which incorporates standard contractual clauses to provide data protection assurances to customers.

• SAP Ariba employees are required to annually pass data protection and privacy/security awareness trainings that cover privacy principles and security topics.

• SAP is committed to helping customers understand how SAP Ariba solutions protect the confidentiality, integrity, and availability of their data and provide ongoing accountability by proactively publishing information about SAP Ariba certifications and attestations, data processing agreements, real-time cloud solution availability, and similar areas in the SAP Trust Center.

SAP ARIBA SOLUTION FEATURES TO SUPPORT GDPR READINESS

• Consent: SAP Ariba solutions capture user consent and acknowledgement of privacy notices before allowing use by new users. This includes, for example, the purpose of processing and the categories of personal data being processed. SAP Ariba is reviewing integrated consent mechanisms such as customer-configurable privacy statements. Solutions also support self-service opt out, so recipients can unsubscribe to unwanted communications such as e-mail notifications.

• Right to be forgotten: Buyer-facing solutions put user and role management in the hands of the customer administrator. SAP Ariba is also reviewing features for personal data deletion and retention, such as personal data deletion and anonymization. In any case, general customer data deletion is performed upon contract termination.

• Right to rectification: SAP Ariba solution users can edit or correct their personal data in user profiles within the system at any time.

• Transparency: SAP Ariba solutions provide visibility to a user’s personal data and preferences. SAP Ariba is also reviewing administrator fea-
Meeting the GDPR Mandate

Features to support export of user data in a standard format and a comfortable view of change logs.

- **Authorization and disclosure control:** SAP Ariba solutions allow customers to manage authorization, authentication, and role-based access for employees, contractors, and third parties. Detailed ticketing and workflow features help new SAP Ariba administrator users to adapt user access to changing roles and manage inactive users.

- **Privacy by design and by default:** SAP Ariba product development follows SAP’s guiding product standard security requirements. Additional privacy principles are applied in the design phase, such as the practice of limited personal data collection. Default settings are set to the maximum restricted, covering:
  - Personally identifiable information (PII) erasure upon contract termination and on demand
  - Consent to privacy notice (customizable)
  - Logging on at the field level and access to logs
  - PII visibility, editing, and portability
  - Configurable retention time and restricted processing
  - Self-service opt in–opt out and logging
  - Industry standard data access, authentication, authorization, and encryption mechanisms

**SAP Ariba Services to Support GDPR Readiness**

- **Data breach notification:** In case of a personal data breach, SAP Ariba services provide full support for obligations to notify of data breaches without undue delay. SAP Ariba offers an end-to-end process from the recognition of a breach up to the customer notification.

- **Data subject rights:** SAP Ariba services support the customer in privacy-related questions and provide assistance when customers have an obligation to respond to an individual’s exercise of rights or for obligations regarding the security of personal information.

- **Transparency:** SAP Ariba services support customers in fulfilling their obligation to keep records of processing activities by providing the SAP Ariba component in full compliance with the GDPR requirements for data processors. SAP Ariba also conducts data protection impact assessments (DPIAs) for new products/services (innovations) and regular product/service changes in the release cycle.

- **Accountability:** SAP Ariba provides assurance through ongoing accountability activities such as regular certification, risk assessment, and security assessment of applications, network, and IT infrastructure; documented security programs and policies; and regular security trainings.

- **Subprocessor compliance:** SAP Ariba ensures ongoing subprocessor compliance by subprocessor contract vetting and assessment of security risks using SAP corporate standard purchasing processes, including data protection agreements that regulate personal data protection. A list of approved subprocessors is regularly provided and updated for customers.
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.