SAP Global Data Protection and Privacy Policy

Version 2.1
May 2017

Public
This attached Policy is provided to you as an information only. It shall have no binding effect on SAP or SAP course of business. SAP reserves the right to change the Policy at any time without giving notice.
This page is intentionally empty in the PUBLIC version of the SAP Global Data Protection and Privacy Policy. Additionally, the annexes with internal content are not provided.
1. Introduction

SAP is bound by data protection and privacy laws. SAP respects and protects the rights of individuals, in particular the right to data protection and privacy during the processing and use of information as well as the right to privacy. The protection of information comprises the personal data of employees, applicants, customers, suppliers, partners, and all other persons within the SAP area of responsibility. To adhere to this obligation, SAP has adopted an SAP Global Data Protection and Privacy Policy (Policy) and reviews it regularly.

The Policy outlines a group-wide minimum standard for handling personal data in compliance with data protection and privacy laws. It defines requirements for all operational processes that affect personal data, as well as clear responsibilities and organizational structures. As soon as a process at SAP involves collecting, processing, or using personal data, the provisions of this Policy are to be adhered to. Management of the individual SAP group companies and the relevant process owners are responsible for ensuring that all processes – during which personal data is collected, processed, or used – are designed such that the provisions of this Policy are fulfilled. It is the duty of all SAP employees to comply with the provisions of this Policy when handling personal data in their daily work for SAP.

SAP is a global company with headquarters in Germany, a member state of the European Union (EU). Therefore, the basic principles established through this Policy are based on the requirements of European data protection and privacy legislation. If, on a case-by-case basis, applicable local law outlines stricter data protection and privacy requirements than this Policy, personal data must be handled in compliance with those stricter laws. Additional standards and/or guidelines within the SAP group that are issued as a result of this Policy must also take the applicable law into account in this respect. Questions on applicable law can be directed to the Data Protection and Privacy Office (DPPO) (privacy@sap.com) and/or the appointed data protection and privacy coordinator (DPPC).

Data protection and privacy rights of employees must be guaranteed in accordance with the law of the country in which the employment contract with the respective SAP group company was concluded, notwithstanding the local law of the country in which the employee data is processed or used. The legal responsibility for collecting, processing, and/or using the personal data of SAP employees always lies with the respective employer. It is the employer’s duty to inform other SAP groups companies (for example, if the manager is an employee of a different SAP company), if within the scope of processing and using personal data for their employees, different provisions apply for the protection of personal data from those defined in this Policy.

This Policy shall not restrict the right of SAP to use employee personal data to the fullest extent legally possible in order to preserve its position during any legal action or official proceedings. However, the applicable data protection and privacy law must be observed by SAP generally.

2. Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymized data</td>
<td>Data in a form that makes the direct or indirect identification of an individual person impossible, even with the aid of other data or information.</td>
</tr>
<tr>
<td>Anonymous data</td>
<td>Anonymous data does not have any reference to a person when it is collected. Anonymous and anonymized data is no longer subject to the internal or external data protection and privacy regulations.</td>
</tr>
<tr>
<td>Commissioned data processor</td>
<td>A natural or legal person, authority, institution, or any other office that processes personal data on behalf of the data controller, for example, an external company or an SAP company that is not the data controller itself.</td>
</tr>
<tr>
<td>Special categories of personal data</td>
<td>Contain data on the racial or ethnic origin, political views, religious or philosophical beliefs, union membership, felonies, penal convictions, health, or sexual preferences of persons, as well as data that can be misused for identity theft. For example, social security numbers, credit card and bank account numbers, as well as passport or driver’s license numbers.</td>
</tr>
<tr>
<td>Person affected</td>
<td>An identified or identifiable natural person whose personal data is affected by a data processing action. A person is deemed identifiable if he or she can be identified directly</td>
</tr>
</tbody>
</table>
Data processing actions
(collecting, processing, and/or using)

Collecting means procuring data on the person affected. Processing describes any operation performed with or without the aid of an automatic procedure, or any set of operations connected with personal data, for example, collecting, saving, modifying, storing, changing, transferring, locking, or deleting personal data. Using means any usage of personal data, except for processing.

Third party

A natural or legal person, authority, institution, or any other office, except for the following:

- The person affected
- The office responsible
- The commissioned data processor
- The persons who, under the direct responsibility of the data controller or the commissioned data processor, are authorized to process the data

For the purposes of this Policy as well as applicable data protection and privacy laws, different companies within the SAP group are classified as third parties in relation to each other.

Consent

This may be explicit or implicit. Explicit consent generally requires an action by the person affected, through which they allow the processing of data – for example, the declaration of consent with the sending of e-mails or entering of personal data (opt-in). Explicit consent granted without duress is deemed to be the legal basis for the processing of personal data, provided no other legal provision is in force. Implicit consent (for example, opt-out) allows processing provided the person affected does not object.

Deletion

Either the physical destruction of data or the anonymization of data in such a way that makes it impossible to relate the data to a natural person.

Personal data

All information on an identified or identifiable natural person (person affected). A person is deemed identifiable if he or she can be directly or indirectly identified – in particular, by reference to an identity number or to one or more factors specific to that person's physical, physiological, psychological, economic, cultural, or social identity.

For example, persons can be identified directly on the basis of names, telephone numbers, e-mail addresses, postal addresses, user IDs, tax numbers, or social security numbers, or indirectly on the basis of a combination of any information. Personal data that is subject to this Policy includes data on employees, applicants, former employees, customers, interested parties, suppliers, partners, users of SAP Web sites and services, and any other persons. The data may be contained in an SAP system, or in systems of third parties that operate these on behalf of SAP. Customer systems – that SAP or third parties on behalf of SAP operate – are also relevant – as are systems operated by customers themselves if SAP employees can access the personal data stored in these systems while providing services, support, or consulting services.

SAP

SAP SE and its global offices and subsidiaries and 'affiliates' as defined by the German Stock Corporation Act (AktG), article 15 ff.

Data controller
(controller)

A natural or legal person, authority, institution, or any other office that – either alone or in collaboration with others – makes decisions on the purposes and means of processing personal data (general legal definition). In the case of SAP, an SAP company is always the controller for the personal data of its employees, customers, suppliers, partners, or other persons. SAP employees, internal units, or organizations cannot be controllers. The controller is represented by the management legally
3. Basic Principles of Protecting Personal Data

During every process that includes collecting, processing, or using personal data, personal data may be processed or used only in accordance with this Policy and to the extent permitted by law.

Processing is only allowed in the following cases:

- If a person affected freely gave their consent, for example, when registering on a Web site
- If required to fulfill contracts with the person affected, for example, for an employment contract or a service contract
- If legally required or permitted, for example, due to tax or social security laws.

Personal data may be collected and processed for lawful purposes only. The respective purpose must be defined before the time at which the data is collected. Processing for a purpose other than the one defined before the data was collected is permitted in exceptional circumstances only if the person affected consents to the processing or if stipulated by law.

Personal data is to be collected directly from the person affected. Otherwise, the person affected must be at least informed of which types of personal data will be collected, processed, and/or used, and for which specific purposes.

Data may only ever be collected to the extent absolutely necessary for fulfilling the purpose specified before it is processed or used; any other processing is not permitted.

Personal data must be accurate at all times and corrected where necessary.

Personal data may be retained only for as long as is absolutely necessary for the purposes specified or other legal requirements. Thereafter, personal data must be deleted or anonymized. For more information, see section 5b.

4. Responsibilities for Data Protection and Privacy

a. Management

The legal responsibility for collecting, processing, and using personal data within SAP lies with the executives of the SAP company that collects, processes, or uses the personal data for their business purposes.

Within SAP, responsibility can be delegated along the organizational structure of SAP by means of documented instructions from management, guidelines, and business processes that involve the explicit transfer of responsibility to managers at different levels as well as employees.

Management is responsible for structuring all processes during which personal data is collected, processed, or used in such a way that the requirements of this Policy are fulfilled.

The following tasks are the responsibility of management in every SAP company:

- Ensuring that there is continuous monitoring of the applicable law
- Ensuring that processes, during which personal data is collected, processed, and/or used, are in line with applicable law and that local and global process owners are informed of necessary changes
- Ensuring that all approvals required by the supervisory authorities for collecting, processing, using, and transferring personal data have been granted and that the necessary notifications have been sent to the supervisory authorities
b. **Global Human Resources**

Before commencing an activity during which access to personal data cannot be excluded, every employee and every third party acting on behalf of SAP are to be instructed that they are not permitted to collect, process, or use personal data without authorization (data protection) and that this data must be handled confidentially (confidentiality). Employees are to be made aware of the consequences of violating data protection and confidentiality. This Policy and other internal company guidelines that govern the handling of personal data are to be brought to employees’ attention. The instruction must be documented in writing or in another form. Furthermore, every employee can access additional information on the DPPO portal page.

The Global Human Resources organization at SAP is responsible for providing the instruction.

c. **Employees**

It is the duty of all SAP employees to treat personal data to which they have access in the course of fulfilling their contractual duties with SAP as confidential.

SAP employees may collect, process, and/or use personal data only to the extent required to fulfill their duties and in accordance with approved processes. If collecting, processing, or using personal data is not recognizably prohibited for the employee, he or she can refer to the legality of the management’s instructions. In case of doubt, employees may contact the DPPO for clarification (privacy@sap.com).

5. **Details**

a. **Notification, Accuracy of Data, and Inspection**

A person affected must be informed in a suitable manner that their personal data is being collected, processed, and/or used. Usually, they are to be informed before the time at which data is collected.

The person affected must be informed of the SAP company collecting the data; the purpose for collecting, processing, or using the data, as well as other recipients to whom their data will be transferred. The information must be provided in a way that is easy to understand.

Stored personal data must be accurate. Inaccurate data must be corrected or deleted as soon as practicably possible. All processes for collecting, processing, and/or using personal data must contain an option for correcting, updating, and, where required by applicable law, deleting or blocking.

A person affected may, at any time, request information about the data stored on them, its origin, purpose for storing, and recipients to whom the data is passed on. Queries or complaints submitted by a person affected must be processed by the responsible SAP company without undue delay or according to those timeframes imposed by local law, whichever is the earlier. Objections from a person affected with regard to the processing of personal data must be investigated and, if necessary, remedial action must be taken.

b. **Duration of Storage and Data Deletion**

For every process in which personal data is collected, processed, or used, a schedule must be defined for the regular deletion of personal data after the specified purpose has been fulfilled or if the legal basis no longer applies.

Instead of deleting the personal data, it may also be irreversibly anonymized, meaning retained in such a way that makes it no longer possible to identify individual persons. If, for technical or legal reasons (for example, if the retention of data is legally required for tax purposes), it is not possible to either delete or anonymize personal data, this personal data must be blocked for any further processing and/or use, as well as for further access.

c. **Additional Rules for Special Types of Personal Data**

Special types of personal data are details on racial and ethnic origin, political views, religious or philosophical beliefs, union membership, health, or sexual preferences. Special types of personal data are equal to such personal data that requires special sensitivity for the persons affected (sensitive data). For example, this is the case for data...
on criminal activities, as well as on those individuals who in their respective country fall below the age legally deemed as adult i.e., minors.

In the instances in which SAP or third parties acting on behalf of SAP collect special types of personal data, management must ensure that the persons affected have been informed in advance and have given their consent for this. Provided that applicable law does not determine otherwise, special types of personal data may be collected, stored, processed, and transferred only with the explicit consent of the persons affected. Increased precautions (for example, physical safety features, encryption, and access restrictions) that are appropriate for the special sensitivity are to be taken for collecting, storing, processing, and transferring this data.

The following additional rules apply for these special categories of data:

- The collection, processing, and/or use of this data must be transparent for the persons affected at all times.
- Consent given by persons affected must refer explicitly to these special categories of data.
- Processes that involve collecting or using special types of personal data may be configured only with a prior check performed by the DPPO or in consultation with the local DPPC.

**d. Transfer of Personal Data and Commissioned Data Processing**

If personal data is to be exchanged within the SAP group or with other companies, it must first be checked whether contractual agreements on data protection and privacy, and data security are required. Such a check is always required if an SAP group company is to process data on behalf of another SAP group company, or if an external service provider is to process data on behalf of an SAP company (transfer for processing purposes). A check is also necessary if an SAP group company transfers data to another SAP group company or an external company (for example, a service provider, partner, or customer), and the receiving company wishes to use the data for its own business purposes (transfer for own purposes). The legally compliant transfer of personal data within the SAP group is ensured based on internal company commissioned data processing agreements (intra-group data transfer agreements - IGA).

If personal data under the legal responsibility of SAP is transferred to a recipient located outside the European Economic Area (EEA), it must also be ensured in advance that a suitable level of protection in accordance with Articles 25 and 26 of the EU Data Protection Directive (95/46/EC) is guaranteed.

If personal data is transferred, the following rules apply:

**Transfer for commissioned processing:**

The SAP company that commissions or instructs another SAP company or an external company to collect, process, or store personal data is responsible for compliance with the requirements of data protection and privacy regulations. This responsibility does not cease with the transfer to the other SAP or external company.

Every SAP company must ensure that external companies that collect, process, or store personal data on their behalf, are reviewed in advance and then regularly to ensure that they comply with the requirements of data protection and privacy regulations and that the necessary contracts with these companies have been concluded. The review can be delegated to central units within the SAP group. A regular review also takes place within the companies of the SAP group.

**Transfer for recipient's own purposes:**

The transfer of personal data to another company within the SAP group or an external company for their own purposes is allowed only if this is permitted or required by law or if the persons affected have given their prior consent. The transferring SAP company must ensure that the legal requirements are checked before the data is transferred.
Transfer to state agencies (authorities and courts):

SAP will transfer personal data to governmental agencies only on the basis of applicable law and after the DPPO and Global Legal organization within SAP have performed a prior check, taking into account other required areas within the SAP group. In the event of a request for information from a governmental authority or a court of competent jurisdiction, SAP will inform the person affected of this without undue delay.

6. Transfer of Customer Data

SAP processes customer personal data. This means not only the personal data pertaining to a customer's employees and business partners but also the personal data pertaining to the customers of SAP customers. The transfer and use of such customer data must be performed in full compliance with applicable law and those additional obligations agreed in the contract between SAP and the customer. Personal data of customers may never be passed on to third parties without an appropriate legal or contractual basis.

In this respect, SAP works with its customers to support them in complying with applicable data protection and privacy legislation; however, this does not include providing our customers with any legal advice or giving them any guarantee that their legal compliance with data protection and privacy laws are guaranteed.

7. Data Protection and Privacy Supervisory Authorities

If so required by law, contract and/or the obligations set down in this Policy, SAP companies must always cooperate with any data protection and privacy supervisory authority irrespective of whether such authoritative entity is based inside or outside the EEA.

If a data protection and privacy supervisory authority requests information or otherwise exercises their right of investigation, the DPPO must be informed without delay (privacy@sap.com). The DPPO shall then act as the primary coordinator to formulate an appropriate response to the query, in consultation with the other responsible departments (for example, Global Legal; Legal Compliance and Integrity; IT Security; and Global Governance, Risk, and Compliance). In addition, the DPPO will act as the direct contact with the respective data protection and privacy supervisory authorities.

8. Data Protection, Privacy, and Data Security

Certain data protection and privacy laws require special security measures to be implemented when collecting, processing, and/or using personal data. SAP shall define such measures in compliance with the legal requirements in the SAP security policy and related security standards and guidelines. The DPPO shall assist in defining and updating these standards and guidelines.

9. Data Protection and Privacy Organization

a. Position of the Data Protection Officer and Global Organization

The DPPO is an appointed organizational unit within SAP SE. It reports directly to the responsible board member and is managed by the data protection officer at SAP SE.

The DPPO determines the SAP group's data protection and privacy strategy in accordance with the strategic objectives of the SAP group and ensures that the SAP group companies adhere to the applicable provisions of the data protection and privacy regulations. The DPPO is to be supported in performing its tasks. In particular, the DPPO is to be provided with the resources required to perform its tasks and is to be provided with any requested information fully and without undue delay.

The data protection officer is free to exercise tasks as he/she sees fit. DPPO employees are only bound by the instructions of the data protection officer. The data protection officer and DPPO employees must not be discriminated against for performing their tasks.

This attached Policy is provided to you as an information only. It shall have no binding effect on SAP or SAP course of business. SAP reserves the right to change the Policy at any time without giving notice.
The DPPO maintains a network of data protection and privacy coordinators, who, in accordance with section 9b of this Policy, are to be appointed by respective SAP companies and central organizations. The tasks of the global organization are defined in Annex 1. The DPPCs are to be supported by their respective SAP companies in performing their tasks and must not be discriminated against for performing their tasks.

b. Organization at Local, Regional, and Line-of-Business Level

This obligation is broken down into 2 key subsections, as follows:

(1) It is the duty of every SAP company to appoint a DPPC for their business unit and to inform the DPPO about the name of the personnel appointed. More than one SAP company can also appoint the same DPPC jointly.

All DPPCs must have a direct functional reporting line to the head of the relevant SAP unit to which they have been appointed. They must ensure compliance with relevant data protection and privacy laws and the provisions of this Policy. They shall regularly align their activities with the DPPO, but are otherwise free to exercise their expertise in the area of data protection and privacy as they see fit, and they must not be discriminated against for performing their tasks.

The appointment as DPPC can only be revoked in agreement with the data protection officer of SAP SE. If a DPPC's appointment comes to an end or is otherwise terminated, the respective SAP company must appoint a new DPPC in good time and inform the DPPO.

The respective business units to which the DPPCs are appointed shall provide the DPPCs with reasonable time to work required by the DPPC to administer its DPPC duties and suitable resources shall be allocated to the DPPC for them to perform their tasks. To ensure that DPPCs retain and benefit from learning resources to ensure the necessary expertise to fulfill their duties, they shall be permitted to participate in further education and professional development funded by SAP upon mutual agreement with their managers.

A DPPC shall undertake those tasks outlined in Annex 2. In the event of any query regarding the nature and scope of such tasks, the DPPC (or manager responsible for the DPPC) may contact the DPPO for further clarification.

(2) Organizations and/or business units of an SAP company that do not process personal data in their daily tasks are also, at the request of the DPPO, obliged to appoint a DPPC responsible for the respective organization. Accordingly, the provisions of section 9b (1) apply to the DPPCs.

10. Data Protection and Privacy Standards

The requirements under this Policy can be specified and enhanced through data protection and privacy standards. Such data protection and privacy standards may only come into effect after the DPPO has reviewed and approved their compatibility with this Policy.

11. Raising Awareness

The DPPO and DPPCs shall take measures to raise awareness at regular intervals. All employees and third parties acting on behalf of SAP are regularly informed about both their duties and their rights within the scope of this Policy and applicable laws.
This attached Policy is provided to you as an information only. It shall have no binding effect on SAP or SAP course of business. SAP reserves the right to change the Policy at any time without giving notice.