Global SAP Data Protection and Privacy Policy

Version 3.0, 2019

This version of the Policy is PUBLIC.

Contents

Purpose	The global SAP Data Protection and Privacy Policy defines the rules for compliance with data protection and privacy laws that are applicable for the SAP Group. The policy defines the basic principles for processing personal data, assigns responsibilities and competencies within the organization and provides tips for their organizational execution.
Reasons	
Benefits	SAP must comply with relevant laws when processing personal data. Such compliance is relevant for SAP to meet the expectations of authorities, auditors, data protection and privacy auditors, customers, investors, and business partners and to gain the necessary trust of employees, applicants, customers, suppliers, other individuals and the general public in the data protection compliant processing of their personal data.
Risks of Non-Compliance for SAP	Violations of data protection and privacy laws can result in administrative measures, fines, and even criminal sanctions. Also, data subjects can claim compensation for damages or injunctive relief. Informing the general public about potential privacy breaches may damage our reputation, SAP's brand and its value.
Scope	
Primary Target Group	This Policy primarily addresses the company's management. The management is responsible for establishing business processes, so they ensure compliance with applicable data protection and privacy laws.
Indirectly Affected Areas	SAP employees and external business partners who process personal data on behalf of SAP are required to follow these principles when processing personal data in the course of their daily work.
Confidentiality Level	Public.
Enforcement	Compliance with the Policy is ensured through regular consultation by DPP, group-wide information and training courses and the control of processing activities. Compliance with statutory data protection requirements is regularly monitored by the Data Protection Management System (DPMS). Violations of the Policy are investigated by DPP with the involvement of local data privacy coordinators or other functions. The DPMS itself is audited and certified regularly by an external body.
Responsibilities	
Policy Owner	Mathias Cellarius, Group Data Protection Officer at SAP
Executive Board Area	Finance and Administration
Responsible Executive Board Member	Luka Mucic
Contact Person for Executive Board Area	Mathias Cellarius
Review by	Scholten, Jochen (Global Legal), Vivianne Gordon-Pullar (Legal Compliance and Integrity Office), Christian Behre (SGS), Alexander Rodde (GRC Internal Controls SE), Barbara Althoff-Simon (Global HR), Rico Modess (Office of CEO), Robin Manherz (IEG).
Approved by	SAP Executive Board
Document History	
Date of Publication	Version 3.0, 2019
Next Review/Update	This policy will be reviewed every two years or after major changes to the regulations.

Version History	Version 1.0, 2012; Version 2.0, 2017; Version 3.0, 2019

1. Introduction

SAP is committed to data protection and privacy. As such, SAP respects and protects the rights of individuals, particularly the right to data protection and privacy in context of the processing and use of personal data. This applies equally to employees, applicants, customers, suppliers, partners and all other persons whose personal data SAP processes.

SAP is a global group corporation with its headquarters in Germany, a member state of the European Union (EU). The group parent company is SAP SE, headquartered in Walldorf. Within the Executive Board of SAP SE, the Chief Financial Officer's division is responsible for compliance and enforcement of data protection and privacy. On its behalf, the Data Protection and Privacy (DPP) department, headed by the Group Data Protection Officer, has issued the SAP Global Data Protection and Privacy Policy ("Policy") to account for SAP's obligation to data protection.

The Policy defines a group-wide minimum standard for the data protection compliant processing of personal data. It defines requirements for business processes that involve personal data and assigns clear responsibilities. Further information, topic-specific data protection standards, and guidelines can be found on the wiki page of the DPP department.

The executive management of the single SAP group companies and the responsible process owners must ensure that all processes that involve the processing of personal data are designed to fulfill the regulations in this Policy. As employers, the SAP group companies also bear legal responsibility for the processing of their employees' personal data. When handling personal data in course of their duties for SAP, all employees are required to follow the provisions of this Policy.

The principles established by this Policy are based on European data protection and privacy laws and take into account the requirements of the EU General Data Protection Regulation (Regulation (EU) 2016/679 - GDPR). They apply generally and globally to all SAP group companies. Deviations from these principles are possible in the following exceptional cases:

1. Applicable local law defines stricter or alternative data protection and privacy requirements than this Policy. In this case, the local SAP Group companies must ensure compliance with these requirements.

2. The material and territorial scope of the GDPR does not apply to processing activities of an SAP group company and applicable local law defines less strict requirements than those in this Policy. In this case, deviations from this Policy are possible in a local policy, provided that said deviations do not have any impact on other SAP group companies. In any case, all deviations from this policy must be coordinated with DPP.

2. Definitions

Anonymous data Anonymized data	Anonymous and anonymized data does not refer to an identifiable natural person. Even if other data or additional information were added, identification of the natural person is not (or is no longer) possible. This Policy does not apply to such data.
Processor	A natural or legal person that processes personal data on behalf of the controller, such as an external service provider or a different SAP group company that is not the controller itself.
Special categories of personal data	Certain personal data that is particularly sensitive due to its nature, whose processing is likely to result in significant risks for the rights of the data subject and therefore requires special protection. This includes data concerning health, *genetic* data*, biometric* data processed to uniquely identifying a personal data, information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life, or sexual orientation. Depending on the context, this may also include data that could

	be misused for identity theft purposes, such as social security-, credit card- and bank account numbers, ID-card or driver's license-numbers, also personal data regarding criminal investigation proceedings, convictions, and crimes, or data that is subject to professional confidentiality obligation.
Processing	Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. The anonymization of data also represents a processing of personal data.
Third party	A natural or legal person, public authority, agency, or body other than • the data subject, • the controller, • the processor and • the persons who are authorized to process personal data under the direct authority of the controller or processor.
Consent	Any freely given and unambiguous statement or other clear affirmative action by which the data subject indicates in an informed manner that he or she agrees to the processing of his or her personal data for a specific purpose.
Recipient	A natural or legal person, public authority, agency or another body, to which the personal data is disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients.
Data concerning health	Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
Erasure	The irretrievable obliteration or physical destruction of saved personal data or its anonymization in such a way that makes it impossible to re-identify the natural person after the fact.
Personal data	Any information relating to an identified or identifiable natural person ("data subject"). 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. Natural persons can be identified directly based on, for example, names, phone numbers, e-mail addresses, postal addresses, user IDs, tax and social insurance numbers or indirectly through a combination of any other information. The personal data that is subject to this Policy includes data of employees, applicants, former employees, customers, potentials, suppliers, partners, and users of SAP websites and services. It can be contained in SAP's own systems, in systems that third parties operate on behalf of SAP, and possibly in customer systems operated by the customers themselves, by SAP, or by third parties, to the extent that SAP employees could gain access to the saved personal data there in the course of support and consulting activities.
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person (such as fingerprints or facial images).
Genetic data	Personal data relating to the inherited or acquired genetic characteristics of a natural person that gives unique information about the physiology or the health of that natural

	person and which result in particular from an analysis of a biological sample from the natural person in question.
Pseudonymization	Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person. Pseudonymized data constitutes personal data as defined in the GDPR; therefore, this Policy also applies to pseudonymized data.
SAP	SAP SE and its worldwide branch offices and subsidiaries (affiliated companies as defined in section 15 ff. German Public Companies Act).
DPP	The organizational unit "Data Protection and Privacy" at SAP, which bears global responsibility for data protection and privacy and is headed by the SAP Group Data Protection Officer.
DPPC	Data Protection and Privacy Coordinators who are appointed at the level of the individual SAP group company and who ensure the accessibility of the Group Data Protection Officer and work locally toward compliance with the Policy and relevant data protection and privacy laws.
RDPPC	Regional Data Protection and Privacy Coordinators who support the DPPCs in the performance of their duties; they report to the SAP Group Data Protection Officer.
Controller	Any natural or legal person that, alone or jointly with others, determines the purposes and means of the processing of personal data. At SAP, an SAP group company is always the controller for the personal data of its employees, customers, suppliers, partners, or other persons. Purely internal organizational units and bodies such as the Works Council, as well as individual SAP employees, are generally not controllers. The controller is represented by the legally responsible management, for example, the SAP SE by the members of the Executive Board, or other SAP Group companies by the managing directors.

3. Principles for Protecting Personal Data

Personal data shall only be processed lawfully and in accordance with the principles set out below.

a. Lawfulness, Fairness, and Transparency

Personal data may only be processed lawfully, fairly, and in a transparent manner in relation to the data subject. This is the case when:

- processing is legally permitted in the specific case. Among others, the laws permit all cases of data processing that:
  - are necessary for the performance of contracts with the data subject (e.g. the storage and use of necessary personal data in the context of an employment- or service contract),
  - are necessary to take steps at the request of the data subject prior to entering a contract (e.g. a customer requests information about product X and then purchases said product. The data necessary to send the information material and to execute the contractual relationship may be processed),
  - are necessary for compliance with legal obligations, e.g. due to tax or social insurance laws,
  - are necessary to protect the vital interests of the data subject or of another natural person,
  - are necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (e.g. for direct marketing),
  - include decision-making based on automated processing in an individual case that produces legal effects concerning the data subject, when this automated decision is legally permitted, required for

the performance of a contract with the data subject, or for which the data subject has explicitly granted consent,

or

- when a data subject has granted his or her consent (for example, when registering on a website or subscribing to a newsletter).

Personal data should be collected directly from the data subject. If this is not the case, the data subject must be notified, particularly about the types of personal data that are being collected, processed, and/or used and for which specific purposes this occurs.

b. Specific Purpose

Personal data may only be collected for specific, explicit purposes. It may not be processed in a manner that is incompatible with those purposes.

The specific purpose must be defined before data collection. Processing for a purpose other than that for which the data have been collected is only permitted in exceptional cases, when a law permits processing for another purpose or if it is based on the data subject's consent. To ascertain whether the other purposes are compatible with the agreed purposes, the reasonable expectations of the data subject toward the company with regard to such further processing, the type of data used, the possible consequences of the intended further processing for the data subject, and measures of encryption or pseudonymization must be taken into account.

c. Data Minimization

Personal data may only be collected to the extent absolutely necessary to fulfill the defined purpose. Processing must be adequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed.

d. Accuracy

Personal data must be accurate and up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.

All processes that involve the processing of personal data must provide an option for rectification and update.

e. Storage Limitation (Obligation to Erase)

Personal data may only be stored as long as is necessary for the purposes for which it is processed or due to other legal requirements, particularly to comply with statutory retention periods. After this point, personal data must generally be erased or anonymized.

All processes for processing personal data must contain an option for erasure or blocking to the extent required by law.

f. Integrity, Availability, and Confidentiality

Personal data and its processing operations must always be appropriately protected by means of technical and organizational measures. This includes, in particular, suitable measures to protect against unauthorized or unlawful processing, accidental loss, destruction or damage, accidental disclosure and unauthorized access.

g. Processing of Special Categories of Personal Data

The collection, processing, and use of special categories of personal data should always be transparent for the data subject. Unless the collection and processing of such data is explicitly authorized by law, e.g. if

necessary for carrying out obligations and exercising rights in the field of employment, social security, social protection, it should only be collected on the basis of explicit prior notification and consent of the data subjects. The consent must explicitly refer to these special data categories and their processing for one or more specified purposes.

Unless applicable laws stipulate otherwise, special categories of personal data may only be processed and used with the explicit consent of the data subjects. Increased protective measures must be established to protect the data (e.g. physical security measures, access restrictions and encryption).

Processes that are used to collect or use special categories of personal data may only be established based on a prior data protection impact assessment and approval by DPP.

4. Rights of Data Subjects

a. Right of Access and Data Portability

Data subjects have the right to obtain from SAP confirmation as to whether or not personal data concerning her or him are being processed. In this case, SAP shall provide for access as required by law. The information is provided in writing, unless the data subject submitted the request for information electronically. The information must include the purpose of storage, the recipients of the data, and all other legally required information pursuant to Article 15 GDPR. The data subject must be provided with a copy of the personal data that are undergoing processing.

Upon request by the data subject, the data that he or she has provided to the controller must be made available in a structured, commonly used and machine-readable format.

b. Right to Rectification, Restriction, and Erasure

When personal data prove to be incorrect, incomplete, or out of date, each data subject has the right to rectification of his or her personal data. This can be the case, for example, if the data subject has changed his or her name due to marriage.

Data subjects also have the right to obtain restriction of processing of their personal data when one of the following applies:

- The data subject contests the accuracy of the personal data and verification of the accuracy of the personal data takes some time. In this case, the data subject can demand restriction for the period of the verification of the accuracy.
- The processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of its use instead.
- The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise, or defense of legal claims. Should it become apparent that certain information have a respective value to the data subject, the data subject must be notified of the pending erasure with reasonable notice.
- The data subject has objected to processing for the duration of the clarification as to whether the legitimate interests for processing outweigh those of the data subject.

Within the restriction process, the stored personal data of the data subject must be marked with the aim to restrict access and limit their further processing.

In addition, data subjects have the right to erasure of their personal data in the following cases:

- The purpose of the data processing no longer applies.
- The data subject withdraws his or her consent for a specific purpose of processing.
- Address data is used for direct marketing purposes and the data subject objects to such use.
- The data is processed unlawfully.
- Erasure is required to meet legal obligations.

All processes in which personal data is collected, processed, or used must include a concept for the regular retention and deletion of personal data. This concept must ensure that personal data is erased in a timely manner after the fulfillment of the specified purpose or the lapse of the authorization for storage, particularly statutory retention terms. Instead of erasure, personal data may also be anonymized.

If there is an obligation to erase personal data and said data has already been made public, other controllers shall be notified of the request to erase his or her data, including all links to this data.

c. Right to Object

Data subjects have the right to object to data processing when SAP processes personal data based on a decision in favor of its legitimate interests. In this case, the data subject must claim own rights or interests on grounds relating to his or her particular situation, which outweigh SAP's legitimate interest to process the data. Data subjects can object to the processing of their personal data for purpose of direct marketing, including profiling if such is related to direct marketing, at any time and without giving reasons.

If an objection is raised, SAP will not process this data further for these purposes. This does not apply if the processing cannot be ceased due to compelling legitimate grounds for the processing, particularly the establishment, exercise, or defense of legal claims.

d. Right to Complain

Should a data subject wish to file a complaint with regard to processing of her or his personal data, they can do so directly in an e-mail to the data protection officer: privacy@sap.com.

The data subject must be notified about all measures taken based on her or request within one month at the latest.

5. SAP Data Protection Governance Structure

Responsibility for compliance with data protection requirements rests with the executive management of the respective SAP group company that processes the personal data for its business purposes. Executive management may delegate the task to fulfill this responsibility to managers at different levels within the organizational framework and the associated business processes.

Accordingly, the individual global SAP lines of business (LoBs) have a mandate to implement data protection and privacy requirements within their respective LoB.

This task is being fulfilled by so-called *management accountables* of the LoBs, who are defining the LoB-specific data protection compliance measures and implementing them through an established network of coordinators and representatives.

At the local SAP group company level, the executive management must transfer the operational responsibility for compliance with data protection and privacy regulations to the local Chief Financial Officer (CFO). The CFOs must appoint a Data Protection and Privacy Coordinator (DPPC) for each SAP group company and provide the resources needed to implement the data protection and privacy measures. Local DPP compliance measures, that are needed outside of the LoB structure as described above, are implemented by the CFOs through the established DPPC network.

The DPPCs are also supported by regional DPP coordinators (RDPPCs). They are under the control of the Group Data Protection Officer and thus report directly to DPP. The RDPPCs monitor the local data protection requirements in the regions they are responsible for and works towards compliance with these requirements. The RDPPCs support the local DPPCs in the performance of their tasks and serve as contact person to the local data protection authorities. RDPPCs shall not receive any instructions from local management regarding the exercise of their tasks and must not be dismissed or penalized for performing their tasks.

The SAP Group uses this overall management and governance framework to ensure compliance with applicable data protection requirements.

6. Responsibilities for Data Protection Compliance

a. Executive Management of SAP Group Companies

The executive management of the respective SAP group company must ensure that the processes in their areas of responsibility in which personal data is processed (herein: “processes") meet the requirements of this Policy. This responsibility includes the following tasks:

- Appointing a DPPC for their respective SAP group company and notifying DPP accordingly. The appointment of a shared DPPC for multiple SAP Group companies is possible.
- Equipping the DPPCs with the time and budget they need to perform their duties, including the participation in necessary education and training activities.
- Ensuring that the local processes are enrolled in the central record of processing activities (PET) and checked regularly to ensure they are up to date.
- Ensuring that the processes are in compliance with this policy and applicable law.
- Notifying the local and global process owners about amendments to applicable laws.
- Ensuring, in coordination with the Group Data Protection Officer, that all necessary communications are sent to local supervisory authorities and that all necessary permits are being obtained.

b. DPMS Organization

As of 2010, a group-wide data protection management system (DPMS) was implemented at SAP. It is based on the assignment of responsibility for compliance with data protection and privacy to the LoBs, as set out above. Within a LoB, the global DPMS organization is represented by the roles *DPMS Management Accountable*, *DPMS Coordinator*, and *DPMS Representative*. Their respective tasks and the overall functioning of the DPMS are described in more detail in the DPMS General Book. The SAP LoBs must provide the necessary personnel, budget, and materials required for the DPMS.

The DPMS itself is audited regularly according to international standards for data protection management systems. The current certificate is available on the DPP wiki page and the Cloud Trust Center website.

c. DPPC Organization

DPPCs work at their respective SAP group companies to ensure compliance with the provisions of this Policy and with applicable local data protection laws. They have a direct functional reporting line to the executive management of the SAP group companies for which they were appointed, as well as an informational reporting line to DPP. They ensure that the Group Data Protection Officer (DPO) is easily accessible from each SAP group company.

The tasks of the DPPCs are described in the DPPC Handbook and other handouts provided by DPP, which are reinforced in training courses and regular coordination meetings. They must coordinate their activities with DPP regularly, which shall be based on an action plan defined at the beginning of each year. DPPCs must be supported by their respective SAP Group companies in the performance of their duties. They shall not receive instructions from local management regarding the exercise of their tasks as DPPC and must not be dismissed or penalized for performing their tasks.

The CFO of a respective SAP company must notify DPP promptly upon appointing a new DPPC.

d. Data Protection Officer and DPP

The SAP Group Data Protection Officer is responsible for the entire group of undertakings. As such, he is the data protection officer responsible for all Group companies. The data protection officer shall not receive instructions from global or local management regarding the performance of his duties.

DPP reports directly to the DPO and supports him in the performance of his duties. DPP employees are only subject to the instructions of the DPO. Neither the DPO nor employees on the DPP team must not be dismissed or penalized for performing their tasks.

DPP defines the data protection strategy of the SAP Group in harmony with its strategic objectives and works towards compliance with relevant data protection and privacy requirements in the group companies. Global and local responsible roles support DPP in the performance of their tasks. In particular, they provide the necessary means for DPP to perform its tasks and provide all requested information completely and without delay.

DPP coordinates the DPPCs and RDPPCs and ensures the consistent application of data protection and privacy regulations, as well as a consistent level of data protection and privacy at SAP. The RDPPCs are assigned by the DPO for a respective region and form part of DPP.

For more information on the duties of the global organization, see Appendix 1.

e. Global Human Resources

All SAP employees and all other individuals working on behalf of SAP must acknowledge, before they start their activities for SAP, to keep personal data confidential and to not collect, process, or use such data without authorization (confidentiality) when access to personal data cannot be excluded. This must include the information of the consequences of breaches of these obligations. They must be made aware of this Policy and other internal company guidelines that regulate the use of personal data. This instruction must be documented in written or electronic form.

Responsibility for obtaining the confidentiality commitments lies with SAP Global Human Resources or, in individual cases, with the responsible LoB in the respective group company.

f. Employees

All SAP employees are required to handle all personal data that they can access in the course of performing their duties for SAP with strict confidentiality and to not collect, process, or use such data without authorization.

SAP employees may only process personal data within the scope necessary to fulfill their duties as defined by their employment contracts. If the processing of personal data is not recognizably prohibited for an employee, he or she may assume the legality of the instructions from their superiors. When in doubt, employees may turn to the DPPC responsible for their line of business or to DPP (privacy@sap.com). In addition, more information is available for all employees on the DPP wiki page.

7. Transfer/Commissioned Data Processing

If personal data is to be transferred within the SAP group of undertakings or to other companies, a review must first take place as to whether contractual agreements regarding data protection and privacy are needed. Such review is always required when an SAP group company or external service provider is to process personal data on behalf of (another) SAP group company (referred to as “transfer for processing purposes"). Such review is also required when an SAP group company transfers personal data to another SAP group company or an external company (such as a service provider, partner, or customers) and the receiving company intends to use this personal data for its own business purposes (“transfer for own purposes"). The permissibility of transferring personal data within the SAP group is ensured through a multilateral contract that has been signed by all SAP Group companies (Intra-Group Data Protection Agreement or IGA).

If personal data that is the responsibility of an SAP group company within the European Economic Area (EEA) is to be transferred to a country outside the EEA, it must be ensured beforehand that an appropriate level of protection is guaranteed, pursuant to Article 44 et seqq. GDPR.

In addition, the following rules apply to the transfer of personal data:

- **Transfer for commissioned processing:**

  If an SAP group company commissions another SAP group company or an external company with the processing of personal data, it remains responsible for compliance with data protection and privacy requirements. This responsibility does not cease with the transfer of the data to the other SAP group company or external company.

  Each SAP group company must ensure that external companies which process personal data on their behalf are audited prior to the processing and then regularly to ensure compliance with data protection and privacy requirements and that the necessary contracts with these companies are in place. This review can be delegated to central units within the SAP Group. A regular audit also takes place within the companies of the SAP Group.

- **Transfer for the recipients' own purposes:**

  An SAP group company may transfer personal data to another SAP group company or external company for their own purposes only if this is legally permitted or required, or if the data subjects have first given consent. The transferring SAP group company must ensure that the legal requirements are reviewed prior to the transfer.

- **Transfer to government agencies (authorities and courts):**

  SAP will transfer personal data to government authorities and courts only based on applicable laws and upon prior review by DPP and Global Legal, with the inclusion of other departments within the SAP group, if necessary.

  SAP will notify the data subject(s) immediately when an official request for information is received from a government agency or court.

8. Transfer of Customer Data

SAP processes personal data of customers and on behalf of customers. The use and, if relevant, transfer of such customer data must take place in compliance with applicable laws and contractual obligations. Personal data of customers must not be processed or transferred to third parties without an appropriate legal or contractual basis. SAP concludes commissioned data processing contracts with its customers in all cases of activities relevant to data protection and privacy.

SAP collaborates with its customers in this regard, to support them in complying with applicable data protection and privacy laws; this does not include however legal advice.

9. Data Protection Authorities

SAP Group companies must always cooperate with data protection authorities, whether due to legal requirements, contractual obligations or this Policy. This includes cross-border cooperation.

When a data protection authority requests information or otherwise exercises its administrative powers, DPP must be notified without delay. DPP coordinates the response to the inquiry in coordination with the affected or otherwise responsible departments (e.g. Global Legal, Legal Compliance & Integrity, IT Security, Global GRC) and serves as direct point of contact to the respective data protection authority.

10. Data Protection and Security

When personal data is processed, appropriate technical or organizational measures must be implemented to ensure that the level of protection of the data subjects is commensurate to their risk. SAP defines such measures in harmony with legal requirements in the Global SAP Security Policy and the associated security standards and guidelines. The DPP team supports the definition and amendment of these standards and guidelines.

11. Awareness-Raising and Training

DPP and the DPPCs ensure awareness-raising and trainings at regular intervals. All employees and third parties working on behalf of SAP are regularly instructed not only in their obligations, but also their rights in the framework of this Policy and the relevant laws.

12. External Certifications

In addition to the aforementioned certification of the SAP DMPS under BS 10012:2017, many departments at SAP have also been certified under other certification standards – particularly ISO 27001, ISO 9001, etc. Additional information is available on the Cloud Trust Center website.