CONFIDENTIALITY and PRIVACY STATEMENT V3.0

In consideration of your engagement within the SAP Group (thereafter "SAP") and disclosure by SAP of Confidential Information, you hereby covenant and agree as follows:

1. CONFIDENTIALITY/SECURITY

You undertake not to disclose any Confidential Information. Confidential Information shall mean all information and sensitive data which the Disclosing Party protects against unrestricted disclosure to others or which is identified as "Confidential" or "Proprietary" or would otherwise ordinarily be expected to be confidential or proprietary regardless of the manner in which it is furnished, including but not limited to, any trade and business secrets of SAP, SAP customers, SAP partners and/or other third parties, about which you obtain knowledge during the course of your activities for SAP. You shall keep all Confidential Information confidential and not disclose any Confidential Information to any person other than SAP personnel on a need to know basis and only for the purpose of fulfilling your duties. You undertake to disclose Confidential Information to third parties only with prior written approval by SAP. This obligation shall remain in force even after termination of your access to SAP confidential information.

You also acknowledge that you are obliged to the terms and conditions of SAP's Security Policy and the related Standards, including but not limited to the SAP Global Security Policy (Appendix II), SAP Global Data Protection & Privacy Policy Public (Appendix IV) or any amendment or new version thereof.

2. TRADE SECRETS AND COPYRIGHTS OF OTHER COMPANIES

You undertake to respect the rights, especially the copyrights, of third parties. Unless the copyright holder has given its express consent in writing and SAP has given its approval for the respective use, third party software or materials shall not be used or modified in any way.

You acknowledge that SAP has no interest whatsoever in Confidential Information of other companies. You undertake not to disclose any Confidential Information or copyright protected materials of third parties to SAP. In addition you shall not keep or store any such information in SAP premises or on SAP systems. Any disclosure is subject to a written non-disclosure agreement to be concluded between SAP and the respective third party before such disclosure.

3. OBLIGATION TO OBSERVE DATA SECRECY

You agree to treat personal data (e.g. customer data, employee data) to which you gain access or of which you become aware of during your engagement as confidential and to process these personal data only in accordance with the instructions of SAP (confidentiality pursuant to Art. 5 (1) lit. f, Art. 28 (3) lit. b, Art. 29 and Art. 32 (4) GDPR).

You are not allowed to process personal data without authorization. The processing includes 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 of personal data. You agree, in particular, to

(a) process personal data for no other purpose than the purpose to lawfully perform the tasks,

(b) comply with all statutory and internal regulations regarding the handling and protection of personal data,

(c) comply with all technical and organizational measures regarding data security,

(d) use the data entrusted to you exclusively to the extent provided to you for the specific task,

(e) refrain from violating the security of the processing, either intentionally or unintentionally, in a manner that leads to destruction, loss, alteration, unauthorized disclosure or unauthorized access.

You are aware that the obligation of non-disclosure and the obligation to confidentiality continue even after the termination of your engagement with SAP.

Violations of the obligation of non-disclosure and the obligation to confidentiality can be prosecuted under criminal law, lead to administrative fines or lead to claims for damages.

I acknowledge and agree to the regulations of the CONFIDENTIALITY AND PRIVACY STATEMENT V3.0 including its Appendices I-IV which shall form an integral part of this Statement. With my signature I especially acknowledge the regulations of the General Data Protection Regulation (GDPR) outlined in Appendix I.

Please enter your data using block letters:

First name:_____ Middle name:_____ Last name:_____

Company:_____ SAP customer/partner no:_____

Company Address:_____

Date:_____ Signature:_____

APPENDIX I – Extracts from the GDPR:

Art. 4 No. 1 GDPR: "personal data" means any information relating to an identified or identifiable natural person (hereinafter "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;

Art. 4 No. 2 GDPR: "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;

Art. 5 (1) GDPR: Personal data shall be

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("purpose limitation");

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimization");

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy");

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation");

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality").

Art. 28 (3) lit. b GDPR: The processor ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

Art. 29 GDPR: The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Art. 32 (2) GDPR: In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

Art. 32 (4) GDPR: The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Art. 33 (1) GDPR: In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority […], unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Art. 82 (1) GDPR: Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

Art. 83 (1) GDPR: Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation […] shall in each individual case be effective, proportionate and dissuasive.

SAP Global Security Policy

Version No.	2.1
Date	2016-05-15

Table of contents

1 Introduction 8

2 Definitions 8

3 Policy content 9

Cover Sheet

Objective	• The overall aim of the Security Policy and related SAP security documentation is to set the requirements for an effective and appropriate level of security within SAP. The purpose of the SAP Security Policy is to govern security at SAP and protect employees, customer assets entrusted upon SAP and SAP's own assets from security threats; whether internal or external, deliberate or accidental.
Rationale	
Why – the benefits and strategy alignment	• The responsibility for security resides ultimately with the SAP Executive Board but cascades to all personnel working with, or affiliated with SAP. An appropriate, up-to-date, and fitting global policy defines the company-wide requirements for the protection of all personnel, their work, all customers, and their information which they entrust SAP with. • Through its related Security Standards the Security Policy covers Security within SAP in detail.
Risk of Non-compliance to SAP	• Increased risk for SAP for financial impact, reputational loss, and/or legal claims, loss of customers or the prevention of new contracts. • Non-compliance in audits (financial audit and/or security audit) which may prevent or cause the loss of security certifications and/or attestations which further may cause loss of customers or the prevention of new contracts.
Applicability	
Primary group applicable to	• The SAP Security Policy is binding for all companies within the SAP Group, all SAP employees and external workers, suppliers, companies and members of the partner ecosystem (hereafter external parties). All companies that are integrated directly in the SAP network are required to comply with and implement this policy.
Indirectly Affected Areas	• None
Confidentiality	• Customer
Enforcement	• Non-compliance with the SAP Security Policy or applicable laws may lead to measures under applicable labor law, damage and other claims under civil law, as well as to prosecution under criminal law.

Ownership	
Policy Owner	• Chief Security Officer, SAP SE.
Board Area	• Product and Innovation.
Reviewers	• Barbara Althoff-Simon, Head of Global HR Service Delivery and Talent Acquisition, Executive Vice President, Corporate Officer, SAP SE • Thomas Bamberger, Senior Vice President, Head of Maintenance go to Market and Global Licensing Audit Services, SAP SE • Mathias Cellarius, Data Protection Officer, Head of Global Legal/Regulatories and Processes, SAP SE • Gerold Huebner, Development Executive, Chief Product Security Officer, SAP SE • Cornelia Koch, Lead Senior Legal Counsel Compliance, SAP SE • Peter Rasper, Executive Vice President Global Finance Infrastructure and Chief Operating Officer Finance & Administration • Ralph Salomon, Vice President Operations Security, SAP SE
Approved by (Board Members)	☐ Ingrid-Helen Arnold, President Data-as-a-Service, SAP SE ☐ Bernd Leukert, Head of Products & Innovation, Member of the Executive Board of SAP SE ☐ Luka Mucic, Chief Financial Officer, Member of the Executive Board of SAP SE ☐ Gerhard Oswald, Head of Product Quality & Enablement, Member of the Executive Board of SAP SE ☐ Editorial Changes approved by Justin Somaini, Chief Security Officer, SAP SE
Document Information	
Master Document URL	• This is the officially released version of the policy
Release Date	• Version 2.1, released on 2016-05-15 • Version 2.0, released on 2015-11-02 • Version 1.4, released on 2014-02-21 • Version 1.3, released on 2008-11-01 • Version 1.2, released on 2007-07-18 • Version 1.1, released on 2006-07-11 • Version 1.0, released on 2004-06-01 Revision table is at the end of the document.

1 Introduction

Security is a top priority for SAP. We are committed to ensuring a secure environment for our people, for product development, for security in the Cloud, and for SAP's products, systems, services, for customer data, for personal data, and for our supplier relationships. SAP will continue to offer the level of security our customers are accustomed to and reinforce our reputation as a trusted and secure partner.

SAP is committed to safeguarding the confidentiality, integrity and availability of assets to ensure that regulatory, operational, and contractual requirements are fulfilled. To achieve this SAP adopts a risk based approach to apply appropriate security controls.

The purpose of the SAP Security Policy is to govern security at SAP and protect both customer assets entrusted upon SAP in addition to SAP's own assets, from security threats; whether internal or external, deliberate or accidental.

2 Definitions

2.1 Vocabulary

- Assets: people, intellectual property, facilities, equipment, hardware, software, information, systems, data and outsourced services.
- Availability: accessibility and usability upon demand by an authorized entity.
- Confidentiality: information is not made available or disclosed to unauthorized individuals, entities, or processes.
- Security control: security measure mitigating risk.
- Integrity: accuracy and completeness.
- Intellectual property: patents, copyright, trade secrets, trademarks and other intellectual and industrial property rights protected by applicable law.
- Risk: the combination of the probability of an event and its consequences.
- Security documentation: SAP Security Policy, SAP Security Standards, Line of Business Security Directives, and Security Procedures.

2.2 Entities

- External parties: external workers, suppliers, companies and members of the partner ecosystem.
- Reviewing authority: a cross-representation of senior level managers representing security and related areas in SAP.

3 Policy content

3.1 Scope

The SAP Security Policy is binding for all companies within the SAP Group, all SAP employees, and external parties. All companies that are integrated directly in the context of the SAP Group are required to comply with and implement this policy.

In addition to the SAP Security Policy and to ensure baseline security coverage, SAP has a set of security documentation as follows:

- Level 1: The SAP Security Policy defines purpose, scope and responsibility for security in SAP and defines the high level requirements for security.
- Level 2: The SAP Security Standards define SAP-wide standards for implementation of the SAP Security Policy. The SAP Security Standards cover in detail the contents of this policy. The contents may be from a specific Line of Business or have SAP wide application, for example, on IT Security.
- Level 3: The SAP Security Directives exist for IT Security and Physical Security and define how SAP Security Standards (Level 2) must be implemented. Specific documentation required for varying certification scopes falls into this category.
- Level 4: The SAP Security Procedures describe instructions for the operative implementation of the requirements from standards and directives.

The SAP Data Protection and Privacy Policy is a separate framework. Security relevant contents are aligned with the SAP security documentation by the reviewing authority.

3.2 Responsibilities

3.2.1 Governance

SAP Global Security:

- Owns the SAP Security Policy (Level 1 security documentation) and the process for the SAP Security Policy and SAP Security Standards (Level 2 security documentation).
- Governs annual reviews of the SAP Security Policy and SAP Security Standards. Changes are reviewed and released by a reviewing authority. This reviewing authority authorizes the contents of the SAP Security Policy and SAP Security Standards, formally releases new versions, and is also responsible for setting and monitoring global security objectives and initiatives.

3.2.2 Managing Level 3 and Level 4 security documentation

Any SAP Line of Business who publishes Level 3 and Level 4 security documentation:

- Is responsible for any Level 3 and 4 security documentation.
- Must ensure that any Level 3 and Level 4 security documentation is compliant with the SAP Security Policy and SAP Security Standards.

3.2.3 Management

Each member of management is responsible for ensuring that:

- The Security Policy is implemented within their area of responsibility.
- Security risks are identified and dealt with according to the SAP Risk Management Policy.

3.2.4 Employees and external parties

Each individual is responsible for:

- Complying with the SAP Security Policy and SAP Security Standards and applicable Line of Business Directives/Procedures. The SAP Security Standards cover such areas as product security, IT Security for all employees, access control, authorization, keeping a clean desk, physical security and information classification. SAP Security Directives exist for IT Security and Physical Security and are specific for employees within IT Operations - teams including SAP Cloud operations and Physical Security respectively. SAP Security Procedures exist for IT Security and are specific for employees within IT Operations teams including SAP global cloud operations.
- Reporting security incidents without delay.
- Attending mandatory security training.
- Respecting and protecting the confidentiality of data.
- Ensuring that they do not participate in activities that may damage information or IT infrastructure belonging to SAP or its customers and partners which could lead to unauthorized disclosure of intellectual property or confidential data. This includes, but is not limited to circumventing security measures, taking advantage of weaknesses, cracking passwords, and accessing information without authorization.

3.2.5 External parties with access to the SAP corporate network

External parties who obtain access to the SAP corporate network, business systems or development systems must sign a statement binding them to fulfil legal and SAP internal regulations.

3.3 Protection of assets

3.3.1 General

The protection of SAP employees, external parties and guests, in particular the protection of life and physical integrity, has priority over all other security measures.

3.3.2 Business continuity and operational resilience

A Business Continuity Management framework must be established and aligned with international standards and stakeholder demand on SAP business processes, which enables SAP to minimize the impact of unplanned interruptions on its business operations.

3.3.3 Secure development of SAP on premise/cloud applications, products and tools

During the development of SAP on premise/cloud applications, products and tools, SAP security standards must be applied as an integral part of an applied Secure Software Development Lifecycle.

3.3.4 Information classification and access

To protect information assets, information must be classified and labelled appropriately as described in the SAP Security Standard for Information Classification.

Information and systems belonging to SAP and its customers and partners must be handled and protected so that:

- Confidentiality is maintained (only persons authorized by the owner of the information receive access).
- Integrity is ensured (only persons authorized by the owner of the information can change the information).
- Availability is guaranteed (the information is available within the bounds defined by the owner of the information).

Access to information must be provided on a strict "need to know" basis. In other words, employees and external parties should have access only to the information they require in order to carry out their work.

Access to information must be role based and risk based.

All access authorizations must be removed when leaving SAP and internal moves require access authorization changes based on role and risk as appropriate.

3.3.5 Customer and partner data

Access to data and systems belonging to customers and partners must be provided on a strict "need to know" basis only.

Employees and external parties may view confidential data only if there is a specific requirement.

Data which is received from partners and customers during the course of work must be treated as confidential.

3.3.6 Data protection

Personal data is subject to strict technical and organizational security requirements on the basis of the European Union (EU) Data Protection Directive and the laws of the EU and European Economic Area (EEA) member states implementing the Data Protection Directive, as well as other applicable data protection and privacy laws in Europe and other countries around the world.

Employees and external parties must abide by the SAP Global Personal Data Protection and Privacy Policy when collecting or otherwise processing personal data on behalf of SAP and/or SAP’s customers.

3.3.7 Secure supply chain

Secure development environments and software distribution mechanisms (code signing) are important prerequisites for a secure supply chain and must be upheld.

All relevant suppliers, partners and service providers of SAP are required to have implemented security measures to ensure compliance with the SAP Security Policy and associated Security Standards when delivering services to SAP.

Measures and supplier assessment processes must be taken to achieve compliance with applicable data protection laws and privacy laws and regulations regarding the processing of data by suppliers, partners and service providers on behalf of SAP and/or SAP's customers as well as compliance with further legislations and contractual bindings, such as agreed in SAP contracts.

3.3.8 Physical security

The premises of SAP must be protected to prevent unauthorized persons from obtaining unauthorized access to SAP assets. The premises of SAP must be protected to prevent unauthorized persons from entering. The SAP Security Standard for Physical Security must be followed. This standard determines how to protect people, how to protect infrastructure from sabotage, and how to control inadvertent physical information outflow and loss of high-value assets.

3.4 Compliance

SAP provides relevant security related certifications and/or attestations provided by third party auditing organizations covering general security, architecture security, availability, processing integrity, confidentiality and privacy.

Legal, supervisory, and contractual obligations related to security must be fulfilled.

Non-compliance with the SAP Security Policy or applicable laws may lead to measures under applicable labor law, damage and other claims under civil law, as well as to prosecution under criminal law.

SAP Security Policy & Standards short form

The SAP Security Policy defines all security objectives for SAP which is binding to all employees and external workers. The objectives are stipulated as detailed security accountabilities and requirements within the related SAP Security Standards. This appendix summarizes the most important regulations of the SAP Security Standards and should be used as a short reference guide for security-compliant behaviour. However the original form of each SAP Security Standard is binding as published within the SAP Corporate Portal under Quick Link: /securitystandards.

Authorization

It is generally forbidden to try to get access to or to manipulate information. This particularly refers to illegal technical methods for circumventing access restrictions and to obtaining access rights without being authorized to do so. Information owners who are responsible for issuing access and system rights must grant access privileges on a risk based approach which means that possible segregation of duties (caused by functional combinations) or access to confidential data must be avoided as much as possible. In the case such access risks cannot be avoided respective mitigation controls must be implemented and effectively managed.

Clean Desk

All desks must be organized in such a way that unauthorized persons cannot get hold of confidential documents and data. In addition, valuables (especially laptops, PDAs, and mobile phones) must be protected against misuse and theft. Any PCs, laptops, smartphones and tablets must be locked adequately when the desk is left for a longer time period. This might be ensured by locking the office door or by storing the devices in a lockable cabinet. It must be ensures that confidential documents will not be disclosed to unauthorized persons while they are printed. Therefore PIN based secure printing shall be used when available. Also confidential materials in meeting rooms may not be left (Whiteboards must be cleaned and flipchart papers must be stored away or destroyed respectively). Secure methods which are released by SAP Global IT must be applied to destroy data carriers that contain confidential or strictly confidential information.

Communication

When using an SAP e-mail account every user seems to be a SAP employee. When e-mail communication is used, it is required to ensure that documents and information are not passed on to unauthorized parties. Distribution list members must be checked before confidential documents are sent for example. It is an obligation of everyone to protect the SAP voice mail box by applying a PIN. The same applies to the SAP mobile phone. Official press statements or other publications for authorities, and other external bodies must always be coordinated with SAP Global Communication.

Information Classification

Documents at SAP are classified according to the following five categories: public, customer, internal, confidential, and strictly confidential. These globally valid categories are to be used globally in English. All documents and other information must be classified by the information owner. All employees and external workers need to protect the classified information accordingly with given protection solutions and organizational measures. Those must be applied in accordance with the classification and handling matrix. Documents or other information that have not been classified must be treated at least as internal.

Facility Access Card

Each person which is an employee or external worker needs a valid facility access card to get into SAP buildings. The facility access card must display the employee's or external worker's name with a respective photograph and must be carried all time visible while staying at SAP premises. Generic visitor cards are available for short-term visitors only. It is forbidden to pass the facility access card to other third parties. If the facility access card gets lost, the local security office (front desk) that issued the card or SAP Security in Walldorf (+49 62277 42400) must be informed immediately.

IT-Security – All Employees

The security standard 'IT-Security - All Employees' combines all IT-related security requirements for employees in one single document. All employees cover requirements which have to be fulfilled by all employees, but also external workers and partner ecosystem users who will obtain access to the SAP IT infrastructure and applications. The 'Roles and Responsibility' section has been clearly structured and explains these responsibilities. The section for actual system security has been split into PCs/Laptops (i.e. MS Windows-based devices) and other mobile devices (i.e. smartphones and tablets based on iOS, Android, and other mobile operating systems). Requirements are defined related to the correct password chose, anti-virus protection, secure authentication and others according the ISO 27001/2 framework. One major contributor to better understandability and clarity is that all information pertaining to system operation has been moved to the security standard 'IT Secure System Operation - Operational Groups'. This is also part of the IT-Security Framework.

Internal Applications

Security-relevant requirements for the secure development of all SAP products are described in the SAP Security Standard for the product innovation life cycle (PIL). These security requirements also apply to the development of internal applications and must be applied accordingly.

Managing Access of External Parties at SAP

This SAP Security Standard describes the requirements for providing access rights to external party users (C-users) to the SAP corporate network and associated business applications. Important is to understand that external party users cannot approve access requests of other external party users. Only trustworthy external party users can obtain access to strategic internal projects or confidential business information. It is also a must that external party users return their SAP owned equipment back after completing their services to SAP. Therefore a start and end date for external party users must be specified in accordance with the external party contract.

IT Secure System Operation – SAP Operational Groups

The security standard 'IT Secure System Operation – SAP Operational Groups ' is relevant only for those users that operate IT systems as part of their job description. This may also include external workers or members of the partner ecosystem who will operate SAP IT systems under the duty of contractual agreements. It is an integral part of the IT Security Framework that has been closely aligned with ISO27001/2. The 'Security Standard IT Secure System Operation – SAP Operational Groups', the thereof depending security directives and the security procedures form a comprehensive IT Security Framework which summarizes all requirements when operating IT systems at SAP. These requirements relates for instance for the secure development of internal applications, security requirements for implementation & configuration of IT systems, introduction of a required IT system security lifecycle management and the secure operations (for instance required change management, incident management and others) of these IT systems.

Third Party Systems

In exceptional cases it might be required that non-SAP IT systems (e.g. laptop, tablet, etc.) of external workers might need to be connected to the SAP corporate network. This is only allowed if a valid business reason exists. SAP owned devices that are provided by Global IT must always be the first choice. The non-SAP IT systems must be validated by SAP Global IT if best practice security measures are implemented and activated correctly before connecting them to the SAP corporate network.

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 SAP's 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") (mail:privacy@sap.com) and/or the appointed Data Protection and Privacy Coordinators ("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 actually 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 Group 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 SAP's right 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

Anonymized data Anonymous data	Anonymized data is 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. 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.
Commissioned data processor	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.
Special categories of personal data	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.

Person affected	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 or indirectly, 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.
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, via 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 websites and services, and any other persons. The data may be contained in an SAP system, or in systems of third parties, who 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 responsible, for example, by the members of the SAP SE Executive Board, or the directors of other SAP companies.

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 website
- 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:

- 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 Data Protection and Privacy Office portal page.

SAP Global Human Resources 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 (mail: 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 SAP company responsible 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, 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/ 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 or an ‘IGA’).

If personal data under SAP’s legal responsibility is transferred to an SAP company located in the European Union or in Switzerland, Liechtenstein, Iceland, or Norway, or in a country not mentioned, 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 who are to 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 have performed a prior check, and 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 of a customer's employees/business partners etc. but also the personal data belonging to SAP's customer's own 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 us. 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 the 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 within the EEA 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 (mail: privacy@sap.com). The DPPO shall then act as primary coordinator to formulate an appropriate response to the query in consultation with the other responsible departments (for example, Global Legal, Legal Compliance & Integrity, IT Security, Global GRC), and acts as a direct contact person with the respective data protection and privacy supervisory authorities.

8. Data Protection and 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 the 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 SAP SE Data Protection Officer.

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 his/her tasks as they see fit. The DPPO employees are only bound by the instructions of the Data Protection Officer. The Data Protection Officer and the DPPO employees must not be discriminated against for performing their tasks.

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 the 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 the name of the 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 must not be discriminated against for performing their tasks.

The appointment as DPPC can only be revoked in agreement with the SAP SE Data Protection Officer. 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 in order for them to perform its tasks. To ensure that the DPPC retains and benefits from learning resources to ensure the necessary expertise to fulfil 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 at 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 who do not in their daily tasks administer personal data 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.