

## PRIVACY POLICY FOR CLOUD & MANAGED SERVICES

This Privacy Policy covers the privacy practices of the Supplier with effect from 1st September 2018 in relation to the use of the Cloud Services ("**Services**") by the Customer.

### 1 INFORMATION COLLECTED

- 1.1 **Collected Data:** The Supplier may collect and process Personal Data (within the meaning of the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR") in connection with Customer's access and use of the Services.
- 1.2 **Scope:** This Privacy Policy does only apply to Personal Data that is collected by the Supplier in its role as data controller in order for the Cloud Services to perform the function for which they are designed. For any Personal Data that is processed by the Supplier in its role as data processor on behalf of the Customer, the Data Processing Agreement entered into between Customer and Supplier shall apply. Any Personal Data that is processed within the Cloud Services for purposes and means determined by the Customer (e.g. Personal Data of the Customer's customers/employees/officers/etc.) is being processed on behalf of the Customer.
- 1.3 **Categories of Data:** The data the Supplier is collecting and processing in its role as data controller comprises the following categories of Personal Data:
- first name, last name, email address, country, job title, phone number, fax number, company name, used products of the Supplier and additional information provided when contacting the Supplier using the websites, especially information provided in free text fields of contact forms ("contact data");
  - additional data provided to the Supplier in comments on the Supplier websites, especially in forms of discussion boards and using the comment features of blogs ("comment data");
  - Personal Data sent by the User's web browser, i.e. information about the type of web browser, the operating system and selected settings (e.g. language, region, font size, font types and other configuration) may be collected ("browser data");
  - IP address, information about the amount of data transferred, stored in access log files ("usage data").

### 2 PURPOSES AND LAWFULNESS OF THE DATA PROCESSING

- 2.1 **Purposes:** The Supplier collects, processes, and uses Personal Data to the extent required to fulfill the respective purposes:
- (a) **Providing the Services:** In accordance with the terms and conditions of the Cloud Services Agreement, the Supplier collects processes and uses Personal Data for the purpose of providing the Services, preventing or addressing service or technical problems, in connection with a Customer support matter, for billing, customization, training or as may be required by law. The lawfulness for the data processing is the performance of a contract (the Cloud Services Agreement). Using this Personal Data is required to provide the contractual obligations. Without this Personal Data it would be not possible to receive the Services offered by the Supplier.
- (b) **Security Purposes:** The Supplier will also use usage data for internal system-specific

purposes to secure the websites and IT systems from malicious attacks by third parties. The lawfulness is a balancing of interests of the conflicting interests of the security of the IT systems on the Supplier's part and the Customer's potentially conflicting interests in a non-processing of the usage data by the Supplier. Taking into account the security and organizational measures of the processing of the usage data by the Supplier, the Supplier considers Customer rights and interests appropriately taken into account and protected.

- (c) **Marketing Purposes:** In so far that consent has been given, the Supplier will also use Personal Data for marketing purposes, e.g. to send newsletters. The lawfulness for processing this data is the Supplier's legitimate interest, e.g. to improve the Services, or consent.
- (d) **Improvement:** In so far that consent has been given, the Supplier will also use browser data for market research and the improvement of its Services, and to improve the user experience. The lawfulness for processing this data is consent or the Supplier's legitimate interest.
- (e) **Statistical Purposes:** In so far that consent has been given, the Supplier will also collect usage data for statistical purposes, for the analysis of advertisement on its websites, and for adapting the advertisement for its products and services to better match the users' interests. Log files are only used for statistical analysis of the visitors of the Supplier websites. The data is deleted after having been analyzed. The lawfulness for processing this data for statistical purposes is the Supplier's legitimate interest, e.g. internal organization, or consent.

Providing direct marketing data and browser data is optional. If such data is not provided, no direct marketing information will be sent and Personal Data will not be used to improve the user experience and will not be used for statistical purposes.

Beyond these purposes, the Supplier uses and processes Personal Data only if prior consent has been expressly granted thereto and if information about the purposes has been provided. In particular, the Supplier does not use Personal Data for automated individual decisions and profiling.

### 3 DATA RECIPIENTS

3.1 **Supplier's Departments:** Personal Data will be processed by employees/officers/agents of the Supplier in the respective departments who need to know the Personal Data for the respective purposes.

- (a) contact data: any departments that might be involved to process a Customer request; marketing and sales departments responsible for the Customer's region
- (b) comment data: marketing or the respective product departments that are responsible for operating the blogs or discussion boards
- (c) browser data and usage data: marketing and the IT departments that are responsible for operating the respective websites

3.2 **External Service Providers:** The Supplier has contracted external data processing service providers to collect and process Personal Data on behalf and according to the instructions of the Supplier. Such service providers support the Supplier, especially relating to administering, hosting, distributing, reselling, and/or supporting the Services, hosting and operating the websites and blogs, marketing purposes, statistical analysis, improving the websites and sending Supplier's email newsletters. If these external companies have access to Personal Data,

respective data processing agreements are in place. The entity hosting the Services (“**Hosting Entity**”) is identified in the Cloud Services Attachment or other contract document between the Supplier and the Customer.

- 3.3 **External Service Providers outside the EU/EEA:** The service providers may be located outside the European Union or the European Economic Area. The Supplier is a globally operating corporation. In order to better process the Customer’s matter, it might be also necessary to forward data to local subsidiaries or to local distribution partners, whose registered office might also be located in countries outside the European Union or the European Economic Area. Such data transfers take place within the Supplier’s group companies and the service providers listed in Appendix 1 only for the aforementioned purposes. The lawfulness of the data export is the Supplier’s legitimate interest or legitimate interests of the recipients, e.g. internal administrative purposes, and no higher legitimate Customer interests, the fulfillment of legal obligations or consent.

Beyond that, the Supplier does not forward Personal Data to other third parties, unless the Supplier is obliged to do so by virtue of statutory provisions or order of any judicial or other public authorities or consent has explicitly been given for that purpose. In particular, Personal Data will not be sold, leased or exchanged.

## 4 DATA TRANSFERS TO THIRD COUNTRIES

- 4.1 The recipients of Personal Data might be located outside the European Union or the European Economic Area and therefore might not have a data protection equivalent to EU data protection law.

Unless there is an adequacy decision by the EU Commission for these states or the transfer is based on an exemption provided for by the GDPR (e.g. express consent, assertion, exercise or defense of legal rights), the Supplier will take all necessary measures to ensure that transfers to such organizations are adequately protected, e.g. by signing the standard contractual clauses stipulated by the EU Commission (“SSC”) with the data recipients or be relying on Privacy Shield Principles (“PSP”). A copy of these reasonable warranties may be requested by contacting the Supplier’s Data Protection Department at: [dataprotection@softwareag.com](mailto:dataprotection@softwareag.com).

A transfer of data to official authorities in countries outside the European Union or the European Economic Area (so-called third countries) takes place, if required by law, express consent has been given or this is legitimated by the legitimate interest of the Supplier or the third party for data protection purposes, e.g. internal administrative purposes and no higher legitimate interests by Customer.

## 5 COMPLIANCE WITH PRIVACY SHIELD FRAMEWORKS

- 5.1 If Supplier transfers Personal Data from the EU and/or Switzerland to the U.S., respectively, the Supplier relies either on the EU - U.S. Privacy Shield and the Swiss – U.S. Privacy Shield Principles and/or in some cases standard contractual clauses have been signed. It is marked in Appendix 1 for which transfers the Supplier relies on EU - U.S. Privacy Shield and the Swiss – U.S. Privacy Shield Principles and for which standard contractual clauses have been signed. When the Supplier uses service providers to process personal information received in reliance on the Privacy Shield Principles, the Supplier is responsible if that service provider processes Information in violation of the Privacy Shield Principles (unless the Supplier can prove that it is

not responsible for the service provider's action that violated the Privacy Shield Principles).

Supplier complies with the EU - U.S. Privacy Shield Framework and the Swiss – U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States, respectively. The Supplier has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this Privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield Framework and its Principles, and to view the Supplier's certification, please visit <https://www.privacyshield.gov/>.

## **6 RETENTION**

- 6.1 Personal Data will be kept by the Supplier as long as necessary to provide the Customer with the requested Services. If the Supplier no longer needs the Customer's Personal Data to comply with contractual or legal obligations, they will be deleted from the systems or anonymized accordingly, so that identification is not possible, unless the Supplier has to keep the information, including Personal Data, to comply with legal or regulatory obligations (e.g. statutory retention periods which may arise from the commercial laws or tax laws and may in principle be 6 to 10 years or, if during the statutory limitation periods, which are regularly 3 years, but may be up to 30 years, evidence must be secured).

## **7 SECURITY**

- 7.1 The Supplier implements the technical and organizational measures that are commercially reasonable in relation to the respective purpose of data protection, in order to protect the information provided by the Customer against abuse and loss. Such data is stored in a secure operating environment that is not accessible to the public. In addition, each of the Supplier's employees is instructed on data protection and obliged to enter into a confidentiality agreement.

## **8 INFORMATION TRACKING**

- 8.1 Information about the usage of cookies, especially for marketing purposes, can be found in the Cookie Policy.

## **9 DATA SUBJECT RIGHTS**

- 9.1 Under applicable law, the Data Subject has the right under certain circumstances to (i) request information about the stored Personal Data, (ii) rectification of Personal Data, (iii) restriction of processing of Personal Data, (iv) deletion of Personal Data, (v) data portability, (vi) revocation of consent for processing of Personal Data and (vii) object to the processing of Personal Data. Further information on the individual rights can be found in Appendix 2 to this Privacy Policy. To exercise these rights and/or to address any questions, comments, or complaints regarding this Privacy Policy or the privacy practices of the Supplier, please contact the Supplier's Data Protection Department at:

Software AG Data Protection Officer  
Uhlandstraße 12  
64297 Darmstadt  
Germany  
Email: [dataprotection@softwareag.com](mailto:dataprotection@softwareag.com)

It is possible to send encrypted emails using S/MIME:

- [X.509 certificate](#) (zip file, contains dataprotection.cer)
- [Software AG root certificate](#) (zip file, contains SoftwareAGInternalCa2.cer).

The Data Subject also has the right to file a complaint with a data protection supervisory authority.

Additionally, in compliance with the EU - U.S. Privacy Shield and the Swiss – U.S. Privacy Shield Frameworks, the Supplier commits to resolve complaints about Customer privacy and the collection or use of personal information. European Union and Swiss individuals with inquiries or complaints regarding this privacy policy should first contact the Data Protection Officer at the contact details mentioned above.

The Supplier has further committed to refer unresolved privacy complaints under the EU - U.S. Privacy Shield and the Swiss – U.S. Privacy Shield Principles to JAMS, an independent alternative dispute resolution provider located in the United States. If the Data Subject does not receive timely acknowledgment of his/her complaint, or if the complaint is not satisfactorily addressed, please visit [https:// www.jamsadr.com/eu-us-privacy-shield](https://www.jamsadr.com/eu-us-privacy-shield) for more information and to file a complaint.

If the complaint is not resolved by contacting the Supplier or through the independent dispute resolution process, the Data Subject may choose to invoke binding arbitration before the Privacy Shield Panel to be created by the U.S. Department of Commerce and the European Commission or may contact the local Data Protection Authority. The Supplier is subject to the investigatory and enforcement powers of the United States Federal Trade Commission.

## Appendix 1

### Data Recipients in Third Countries

The following organizations in third countries could get access to Personal Data in certain cases. It has been ensured that these organizations provide an adequate level of data protection according to the General Data Protection Regulation (GDPR) either by relying on the EU - U.S. Privacy Shield and the Swiss – U.S. Privacy Shield Principles (“PSP”) and/or in some cases additionally standard contractual clauses (“SCC”) have been signed.

#	Country	Name	Address	Legal Mechanism
1	Australia	Software AG Australia Pty Ltd.	201 Miller Street, Level 16 North Sydney, NSW 2060	SSC
2	Australia	Software AG Cloud APJ PTY Ltd.	Level 16, 201 Miller Street North Sydney, NSW 2060	SSC
3	Bahrain	Software AG (Gulf) S.P.C.	Office No. 31, 3rd Floor, Building No. 1269, Road No. 3227, Block 332 Manama	SSC
4	Brazil	Software AG Brasil Informatica e Serviços Ltda	Av. das Nações Unidas 12.901, 33° andar, Torre Norte CEP 04578-000 São Paulo/SP	SSC
5	Chile	Software AG Factoria S.A.	La Concepción 141, Piso 8, Oficina 808, Santiago de Chile, CP8320176	SSC
6	China	Software AG Limited	Room 1701-2, 17/F, No. 8 Fleming Road, Wanchai, HongKong	SSC
7	India	Software AG Chennai Development Center India Pvt Ltd	VBC Solitaire, 4th Floor, No. 47 & 49, Bazulla Road, T. Nagar 600 017 Chennai	SSC
8	India	Software AG Bangalore Technologies Private Ltd.	Embassy Tech Village 5th and 6th Floor, 2A East Tower, Marathahalli Outer Ring Road 560 103 Devarabisanahalli Bangalore	SSC
9	Japan	Software AG Ltd. Japan	AKASAKA K-Tower 4F, 1-2-7 Motoakasaka 107-0051 Minato-ku, Tokyo	SSC
10	Malaysia	Software AG	Suite 2B-22-1, Level 22, Block	SSC

		Operations Malaysia Sdn Bhd.	2B, Plaza Sentral, Jalan Stesen Sentral 5, Kuala Lumpur Sentral, 50470 Kuala Lumpur		
11	Mexico	Software AG, S.A. de C.V.	Blvd Manuel Avila Camacho No. 88 Piso 11, Torre Picasso, Col. Lomas de Chapultepec 11590 Mexico, Distrito Federal	SSC	
12	Philippines	Software AG, Inc.	12F Multinational Bancorporation Centre, Ayala Avenue, 1225 Makati City	SSC	
13	Russia	Limited Liability Company Software AG	Kosmodamianskaya Naberezhnaya, 52, building 4, 3rd floor, 115054 Moscow	SSC	
14	Singapore	Software AG Pte LTD	12 Marina Boulevard #17-04, Marina Bay Financial Centre Tower 3, 018982 Singapore	SSC	
15	South Africa	Software AG South Africa (Pty) Ltd	Culross on Main Office Park, 34 Culross Road, Building 3, 2021 Bryanston	SSC	
16	Turkey	Software AG Bilgi Sistemleri Ticaret A.S.	Degirmen Yolu Sok. No: 4, Sasmaz Plaza Kat: 9, TR- 34742 Istanbul	SSC	
17	United Arab Emirates	Software AG International FZ- LLC	Star Building, EIB 4, Office # 204, P.O. Box # 502274, Dubai	SSC	
18	USA	Amazon Web Services, Inc.	410 Terry Avenue North Seattle WA 98109	SSC	PSP
19	USA	Software AG Cloud Americas, Inc.	1209 Orange Street Wilmington , DE 19801	SSC	PSP
20	USA	Software AG Government Solutions, Inc.	11700 Plaza America Drive, Suite 700 Reston, VA 20190	SSC	
21	USA	Software AG USA, Inc.	11700 Plaza America Drive, Suite 700 Reston, VA 20190	SSC	PSP

## Appendix 2

### DATA SUBJECT RIGHTS

Under applicable law, the Data Subject has the right under certain circumstances to (1) request information about stored Personal Data, (2) rectification of Personal Data, (3) restriction of processing of Personal Data, (4) deletion of Personal Data, (5) data portability, (6) revocation of consent for processing of Personal Data and (7) object to the processing of Personal Data. In Detail this is:

- 1 **Right to information:** The Data Subject may have the right to ask the Supplier for confirmation of the processing of Personal Data in question and, if so, of the right to information about such Personal Data. The right to information includes, among other things, the processing purposes, the categories of Personal Data being processed and the recipients or categories of recipients to whom the Personal Data is disclosed. The Data Subject may also have the right to receive a copy of the Personal Data that is the subject of the processing. However, this right is not unrestricted, as the rights of others may limit the Data Subject's right to receive a copy.
- 2 **Right to rectification:** The Data Subject may be entitled to request the correction of incorrect Personal Data concerning the Data Subject. In consideration of the purposes of processing, the Data Subject has the right to request the completion of incomplete Personal Data, including by means of a supplementary statement.
- 3 **Right to erasure ("Right to be forgotten"):** Under certain conditions, the Data Subject has the right to ask the Supplier to delete Personal Data.
- 4 **Right to restriction of processing:** Under certain circumstances, the Data Subject has the right to demand that the Supplier restricts the processing of Personal Data. In this case, the corresponding data will be marked and processed by the Supplier only for specific purposes.
- 5 **Right to data portability:** Under certain circumstances, the Data Subject has the right to receive the Personal Data relating to him/her that the Data Subject has provided to the Supplier in a structured, commonly used and machine-readable format and the Data Subject has the right to transfer that data to another person without obstruction by the Supplier.
- 6 **Right to revocation of consent:** If the Data Subject has given consent for some data processing activities, he/she may revoke such consent at any time with future effect. Such revocation shall not affect the lawfulness of the processing on the basis of the consent until the revocation.
- 7 **Right to object:** For reasons arising from the Data Subject's particular situation, he/she has the right to object to the processing of Personal Data relating to him/her on the basis of Art. 6(1f) GDPR (data processing based on legitimate interests). If the Data Subject objects, the Supplier will no longer process his/her Personal Data unless compelling legitimate grounds for processing

that outweigh the Data Subject's interests, rights and freedoms can be established or the processing is for the purposes of asserting, exercising or defending legal claims.