External Worker Questionnaire

SAP and you will treat personal data only as set out herein.

This means in terms of **personal data relating to you** and which SAP requires enabling you to work on SAP's behalf:

- Data controller is the SAP Group entity on whose behalf you are working ("SAP"). If you have any questions regarding the identity of this entity or its contact details, please direct them to SAP_External_Workforce_Center@sap.com. Data protection officer of the SAP Group is Mathias Cellarius (privacy@sap.com).
- SAP will only store your personal data for as long as it is required to enable you to work on SAP's behalf, plus, where required, any applicable statutory retention periods.
- Kindly note that the personal data requested below, or which is otherwise required for SAP enabling you to work on SAP's behalf is mandatorily required for administrative purposes. As a consequence, without this data you cannot work on SAP's behalf.
- If you are a freelancer working on behalf of SAP, legal basis for SAP's use of your personal data is Article 6 para. 1 (b) GDPR (data processing for the purposes of conducting a contractual relationship with you). If you are an employee of a supplier of SAP, legal basis for SAP's use of your personal data is Article 6 para. 1 (f) GDPR (SAP's legitimate interest to properly track who is working on SAP's behalf).
- As part of a global group of companies, SAP has affiliates and third-party service providers within as well as outside of the European Economic Area (the "EEA"). As a consequence, whenever SAP is using or otherwise processing your Personal Data for the purposes set out in this External Worker Questionnaire, SAP may transfer your Personal Data to affiliated and/or third-party service providers in countries outside of the EEA including to such countries in which a statutory level of data protection applies that is not comparable to the level of data protection within the EEA. Whenever such transfer occurs, it is based on the Standard Contractual Clauses (according to EU Commission Decision 87/2010/EC or any future replacement) in order to contractually provide that your Personal Data is subject to a level of data protection that applies within the EEA. You may obtain a redacted copy (from which commercial information and information that is not relevant has been removed) of such Standard Contractual Clauses by sending a request to privacy@sap.com.
- You may request at any time information about, the correction or deletion of your personal data, the restriction of SAP's further use of your personal data, a copy of your personal data (where SAP is using your personal data for the purposes of conducting a contractual relationship with you) or object against SAP's further processing of your personal data (where SAP's use of your personal data is based on SAP's legitimate interest). In case you request the deletion of your personal data or object against SAP's use of your personal data, SAP will stop using your personal data and delete it, unless SAP is by law required to retain your personal data or can demonstrate a prevailing interest to further use it. Please direct any such request to SAP_External_Workforce_Center@sap.com.
- If you take the view that SAP is not using your personal data in accordance with the above statements or applicable data protection laws, you may at any time raise a complaint with the data protection authority of the country where you live or where SAP has its registered seat.

This means in terms of **any personal data (e.g. customer data, employee data) to which you gain access** while working on SAP's behalf that you:

- Keep all personal data to which you have access, or which is otherwise provided to you strictly confidential during and even after the termination of your engagement with SAP ("Data Secrecy").
- Only use, access or otherwise process personal data as instructed by SAP and only for the specific

tasks to be performed on SAP's behalf.

- Process, access or otherwise use any personal data only in accordance with all statutory and internal regulations (in particular SAP's Global Data Protection and Privacy Policy) regarding the handling and protection of personal data and comply with all of SAP's technical and organizational measures regarding data security.
- 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.

Violations of the above obligations can lead to administrative fines and/or have severe consequences for the contractual relationship between you or your employer and SAP including termination of contracts and claims for damages.

Please inform cybersecurity@sap.com immediately of any personal data breaches you become aware of.

With signing this questionnaire, you acknowledge its contents. In addition, you acknowledge your duty to Data Secrecy and the regulations of the General Data Protection Regulation (GDPR) outlined in Appendix I hereto.

Your email address _____

Have you previously worked for SAP as an employee? YES ☐ NO ☐

If YES, please list your last known I/D | | | | | | | | number

Have you previously been engaged as an External Worker for SAP? YES ☐ NO ☐

If YES, please list your last known C Number and Security ID:

Previous C-user ID: | C | | | | | | | |

Previous Security ID: | | | | | | | | | | |

If you do not remember your previous C Number, then please list your name or alias from your previous engagement with SAP below.

FIRST NAME: | | | | | | | | | | | | | | | | | | | | |

LAST NAME: | | | | | | | | | | | | | | | | | | | | |

KNOWN-AS OR NICKNAME: | | | | | | | | | | | | | | | | | | |

Please create a Security ID
FFMMDDZZZZ where:
FF: First 2 characters of First Name
MMDD: 2 digit birth month followed by 2 digit birth day
ZZZZ: Last four digits of Govt. issued ID, if no Govt. ID then last 4 digits of the passport

| | | | | | | | | | |

Signature:_____Print Name:_____Date:_____

Appendix I – Extracts from 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. 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 (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.