SOLUTION PLUS
+49 176 47658461
info@solutionplus.io
solutionplus.io
Kollwitzstraße 76
10435 Berlin, Germany

Version 3.2 · November 2026

Data Processing Agreement

pursuant to Article 28 GDPR, based on the EU Standard Contractual Clauses for controllers and processors (Commission Implementing Decision (EU) 2021/915)

concluded as part of the [contract / offer, number and date] (the **"Service Agreement"**)

between

[Client legal name], [address]
– the **"controller"** –

and

SolutionPlus UG (haftungsbeschränkt), Kollwitzstraße 76, 10435 Berlin, Germany, Amtsgericht Charlottenburg HRB 291768 B, represented by its managing director Saif Ur Rehman Qureshi
– the **"processor"** –

– together the "Parties"; contact details and signatures in Annex I –

Structure of this Agreement

Part	Content
Part A	The Standard Contractual Clauses between controllers and processors adopted by the European Commission (Implementing Decision (EU) 2021/915 of 4 June 2021), reproduced **without change** except for the options selected below (Clause 2(a)).
Part B	Supplementary provisions agreed under Clause 2(b): the EU data boundary and access levels, controlled remote access for Level C (B.2a), time limits, audits, authority requests, deletion, liability, law and jurisdiction. They do not contradict Part A; if they ever did, Part A prevails (Clause 4).
Annexes I–IV	List of parties, description of the processing, technical and organisational measures, sub-processors.
Annex V	Summary of the transfer impact assessment for the sub-processors in Pakistan and the United Arab Emirates (Clause 7.8, Chapter V GDPR).

Options selected in Part A

Clause	Selection
1(a), 8(c)(4), 9.1, 9.2	Option 1: Regulation (EU) 2016/679 (GDPR)
5 (docking clause)	Included
7.7(a)	Option 2: general written authorisation; time period **30 days**

How we work: at a glance

- **Contracting party:** SolutionPlus UG, Berlin, is your processor and answers to you for everyone working on your project, including sub-processors (Clause 7.7(d)).
- **Location:** your production systems and personal data are hosted in the EU/EEA.
- **Level A:** only our team members located in the EU/EEA access personal data.
- **Level B:** our delivery partner in Pakistan and, where Annex IV names it, our affiliated company in the United Arab Emirates (Solution Plus Tech Consultancy FZE) work on code and test systems with synthetic or anonymised data. They have no access to personal data or to production systems. No transfer of personal data takes place.
- **Level C:** access by a named person of a sub-processor outside the EU/EEA only on your documented instruction, for one task and a limited time, under the Standard Contractual Clauses for transfers (Module Three) and the safeguards in Annex V. Typical case: a security incident. Access is display-only, through an encrypted VPN to a locked-down virtual desktop in the EU; copying, download and printing are disabled; every session is logged and recorded (B.2a).
- **Applicable law:** the GDPR and the German Federal Data Protection Act (BDSG) apply to all processing under this Agreement. Pakistan has no comprehensive data protection act in force; the United Arab Emirates has Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (PDPL). The EU has no adequacy decision for either country, which is why Level B is the default (Annex V).
- **Time limits:** 30 days' notice of new sub-processors; breach notification within 24 hours; deletion within 30 days after the end.

Figures 1 and 2 illustrate Part B, section B.2. The binding terms are the text of Parts A and B and the Annexes.

FIGURE 1 · DATA FLOW AND THE EU DATA BOUNDARY

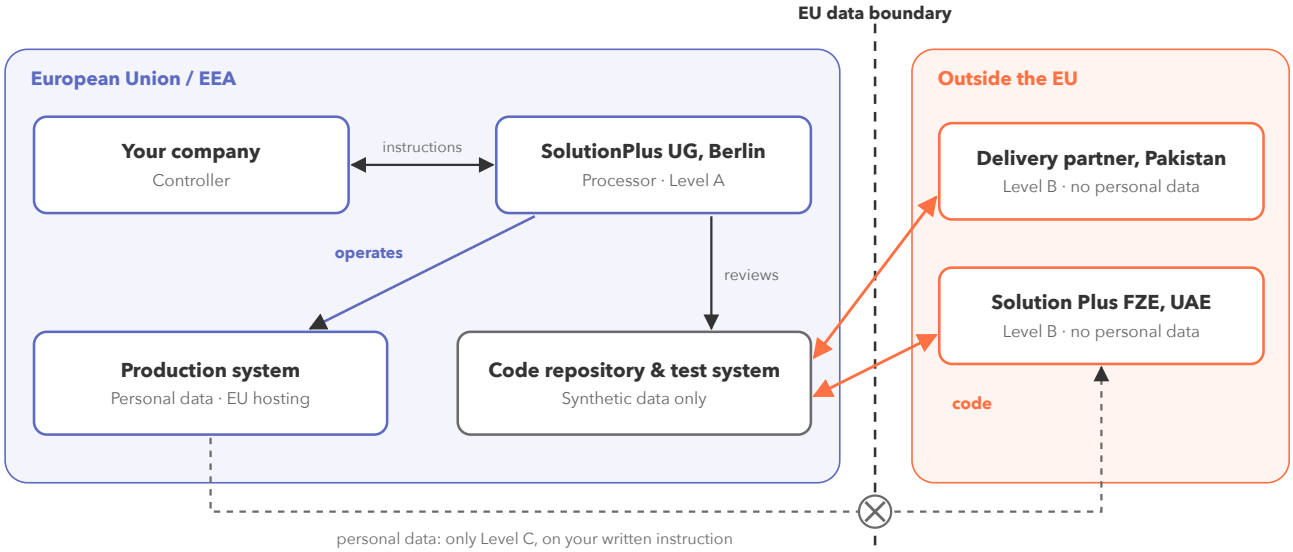
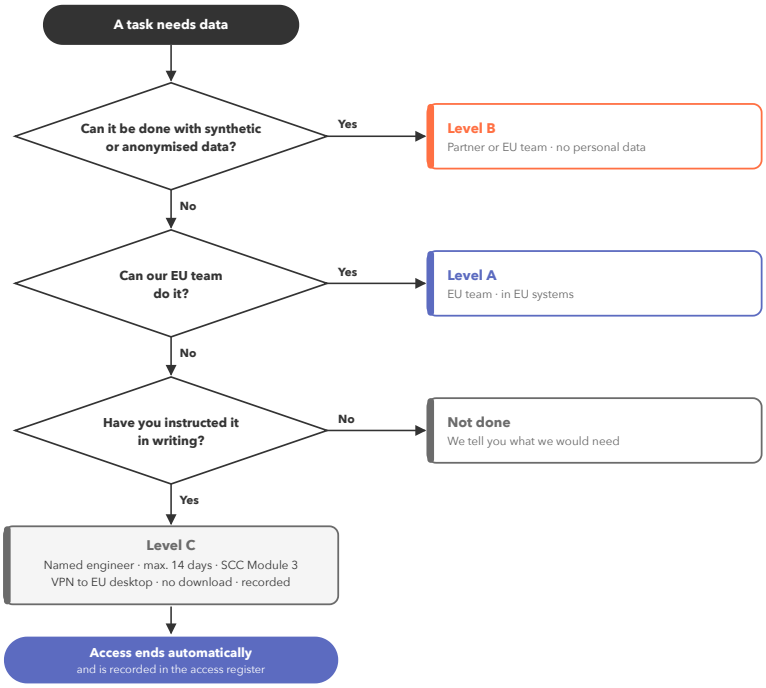


FIGURE 2 · WHO MAY SEE PERSONAL DATA: THE ACCESS-LEVEL DECISION



Part A – Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/915)

Reproduced from the Official Journal (OJ L 199, 7.6.2021, p. 18) without change, except for the options selected on page 1 (Clause 2(a)). Source: EUR-Lex, © European Union, https://eur-lex.europa.eu.

SECTION I

Clause 1 Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2 Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3 Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Optional Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6 Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7 Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) **GENERAL WRITTEN AUTHORISATION:** The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8 Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9 Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10 Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

Part B — Supplementary provisions (Clause 2(b))

B.1 Relationship to Part A and to the Service Agreement

1. Part B adds to Part A. It does not modify Part A and shall be read in accordance with it. In the event of a contradiction, Part A prevails (Clause 4).
2. In matters of data protection, this Agreement prevails over the Service Agreement. This Agreement applies for as long as the processor processes personal data on behalf of the controller.
3. This Agreement does not apply to personal data that the processor processes as a controller of its own, such as contact data of the controller's staff used for contract administration and invoicing.

B.2 EU data boundary and access levels

1. Personal data is stored and processed in the European Union or the European Economic Area. Hosting locations are listed in Annex IV.
2. The processor organises access to personal data in three levels (Figures 1 and 2):
   a. **Level A — EU team.** Access to production systems, to personal data and to screens showing personal data (including support sessions, screen-sharing and meetings) is limited to employees and freelancers of the processor who are located in the EU/EEA at the time of access, on a need-to-know basis (Clause 7.4(b)).
   b. **Level B — outside the EU/EEA, without personal data.** The delivery partner in Pakistan and, where Annex IV names it, the processor's affiliated company in the United Arab Emirates work on source code, design, documentation and development and test systems that contain only synthetic or anonymised data. Level B staff have no accounts on, no access to and no technical path to production systems or other systems containing the controller's personal data, and receive no copies of it. Information that does not relate to an identifiable natural person is not personal data (Recital 26 GDPR); its use is not a transfer under Chapter V GDPR.
   c. **Level C — exception on instruction.** Access to personal data by persons located outside the EU/EEA takes place only on the controller's documented instruction (Clauses 7.1 and 7.8(a)) for a specific task, by named persons and for a period stated in the instruction, under the conditions of B.2a, the safeguards in B.4 and Annex V. Access ends automatically at the end of that period.
3. Level A staff may work from home or while travelling within the EU/EEA under the measures in Annex III. Access to personal data by a Level A person while temporarily outside the EU/EEA requires the controller's prior consent in text form.
4. The processor records every Level C access (who, which data, when, why, on whose instruction) in an access register and makes it available to the controller on request.

B.2a Level C: controlled remote access

1. **Purpose and exception.** Level C is an exception. It is permitted only where a specific task cannot be performed at Level A or Level B in the time it requires, in particular to investigate, contain or remedy a personal data breach, a security incident or an exploitable vulnerability, or to analyse a fault that occurs only with production data. Level C is not used for routine development, testing or support.
2. **Authorisation in text form.** No Level C access takes place without a prior Level C authorisation. This rule has no exception, including for urgent incidents and outside business hours.
   a. A Level C authorisation is a documented instruction of the controller (Clauses 7.1 and 7.8(a)) in text form (§ 126b BGB; e-mail or ticket is sufficient), given by a person authorised to give instructions in Annex I.
   b. It states: the task and its purpose; the systems and categories of personal data concerned; the sub-processor (which must be authorised in Annex IV) and the named persons; whether changes are allowed (paragraph 9(a)); whether sensitive data is included (paragraph 9(c)); the start and end of the access period; and any additional conditions.
   c. The access period is as short as the task requires and at most 14 days. It is extended only by a new authorisation.
   d. The processor may propose an authorisation and states in the proposal why Level A or Level B is not sufficient and what residual risk remains (paragraph 11(c)). The controller decides freely and may refuse.
   e. Until an authorisation is received, the processor continues the work at Level A or Level B only. The controller may name an emergency contact in Annex I for this purpose.
   f. If the processor has reason to doubt that an authorisation is genuine, for example because the controller's e-mail system is affected by the incident, it confirms the authorisation by calling the verification number in Annex I before enabling access.
3. **Withdrawal and refusal.** The controller may withdraw or restrict an authorisation at any time in text form, without giving reasons. The processor then ends open sessions and disables the accounts without undue delay, at the latest within 24 hours, and confirms this in text form. The processor does not carry out Level C access if the conditions of this section cannot be met, and informs the controller.
4. **Access path.** Level C access takes place exclusively as follows:
   a. *Encrypted tunnel.* The authorised person connects through an encrypted and mutually authenticated VPN tunnel to a VPN gateway hosted in the EU/EEA. The gateway is operated by the processor, by the controller or by a provider listed in Annex IV. The processor documents the protocol and configuration used.

b. *EU session host.* From the gateway, the person reaches only a hardened virtual desktop or session proxy hosted in the EU/EEA (the "EU session host"), with a personal account and multi-factor authentication (authenticator app or hardware key, not SMS). All tools used for the task (shell, database client, administration console) run on the EU session host. No direct connection from the person's device to a production system, database or API is possible.

c. *Display only.* Personal data is stored and processed only on systems in the EU/EEA. Only the screen image is sent to the person's device, and only keyboard and mouse input is sent back.

d. *No copy functions.* Clipboard, file transfer, drive, printer and USB redirection are disabled on the EU session host. Its outbound connections are limited to the systems named in the authorisation, so that it cannot reach e-mail, messaging, file-sharing or other internet services.

e. *Device and place.* Access is made from a company-owned device of the sub-processor with full-disk encryption, a supported and updated operating system, malware protection and automatic screen lock, used in a non-public place. The sub-processor confirms this in text form for each named person before first access.

5. **Accounts and time limits.** Level C accounts are personal, disabled by default and enabled by a Level A person of the processor only for the access period. They are limited to the systems and rights needed for the task, expire automatically at the end of the period, and are disabled earlier as soon as the task is complete. Idle sessions are disconnected automatically.

6. **Logging and recording.**

   a. The gateway and the EU session host log every Level C session: person, start and end time, source IP address and systems accessed. In addition, the session is recorded (screen recording or command and query log), unless the controller waives recording in the authorisation.

   b. Logs and recordings are stored in the EU/EEA in a location where the authorised persons and the sub-processor have no write or delete rights.

   c. Session logs are kept for 12 months and recordings for 90 days, unless the controller specifies another period or they are needed for an ongoing investigation. They are then deleted.

   d. Logs and recordings are used only to verify compliance and to investigate incidents. Only Level A persons and the controller have access to them. The processor provides them to the controller on request within 5 working days.

   e. The authorised persons are informed in advance that sessions are logged and recorded.

   f. Each authorisation and each session is entered in the access register (B.2(4)).

7. **End of access.** Within 5 working days after the end of the access period, the processor confirms to the controller in text form that the accounts are disabled, and summarises the sessions held and the actions taken.

8. **Authority requests and changes in law.** B.7 applies. If a public authority contacts the sub-processor or an authorised person about the controller's data during or after a Level C access period, or if the processor learns of a change in law or practice that affects the assessment in Annex V, the processor suspends Level C access at once and informs the controller (B.4(3)).
9. **Minimisation.**
    a. Access rights are read-only unless the authorisation expressly allows changes.
    b. Masked or pseudonymised views are used where the task allows.
    c. Sensitive data (Clause 7.5) is excluded unless the authorisation expressly includes it.
    d. At the controller's request, a Level A person supervises the session live.
10. **Violations.** The processor treats the following as a security incident: any Level C access without a valid authorisation or outside the access path in paragraph 4, any attempt to circumvent these measures, and any loss or compromise of a device or credential used for Level C. In each case it suspends Level C access, informs the controller within the period in B.5, and handles the matter under Clause 9.2 where it is a personal data breach. The controller may exclude the persons or the sub-processor concerned from further Level C access.
11. **Legal nature.**
    a. The Parties acknowledge that remote access from a third country, including display on a screen, is a transfer of personal data under Chapter V GDPR, even though the data is not stored outside the EU/EEA.
    b. Level C access therefore takes place only under B.4(2) and with the measures in Annex V. This section adds to Part A and to the Standard Contractual Clauses under B.4(2) and does not limit them.
    c. The measures in paragraph 4 are designed to prevent the copying, download and onward transmission of personal data. They cannot prevent a person from reading, noting or photographing what is displayed. This residual risk is reduced by limiting access to named persons under written confidentiality obligations, by minimisation under paragraph 9, and by logging and recording under paragraph 6.
    d. The controller remains responsible for reflecting Level C transfers in its own records and privacy information. The processor provides the information needed.
12. **Flow-down.** The processor imposes the obligations of this section in writing on each sub-processor that may receive Level C access (Clause 7.7(b)) and remains fully responsible to the controller for their performance (Clause 7.7(d)).

B.3 Instructions

The Service Agreement and this Agreement are the controller's initial documented instructions. Further instructions are given in text form (e.g. e-mail or ticket) by the persons named in Annex I. Oral instructions are confirmed in text form without delay. The processor does not use personal data for its own purposes, for training artificial-intelligence models or for marketing.

B.4 Sub-processors and transfers

1. The notice under Clause 7.7(a) is given in text form at least 30 days in advance and states the sub-processor's name, location, services and access level. The controller may object on reasonable data protection grounds within that period. If the Parties cannot agree, the controller may terminate the affected services with effect from the date the change would take effect; until then the processor does not use the new sub-processor for the controller's personal data.
2. Level C access by a sub-processor located outside the EU/EEA takes place only after the processor (data exporter) and that sub-processor (data importer) have concluded the Standard Contractual Clauses for the transfer of personal data to third countries, Module Three (processor to processor), Commission Implementing Decision (EU) 2021/914 (Clause 7.8(b)). The processor has assessed the law and practice of Pakistan and the United Arab Emirates and applies the supplementary measures in Annex V. The full assessment is available to the controller on request.
3. If a transfer tool becomes invalid or can no longer be complied with, the processor stops the transfer without delay and informs the controller. The affected work continues at Level A or Level B only until the Parties agree on an alternative.
4. The sub-processor contracts contain the third-party beneficiary clause required by Clause 7.7(e).

B.5 Personal data breaches

The notification under Clause 9.2 is made without undue delay and in any event **within 24 hours** after the processor has become aware of the breach, to the breach contact in Annex I. Notification to the supervisory authority and to data subjects remains the controller's decision.

B.6 Audits (Clause 7.6)

1. The processor answers the controller's security questionnaires and provides documentation first. Where this is not sufficient, the controller or an independent auditor bound to confidentiality may carry out audits, including inspections, normally once per calendar year with at least 30 days' notice, during business hours and without unreasonable disruption. Where there are indications of non-compliance, after a personal data breach or at a supervisory authority's request, audits may take place at any time with reasonable notice.
2. Audits at the delivery partner may be carried out remotely.
3. Each Party bears its own costs of an audit. If an audit reveals a material breach of this Agreement by the processor, the processor bears the reasonable costs of the audit.

B.7 Requests from public authorities

If a public authority of a third country requests access to the controller's personal data from the processor or a sub-processor, the processor (and the sub-processor by contract) will, as far as legally permitted, inform the controller without delay, review the legality of the request, challenge it where there are reasonable grounds, disclose only the minimum required and document the request.

B.8 Return and deletion (Clause 10(d))

After the end of the services, the processor returns or deletes the personal data, at the controller's choice, within **30 days**, including copies held by sub-processors, unless Union or Member State law requires storage. Backups are overwritten in their normal cycle, at the latest within 90 days. The processor confirms the deletion in text form. Source code and documentation without personal data are governed by the Service Agreement.

B.9 Costs of assistance

Assistance under Clauses 8 and 9 is provided without separate charge where it results from the processor's sphere or from its statutory duties. Other assistance may be charged at the rates of the Service Agreement if announced in advance.

B.10 Liability

Liability towards data subjects is governed by Article 82 GDPR. Between the Parties, liability is governed by the Service Agreement, unless mandatory law provides otherwise.

B.11 Final provisions

1. Changes and additions to this Agreement must be made in text form (§ 126b BGB) and refer expressly to this Agreement. Annexes I and IV may be updated by notice under B.4.
2. This Agreement may be concluded in electronic form (Article 28(9) GDPR).
3. Should a provision of Part B be invalid, the remaining provisions remain valid.
4. Part B is governed by German law. If the controller is a merchant, a legal entity under public law or has no general place of jurisdiction in Germany, the place of jurisdiction is Berlin.

Annex I – List of parties

Controller	
Name	[Client legal name]
Address	[address]
Contact person, position, contact details	[name, position, e-mail, phone]
Persons authorised to give instructions	[name, e-mail]; deputy [name, e-mail]
Data protection officer (if any)	[name, e-mail]
Breach contact (B.5)	[e-mail, phone]
Level C: emergency contact and verification number (B.2a(2)(e)–(f))	[name, e-mail, phone reachable 24/7 — or "Level C not used"]

Processor	
Name	SolutionPlus UG (haftungsbeschränkt), Amtsgericht Charlottenburg HRB 291768 B
Address	Kollwitzstraße 76, 10435 Berlin, Germany
Contact person, position, contact details	Saif Ur Rehman Qureshi, Managing Director, info@solutionplus.io, +49 176 47658461
Persons authorised to receive instructions	Saif Ur Rehman Qureshi; deputy: the project lead named in the Service Agreement
Data protection officer	Not required (§ 38 BDSG: fewer than 20 persons regularly process personal data). Data protection contact: info@solutionplus.io
Breach contact (B.5)	info@solutionplus.io, +49 176 47658461

Place, date	Place, date
Controller — name, position	Processor — Saif Ur Rehman Qureshi, Managing Director, SolutionPlus UG (haftungsbeschränkt)

Annex II – Description of the processing

Item	Details
Categories of data subjects	☐ the controller's customers and end users ☐ the controller's employees ☐ prospects ☐ suppliers and business partners ☐ other: […]
Categories of personal data	☐ identification and contact data ☐ account and login data ☐ usage and log data (IP address, device, timestamps) ☐ contract and payment data ☐ content entered by users ☐ communication data ☐ location data ☐ other: […]
Sensitive data (Clause 7.5) and safeguards	☐ none ☐ health data ☐ other: […] If ticked: access at Level A only by named persons; Level C excluded unless the controller instructs otherwise expressly for this category; anonymisation before any use in test systems; access recorded in the access register.
Nature of the processing	☐ development and testing ☐ deployment and operation ☐ maintenance and bug fixing ☐ technical support ☐ data migration ☐ hosting ☐ AI features (provider in Annex IV) ☐ other: […]
Purpose(s)	Providing the services under the Service Agreement: [short description, e.g. development and operation of the web application "…"]
Duration	The term of the Service Agreement, plus the period for return and deletion (B.8).
Access levels used (B.2)	☑ Level A ☐ Level B ☐ Level C planned for: [task, period]
Processing by sub-processors	Delivery partner: Level B, no personal data; Level C only per documented instruction, for the task and period stated in it. Hosting and other providers: as listed in Annex IV, for the term of the Service Agreement.

Annex III – Technical and organisational measures

No.	Measure	Implementation
1	EU data boundary and access levels	Production systems and personal data hosted in the EU/EEA. Access per level (B.2): Level A for named EU-based persons; Level B partner staff without accounts on systems holding personal data; Level C only on documented instruction, time-limited, named and logged. Access lists reviewed at project start and end and at least quarterly.
2	Pseudonymisation and encryption	TLS 1.2 or higher for all connections; encryption at rest offered by the hosting provider enabled; full-disk encryption on all work devices; pseudonymised identifiers in logs and test data where possible.

No.	Measure	Implementation
3	Confidentiality, integrity, availability and resilience	Separate development, test and production environments with separate credentials; least-privilege roles; production rights only for the persons operating the system; dependency and vulnerability checks; hosting on established providers (Annex IV).
4	Restoring availability after an incident	Where the processor operates hosting: automated backups in the EU with defined retention and a tested restore procedure. Where the controller operates hosting, the controller is responsible for backups; code and configuration are kept in version control so the application can be redeployed.
5	Regular testing and evaluation	Review of these measures at least once a year and after significant changes (new tools, staff changes, incidents); access reviews as in No. 1.
6	User identification and authorisation	Personal accounts only, no shared accounts; multi-factor authentication wherever supported; password manager; access removed within 24 hours when a person leaves the project; secrets in a secrets store, never in source code, rotated when a person leaves.
7	Protection during transmission	No personal data by unencrypted e-mail, chat or removable media. Data exchanges (e.g. migration exports) only through encrypted channels agreed with the controller, deleted after use.
8	Protection during storage	No local copies of production data; an unavoidable temporary copy for a Level A task is encrypted, limited in scope and deleted after the task. No personal data in source code, tickets or screenshots.
9	Physical security	Lockable offices and home workplaces; devices not left unattended in public places; data-centre security of the hosting providers per their certifications.
10	Event logging	Access to production systems logged by the respective platform (e.g. cloud audit logs); Level C access additionally recorded in the access register (B.2(4)); logs kept for at least 6 months unless the controller specifies otherwise.
11	System configuration, including default configuration	Hardened standard configuration of work devices (current operating system, automatic updates, screen lock, endpoint protection, no default passwords); application configuration version-controlled; changes reviewed.
12	Internal IT and IT security governance	Named responsibility for access management and device security; written internal rules on passwords, handling of client data, incident reporting and use of AI tools; code review (four-eyes principle) before every release.
13	Certification and assurance	The processor holds no certification at present. Hosting providers are selected for recognised certifications (e.g. ISO/IEC 27001). The processor answers security questionnaires and accepts audits (B.6).

No.	Measure	Implementation
14	Data minimisation	Development and testing with synthetic or anonymised data; only the personal data needed for a task is accessed; no additional copies.
15	Data quality	Validation and plausibility checks in the application as specified with the controller; inaccuracies noticed in support are reported to the controller (Clause 8(c)(3)).
16	Limited data retention	Retention and deletion rules of the production system set by the controller and implemented as specified; temporary data on work devices deleted after the task, at the latest at project end; deletion per B.8.
17	Accountability	Documentation of access rights, instructions, Level C access register and these measures; written confidentiality commitment and instruction of every person (Clause 7.4(b)); refresher at least once a year.
18	Data portability and erasure	Export and deletion functions implemented in the application as specified with the controller; return or deletion of personal data under the processor's control per B.8.
19	Use of AI tools	AI tools used only with settings or contracts that exclude use of inputs for training; personal data of the controller is entered only into AI services listed in Annex IV.
20	Assistance to the controller (Clause 8)	Data subject requests forwarded within 2 working days; technical support for access, rectification, export and erasure in the application; information for data protection impact assessments on request.
21	Breach notification (Clause 9)	Notification within 24 hours (B.5) with, as far as available: time and type of the incident, systems and data affected, approximate number of data subjects and records, likely consequences, measures taken and proposed, contact person; updates without undue delay.
22	Controlled remote access (Level C)	Only on the controller's authorisation in text form (B.2a): named persons connect by encrypted VPN and multi-factor authentication to a virtual desktop or session proxy hosted in the EU/EEA, with clipboard, file, drive, printer and USB redirection disabled, outbound connections restricted and no direct path to production systems. Accounts are disabled by default and time-limited (at most 14 days); sessions are logged and recorded in EU storage that the persons accessing cannot alter (logs 12 months, recordings 90 days).

Annex IV – Sub-processors

The controller authorises the following sub-processors (Clause 7.7(a), Option 2). Tick the rows used in this project; add the project's hosting and service providers.

Use	Name and address	Location of processing	Description of the processing	Access level / transfer tool
☐	Tecsofiy Solutions (Pvt.) Ltd., [registered address], Lahore, Pakistan	Pakistan	Delivery partner: software engineering, design and quality assurance on development and test systems	Level B: no personal data, no transfer. Level C only on instruction: SCC Module Three (B.4, Annex V)
☐	Solution Plus Tech Consultancy FZE, Business Centre, Sharjah Publishing City Free Zone, Sharjah, United Arab Emirates (affiliated company)	United Arab Emirates	[role in this project]	Level B: no personal data, no transfer. Level C only on instruction: SCC Module Three (B.4, Annex V)
☐	Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg	EU, region [e.g. eu-central-1, Frankfurt]	Cloud hosting, databases, storage	EU; provider DPA
☐	Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland	EU	E-mail and collaboration (Microsoft 365) for project communication	EU; provider DPA
☐	[name, address]	[…]	[…]	[…]

Annex V – Transfer impact assessment: summary

Neither Pakistan nor the United Arab Emirates has an EU adequacy decision. Both sub-processors outside the EU/EEA therefore work at Level B by default: they have no accounts on, and no technical path to, systems containing the controller's personal data, so no personal data is transferred to them. This Annex governs a Level C exception only.

Item	Pakistan (delivery partner)	United Arab Emirates (affiliated company)
Adequacy decision (Art. 45 GDPR)	None.	None (European Commission list of adequacy decisions, checked 17 November 2026).
Local data protection law	No comprehensive data protection act in force; the Personal Data Protection Bill has not been passed by Parliament (status checked 16 November 2026: Chambers, *Data Protection & Privacy 2026 – Pakistan*; ICLG, *Data Protection Laws and Regulations 2026 – Pakistan*). Access by authorities is governed in particular by the Prevention of Electronic Crimes Act 2016.	Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (PDPL). It applies in the Sharjah Publishing City Free Zone, because it excludes only free zones with their own data protection legislation, such as the DIFC and ADGM (Article 2). Its executive regulations had not yet been issued (Chambers, *Data Protection & Privacy 2026 – UAE*, checked 17 November 2026). The EU has not recognised the PDPL as essentially equivalent; the processor does not rely on it to protect the controller's personal data.
What counts as a transfer	Making personal data available to a separate company in a third country, including remote access and display on a screen (EDPB Guidelines 05/2021 on the interplay between Article 3 and Chapter V GDPR, version 2.0 of 14 February 2023). The affiliated company is a separate legal entity; access by it is a transfer like access by the delivery partner.	
Assessment	The processor does not assume that contractual safeguards alone ensure an essentially equivalent level of protection for access in the clear from either country (cf. EDPB Recommendations 01/2020, version 2.0). It therefore uses Level B as the default for both: no personal data reaches the delivery partner or the affiliated company, and no transfer takes place.	
Transfer tool for Level C	Standard Contractual Clauses, Module Three, Commission Implementing Decision (EU) 2021/914, between the processor (exporter) and the sub-processor concerned (importer). No Level C access takes place before they are concluded.	

Item	Pakistan (delivery partner)	United Arab Emirates (affiliated company)
Supplementary measures for Level C	Access only under a Level C authorisation in text form for a defined task and period of at most 14 days, by named persons (B.2a). Access is display-only, through an encrypted VPN and a virtual desktop or session proxy hosted in the EU/EEA, with multi-factor authentication. Copy, file-transfer and print functions are disabled and outbound connections restricted, so the importer holds no stored copy of the data that could be handed over or seized. Masked or pseudonymised views are used where the task allows, with re-identification keys kept in the EU; sensitive data is excluded unless expressly authorised. Sessions are logged and recorded in the EU and entered in the access register. Access is suspended immediately at the end of the period, on withdrawal, on any authority request (B.7) or on a relevant change in law. Residual risk: displayed data is readable in the clear by the named persons and can be noted or photographed; the controller is told this before each authorisation and decides whether to accept it.	
Excluded from Level C unless expressly instructed	Sensitive data (Clause 7.5).	
Review	At least annually and whenever the legal situation in Pakistan or the United Arab Emirates changes, in particular if Pakistan enacts a data protection act or the UAE issues the PDPL executive regulations.	