The Linux Foundation
Community Meeting Organizer Data Processing Addendum

Last revised: June 24, 2026

This Data Protection Addendum ("**Addendum**") forms part of the Community Meeting Organizer Terms available at https://www.linuxfoundation.org/legal/community-meeting-terms (the "Agreement") between Organizer and TLF. Capitalized terms not defined herein will have the meaning given to them in the Agreement.

TLF and Organizer acknowledge that each of them may be a Controller of Personal Data that is Processed in connection with the performance of the Agreement:

- TLF, in its capacity (directly or via a TLF-supported entity) as the owner of the Project Marks applicable to Community Meetings, may designate for Organizer a Registration System to enable attendee registration and sign-ups for information about TLF and its projects and offerings.
- Organizer, in its capacity as the operator of Community Meetings under the Agreement, may receive access to the Registration System and Attendee Data for the purpose of operating the Community Meetings (the "**Permitted Purposes**").
- Categories of Personal Data: name, company, job function / title, email address, mailing address, and similar contact information
- Types of Data Subjects: registered attendees at Community Meetings operated by Organizer

TLF and Organizer desire to set forth their respective responsibilities regarding the Processing of Personal Data relating to the foregoing, and accordingly agree as follows:

1) **Definitions**. In this Addendum, the following terms will have the meanings set out below:

a) "**Controller**", "**Data Subject**", "**Personal Data Breach**", "**Process/Processing**", "**Processor**", and "**Special Categories of Personal Data**," or their equivalent terms under applicable Data Protection Laws, will have the same meaning as defined under applicable Data Protection Laws;
b) "**Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with either TLF or Organizer (as the context allows), where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;
c) "**CCPA**" means the California Consumer Privacy Act and any implementing regulations issued thereto, each as amended (including by the California Privacy Rights Act and any regulations promulgated thereto).
d) "**Data Subject Request**" means a request from a Data Subject to exercise any right under Data Protection Laws;
e) "**Data Protection Laws**" means all national, federal, state, provincial, local, and international privacy, cybersecurity and data protection laws applicable to the Processing of Personal Data under this Addendum, together with any implementing or supplemental rules and regulations, each as amended, including but not limited to, to the extent applicable, the CCPA and GDPR.
f) "**Deidentified Data**" means data that (i) is not linked or reasonably linkable to, and cannot reasonably be used to infer information about, a particular individual, household, or personal or household device; and (ii) is subject to reasonable measures to ensure that such data cannot be associated with a particular individual or household (including any or personal or household device), including by any recipient of such data.
g) "**EEA**" means the European Economic Area, and unless otherwise indicated, EEA or Member States of the EEA continues to include the United Kingdom following its exit from the European Union;
h) "**GDPR**" means 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 (known as the General Data Protection Regulation).
i) "**Personal Data**" means any information relating to an identified or identifiable natural person, as well as other information defined as "personal data," "personal information" or equivalent term under Data Protection Laws;
j) "**Restricted Transfer**" means a transfer of Personal Data from Discloser to Recipient (including any onward transfer between the establishments of such), to the extent such transfer would be prohibited or restricted by Data Protection Laws, or by the terms of data transfer agreements, in the absence of the Standard Contractual Clauses;
k) "**Standard Contractual Clauses**" means (i) the standard contractual clauses for the transfer of Personal Data to entities established in third countries as set out in Commission Decision C/2021/3972, with selections for Module One (Transfer Controller to Controller), as updated, amended, replaced or superseded from time to time by the European Commission, or (ii) any other contractual clauses or other mechanism approved by a Supervisory Authority or by Data Protection Laws for use in respect of such Restricted Transfer, as updated, amended, replaced or superseded from time to time by such Supervisory Authority or Data Protection Laws;
l) "**Supervisory Authority**" means (i) an independent public authority which is established by a Member State pursuant to GDPR, Art. 51; and (ii) any similar regulatory authority responsible for the enforcement of Data Protection Laws;
m) "**UK Data Protection Laws**" means the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ("UK GDPR"), together with the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 (as amended) and other data protection or privacy legislation in force from time to time in the United Kingdom. In this Addendum, in circumstances where and solely to the extent that the UK GDPR applies,

references to the GDPR and its provisions shall be construed as references to the UK GDPR and its corresponding provisions, and references to "EU or Member State laws" shall be construed as references to UK laws; and

n) "**UK IDTA**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018, as may be amended or replaced from time to time.

2) **Controllers**

a) The parties acknowledge that each will act as a separate Controller in relation to the Personal Data which they Process.
b) The parties will each comply with their respective obligations under Data Protection Laws in respect of their processing of Personal Data.

3) **Disclosing of Personal Data**. Where acting as a Discloser, each party will:

a) only disclose the Personal Data for one or more defined purposes which are consistent with the terms of the Agreement and the Permitted Purposes;
b) ensure that a notice has been made available and will continue to be accessible to the relevant Data Subject(s) informing them that their Personal Data will be disclosed to the Recipient or to a category of third party describing the Recipient;
c) ensure that it has obtained any necessary consents or authorizations required to permit the Recipient to freely Process the Personal Data for the Permitted Purposes;
d) not disclose any Special Categories of Personal Data to the Recipient; and
e) be responsible for the security of any Personal Data in transmission from the Discloser to the Recipient (or otherwise in the possession of the Discloser).

4) **Processing of Personal Data**. Where acting as a Recipient, each party will:

a) not Process Personal Data in a way that is incompatible with the Permitted Purposes (other than to comply with a requirement of applicable law to which Recipient is subject);
b) not Process Personal Data for longer than is necessary to carry out the Permitted Purposes (other than to comply with a requirement of applicable law to which Recipient is subject); and
c) taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, have in place appropriate technical and organizational security measures to protect the Personal Data against unauthorized or unlawful Processing, or accidental loss or destruction or damage.

5) **CCPA Obligations**. As a non-profit corporation, TLF is not a "business" for purposes of the CCPA. To the extent the CCPA applies to the Processing of Personal Data that one Party provides to the other Party, and without limiting other obligations herein, the following shall apply:

a) The Parties agree that the Parties disclose Personal Data to one another for the Permitted Purposes;
b) The Parties will (i) comply with all applicable Data Protection Laws in the Processing of Personal Data and shall provide the same level of privacy protection as is required by Data Protection Laws and this Addendum; and (ii) only Process Personal Data for the Permitted Purposes or as permitted or required by applicable Data Protection Laws;
c) If either Party believes it will be unable to comply with Data Protection Laws, such Party will promptly notify the other Party. Without limiting the foregoing, the Parties grant one another the right to take reasonable and appropriate steps: (i) to help ensure the Recipient uses Personal Data transferred in a manner consistent with Disclosing Party's obligations under Data Protection Laws; and (ii) to, upon notice, stop and remediate any unauthorized use and Processing of Personal Data. Upon request by a Party, the other Party will provide the information necessary to demonstrate compliance with this Addendum and the CCPA; and
d) To the extent the Parties receive or otherwise Processes Deidentified Data associated with, derived from, or otherwise related to Personal Data under the Agreement, the Parties will: (i) take reasonable measures to ensure that the Deidentified Data cannot be associated with an individual, household or device; (ii) publicly commit to maintain and use the information in deidentified form and not attempt to reidentify the information; (iii) otherwise comply with applicable requirements for retention and Processing of Deidentified Data under Data Protection Laws; and (iv) contractually obligate any further recipient to comply with all provisions of this Section 5(d).

6) **Personal Data Breaches**

a) The Recipient will notify the Discloser without undue delay following any Personal Data Breach involving the Personal Data.
b) Each party will co-operate with the other, to the extent reasonably requested, in relation to any notifications to Supervisory Authorities or to Data Subjects which are required following a Personal Data Breach involving the Personal Data.

7) **Further Co-operation and Assistance**. Each party will co-operate with the other, to the extent reasonably requested, in relation to (a) any Data Subject Requests; (b) any other communication from a Data Subject concerning the Processing of their Personal Data; and any communication from a Supervisory Authority concerning the Processing of Personal Data, or compliance with Data Protection Laws.

8) **Description of Personal Data**. The parties acknowledge that the Personal Data (a) may include the categories of personal data specified in the preamble to this Addendum, which do not include any Special Categories of Data (sensitive data); (b) are related to the types of Data Subjects specified in the preamble to this Addendum; and (c) are disclosed and transferred for the Permitted Purposes.

9) **Restricted Transfers**. With respect to any Restricted Transfers, the parties hereby enter into the Standard Contractual Clauses, which are incorporated by reference into this Addendum as follows:

a) Where personal data is disclosed by TLF, TLF (for itself and its relevant Affiliates) is the "data exporter" and Organizer and its relevant Affiliates are the "data importers."
b) Where personal data is disclosed by Organizer, Organizer and its relevant Affiliates are the "data exporters" and TLF (for itself and its relevant Affiliates) is the "data importer."
c) Both parties have the authority to enter into the Standard Contractual Clauses for themselves and their respective relevant Affiliates.
d) Clauses 17 (Option 1) and 18 of the Standard Contractual Clauses shall specify Belgium as the selected EU Member State.
e) Annex I to the Standard Contractual Clauses shall be deemed to be prepopulated with the relevant information in Section 8 of this Addendum, and the following contact information: (a) data exporter: the relevant data exporter's mailing address set forth in the preamble to the Agreement; and (b) data importer: the relevant data importer's contact information set forth in the preamble to the Agreement; for each, in the case of TLF, Attn: Legal Department.
f) Annex II to the Standard Contractual Clauses shall be deemed to be prepopulated with the following:
    A) Data importer has implemented commercially reasonable technical and organizational measures for protecting Personal Data, including with respect to its relevant information processing systems, and reasonable and appropriate technical, physical and administrative measures will be maintained to protect Personal Data under data importer's possession or control against unauthorized or unlawful Processing or accidental loss, destruction or damage, including:
        (1) employees and other personnel that regularly handle Personal Data receive privacy and security appropriate to their responsibilities;
        (2) documented policies, procedures and processes for managing the security risks related to Processing of Personal Data;
        (3) devices, systems, facilities and assets that Process Personal Data ("assets"), and that are material to the provision of the services, are identified and managed;
        (4) security risks are identified, and are assessed regularly;
        (5) access to assets is limited to authorized users;
        (6) access logs are collected and reviewed as appropriate;
        (7) remote access to assets is restricted and securely managed;
        (8) Personal Data is physically and logically separate from the Personal Data of other clients/customers/partners;
        (9) electronic and paper records containing Personal Data are securely destroyed in accordance with secure destruction policies and procedures;
        (10) appropriate technical security solutions are implemented and managed to protect the confidentiality, integrity and availability of Personal Data;
        (11) maintenance and repair of information system components is performed in a controlled and secure manner;
        (12) incident response processes and procedures are maintained to provide for timely identification of, response to, and mitigation of detected Personal Data Breaches; and
        (13) backups and disaster recovery processes are in place.
    B) Reasonable steps will be taken in an effort to ensure the reliability of personnel having access to Personal Data.
    C) Appropriate due diligence will be conducted on subprocessors to ensure that each is capable of providing an appropriate level of protection for Personal Data.
g) Although Organizer and TLF intend that this Addendum shall be deemed to include the Standard Contractual Clauses as set forth in this Section 9, upon either Party's request Organizer and TLF shall execute a separate copy of the Standard Contractual Clauses, with such selections as set forth herein.
h) To the extent UK Data Protection Laws apply, the Standard Contractual Clauses shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK IDTA, and the Parties confirm that the information required for the purposes of Part 1 (Tables) of the UK IDTA is as set out in the Agreement and/or in this Addendum.
i) The parties agree that, with respect to Swiss Personal Data, the Standard Contractual Clauses will apply amended and adapted as follows:
    A) the Swiss Federal Data Protection and Information Commissioner is the exclusive supervisory authority;
    B) the term "member state" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18; and
    C) references to the GDPR in the Standard Contractual Clauses shall also include the reference to the equivalent provisions of the Swiss Federal Act on Data Protection (as amended or replaced).

10) **Governing Law and Jurisdiction**. Without prejudice to clauses 17 and 18 of the Standard Contractual Clauses:

a) the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and
b) this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.