Presidential Policy

AFS Intercultural Programs, Inc.

LAST UPDATED: 30 November 2018

AFS Network Data Protection Policy

AFS needs to collect and use certain personal data in order to conduct its activities, including organizing AFS exchange programs, orientations, outreach and trainings. This can include personal data of volunteers, participants, online users, host families, natural families, employees, and other people that AFS has a relationship with or may need to contact. AFS may collect and process special categories of personal data to provide its services, such as health related data. AFS also processes data of minors, which requires special safeguards and in certain cases legal guardians' consent.

While each AFS Network Organization, as a separate legal entity, remains fully responsible for its own local and international compliance with any applicable privacy and data protection laws, such as the GDPR, this policy describes certain minimum standards that INT and each AFS Network Organization must follow in connection with collecting, using, storing, sharing and deleting personal data to meet AFS network standards, comply with certain laws, and safeguard personal data of AFS stakeholders.

As a highly interconnected Network involving regular international data transfers, AFS requires a very coordinated effort to maintain and protect AFS stakeholders' data and ensure continuing compliance with different data protection laws around the globe, including laws about international data transfers.

Everyone that handles personal data in connection with conducting tasks for AFS has some responsibility for ensuring that data is collected, stored and handled properly and that individual rights of data subjects are respected. In the GDPR context, depending on the set of data and type of processing operation, INT and each Network Organization can be deemed a data controller or data processor or joint-controllers, and thus be subject to specific obligations reserved to those respective categories of organizations.

You can reach out to the INT data protection team at any point with questions about this policy by sending an email at **privacy@afs.org**. If you have any doubt about your organization's national and international legal obligations you should also always check with your local lawyer/data protection expert.

1. Definitions

AFS Network Organizations	Each legally separate organization licensed by INT to use the AFS brand in connection with AFS programs, as detailed in the AFS Articles of Partnership.
AFS Network	The international network composed of all AFS Network Organizations
INT	AFS Intercultural Programs, Inc., based in New York.
AFS	AFS Network Organizations and INT, collectively.
GDPR	The EU General Data Protection Regulation.
Data Protection Responsible	The person designated by each AFS Network Organization as being responsible to monitor and support compliance with the data protection obligations of such organization. In some cases the Data Protection Responsible will also be a Data Protection Officer[1] for those organizations that appoint one to comply with GDPR legal requirements, national requirements, or good practices.
Registry of Data Processing Activities	A registry of all personal data processing activities conducted, including systems or contexts in which personal data is processed and safeguards implemented to protect the data.
Personal Data (or 'data').	Any information relating to an identified or identifiable natural person ('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, etc.
'processing'	Any operation/s which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, storage, alteration, retrieval, consultation, use, erasure, etc.
'controller'	A natural or legal person which, alone or jointly with others, determines the purposes and means of the processing. Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide sufficient guarantees that the requirements of the GDPR will be met and the rights of data subjects protected.
'processor'	A natural or legal person which processes personal data on behalf of the controller.
Data Processing Agreement	The agreement between a controller and a processor defining their data protection roles and responsibilities. See the Appendix for standard content.

[1] GDPR Art. 37 requires to a DPO if company core activities consist of processing operations which:

- require **regular and systematic monitoring of data subjects on a large scale**; or
- consist of **processing on a large scale of special categories of data** [e.g. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited], or personal data relating to criminal convictions and offences.

2. Data Protection Principles

AFS takes privacy of its stakeholders very seriously and is committed to processing data in accordance with its responsibilities under the GDPR and other national and international data protection laws as they may apply to AFS operations.

Accordingly, personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

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

e. kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of appropriate technical and organisational measures in order to safeguard the rights and freedoms of individuals; and

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

3. General provisions

b. **Scope.** This policy applies to all personal data processed by AFS. Additional INT policies apply to specific or related matters (e.g. Record Retention and Deletion Policy, Data Breach and Incident Response Policy, Social Media Policy, etc.). Also each AFS Network Organization might adopt additional policies and procedures for its own compliance purposes.

b. **Accountability**. Each AFS Network Organization shall appoint a Data Protection Responsible (DPR) to take responsibility for and support the respective organization's ongoing compliance with this policy and with its data protection obligations.

The DPR works closely with ICT, marketing, HR, and other departments or staff and volunteers to monitor and support compliance. The DPR also provides training to staff and volunteers and conducts internal audits and privacy impact assessments as needed. The DPR has a key role in data breach response and compliance with data breach notice requirements.

INT Data Protection Officer (DPO) is the DPO for AFS Intercultural Programs, Inc. only (the NY entity) and it is not the DPO of any Network Organization. The INT DPO works closely with each DPR to ensure Network compliance with this policy.

4. Lawful, fair and transparent processing

a. To ensure their processing of data is lawful, fair and transparent, INT and each AFS Network Organization shall maintain its Registry of Data Processisng Activities.

b. The Registry shall be reviewed at least annually.

c. In most cases individuals have the right to access their personal data and to enforce other data subjects' rights (such as the right to request rectification or erasure of their data or to object the processing of their data); any such requests made to AFS shall be dealt with in a timely and coordinated manner (see section 10 below).

d. To provide clear and transparent information to individuals, including in the context of gathering consent, INT and each AFS Network Organization shall use adequate privacy notices, including online forms and online privacy policies for each AFS website, in clear, concise, plain language.

5. Lawful bases for processing

a. All data processed by AFS must be done on the basis of lawful grounds, such as consent, contract relationship (e.g. participation agreement), legal obligation, vital interests, public task or legitimate interests.

b. Each AFS Network Organiztaion shall note the appropriate lawful basis of each type of processing activity in its Registry of data procesisng activities.

c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept in connection with the personal data of each individual.

d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected and stored accurately in AFS systems and platforms.

6. Data minimization & archiving/removal of data

a. AFS shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

b. The only people (employees, consultants, volunteers, etc.) able to access personal data should be those who need it for their work or performance of tasks assigned by AFS.) Personal data should be kept secure and should not be disclosed to unauthorized people, either within AFS or externally.

b. To ensure that personal data is kept for no longer than necessary, INT and each AFS Netowrk Organiztaion shall maintain a record retention policy compliant with applicable laws. This document will address what data should/must be retained, for how long, and why. AFS Network Organizations adopting record retention policies that have different retention periods than those included in the INT policy for the same category of data shall closely coordinate their needs with INT as they relate to data centrally stored by INT, which is subject to the INT record retention policy.

7. Accuracy

a. AFS shall take reasonable steps to ensure personal data is accurate.

b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date, in line with the rules included in the AFS Global Retention and Deletion Module, as updated by INT from time to time.

8. Security

a. AFS shall ensure that personal data is stored securely using modern software that is kept-up-to-date.

b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

c. When personal data is deleted this should be done safely such that the data is irrecoverable.

d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

a. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, AFS shall promptly assess the risk to people's rights and, if appropriate, report this breach to the relevant authorities and individuals, as detailed in the AFS Data Breach Policy.

10. Data Subject Rights and requests

a. AFS (INT or AFS Network Organizations, depending on who receives the request) must timely address any request received from individuals exercising their data protection rights, such as the request to access their data, or erase it ('right to be forgotten'). Each AFS Network Organiziation shall notify INT (via email to privacy@afs.org) of erasure requests, so that all appropriate steps can be taken to address and record the request.

11. International Transfer of Personal Data

When transferring data to a third country, AFS will ensure that adequate safeguards are in place and that that there is a lawful basis for the transfer (for example when transferring EU data to a country outside the European Economic Area - EEA, the transfer will be made on the basis of consent, EU Model Clauses, Binding Corporate Rules, or another legal basis allowed under GDPR).

12. Outsourcing Processing of Personal Data

a. When engaging outsourced services of a vendor/service provider that qualifies as a data processor, INT or the AFS Network Organization hiring the processor will complete due diligence to ensure that the processor offers adequate levels of security and data protection, and will execute a controller-processor Data Processing Agreement, as applicable.

b. If the processor's performance of the services involves a data transfer, section 11 above also applies.

13. Training

Training of AFS staff and volunteers is a key component, and in some cases a legal requirement, to ensure adequate protection of personal data of AFS participants and other AFS stakeholders. INT and AFS Network Organizations will collaborate to execute data protection trainings on a regular basis.

Appendix - Data Processing Agreement Content

Under GDPR, Data Processing Agreements have to be in writing and must include the following compulsory details:

☐ the subject matter and duration of the processing;

☐ the nature and purpose of the processing;

☐ the type of personal data and categories of data subject; and

☐ the obligations and rights of the controller.

Also, they must include the following compulsory terms:

☐ the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);

☐ the processor must ensure that people processing the data are subject to a duty of confidence;

☐ the processor must take appropriate measures to ensure the security of processing;

☐ the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;

☐ the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;

☐ the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;

☐ the processor must delete or return all personal data to the controller as requested at the end of the contract; and

☐ the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.