vFairs GDPR Compliance

Policy Owner: vFairs Technical Director / vFairs Data Protection Officer

Effective Date: 01-Jan-2020

Last Reviewed: 10-Jan-2021

Committed to serving our clients responsibly, vFairs updated controls and processes protect the data of all EU audiences and uphold their rights to stay compliant with the GDPR.

- vFairs enforces GDPR on all standard registration pages as a default measure to confirm lawful consent so that your event attendees take control of the data they choose to share.
- GDPR is enforced based on the country the user selects on the registration page, this means that all users from EU member states fall under the revised data protection legislation.
- Clients have the ability to customize their own country list as well as the GDPR message that appears on the registration page for clear, easy to understand consent request and disclosures across all levels.
- In the circumstance that a user does not agree to the terms of sharing adequate and relevant data, they will not be registered.
- Users have the right to be forgotten; when requested, the user's profile data will be anonymized within the specified webcast or event domain.
- If a user requests to be forgotten, it is the responsibility of the event owner to notify the third party contact of the user's request (This is currently a manual process; third parties do not allow someone else to externally make an automated call to "forget" a user).
- A report can be made available to display all registered GDPR users from a given event.
- When using the mass upload tool, it is the client's responsibility to provide a list of users who have opted into the GDPR policy.
- When utilizing a third party (i.e. salesforce) for registration, it is the responsibility of the third party to confirm that they're only passing users who have accepted the GDPR policy.
- We work with our integration partners as and when required to ensure our GDPR process is aligned with regulation throughout the data transfer.

I. Measures to ensure confidentiality* (Art. 32 (1) b) GDPR)

1. *Providing access control to the site where the personal data of the controller are processed.*

☒ The personal data are stored/processed on servers at the site of the processor

☒ External data centers/cloud services are used

We use AWS to host our infrastructure which is a ISO 27001 certified supplier.

☒ The necessary data protection agreements (e.g. according to Art. 28 GDPR) have been concluded und contain appropriate technical & organizational measures in accordance with Art. 32 GDPR (*mandatory field, if applicable*)

2. *Providing access control to the system where the personal data of the Controller are processed.*

Kindly refer to vFairs Access Control Policy

3. *Providing access control for using the system where the personal data of the Controller are processed*

Kindly refer to vFairs Access Control Policy

4. *Providing "confidentiality" of the using systems*

☒ Threat Detection systems (e.g. virus scanner, firewall)
Following protections are in place:

- Firewall protection
- DDos protection
- IDS/IPS (intrusion prevention system)
- Web Application Firewall
- Malware and Antivirus protection at the server level

☒ Patch management
Patches are applied as soon as vulnerabilities are identified as part of internal security checks and based on reports of third party vulnerability audits conducted twice a year.
☒ Protections of external influences or sabotage (e.g. DDOS, force majeure)

5. *Measures to pseudonymization* (Art. 32 (1) a) GDPR

Personal data of the controller can be processed in a way that they cannot be assigned without enlistment of additional information to an affected person ("pseudonymization"). A pseudonymization assumes that this additional information is kept separately and is defeated by technical and organizational measures which prevent an unauthorized identification of the data subject. The following measures were taken regarding to this:

☒ Encryption of the additional information necessary for the identification
☒ Management and documentation of different access authorizations concerning additional information for identification
☒ Authorization process or permission routines for authorizations to process additional information for identification purposes

II. <u>Measures to ensure integrity*</u> (Art. 32 (1) b) GDPR)

1. *Measures or encrypting/transmission control* (Art. 32 (1) a) GDPR)

The Processor has taken following measures:

☒ Encryption of the data media on which personal data is stored (laptops, USB sticks, systems/servers)

☒ Encryption concept with respect to the storage (access/location) of the keys

☒ Logging of transmission processes

☒ Employees work beyond the company network (home office, travelling)

☒ Employees of the Processor are bound to ensure the compliance with appropriate technical and organizational measures

2. *Input Control*

Measures to ensure that it can be checked and established at a later stage whether and by whom personal data have been entered, modified or removed in data processing systems:

Audit trail is maintained for typical normal use and security related events. Normal use and security related events such as logins are captured.

☒ Functional responsibilities, organizationally defined responsibilities

☒ Documented assignment of access rights

☒ Document Management System (DMS) with change-history tracking

☒ Logging of access, copying, modifying or removing of data

☒ Versioning

☒ Documented concept for logging and evaluation of the processing processes

III. <u>Measures for ensuring availability and resilience*</u> (Art. 32 (1) b) c) GDPR)

☒ Security concept for software and IT applications.

We use OWASP security guidelines for secure software development.

☒ Ensuring data storage in the secured network

☒ Redundant, locally separated data storage (Offsite Storage)

☒ Back-up procedure

vFairs maintains a 7 day rolling backup of the database

☒ Redundancy of hardware, software and infrastructure (e. g. by replication of hard disks, power supply)

☒ Fire and/or extinguishing safety system

☒ Emergency power supply

☒ Air-conditioned server room

☒ Emergency plan for failure or attack (e. g. manual, emergency exercises, recovery scenarios)

☒ Sufficient capacity of IT systems and facilities

☒ Change-Management – Kindy refer to vFairs Change Control Policy

☒ Incident-Management – Kindly refer to vFairs Incident Response Plan

☒ Representation rules for absent employees

IV. <u>Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures*</u> (Art. 32 (1) d) GDPR)

We have a third party perform security assessment on our platform twice a year. In addition, we are currently engaged for SOC 2 audit report due in 4-6 months.

V. Job control/organizational measures (Art. 32 (1) GDPR)

☒ Regular independent auditing of the data protection management system
☒ Designation of the data protection officer acc. to Art. 37 et seq. GDPR
☒ Guidelines/specifications to ensure technical and organizational measures for the safety of processing
☒ Specific measures to ensure the processing bound by instructions of the employees
☒ Documentation of agreements with internal employees, agreements with external service providers and third parties from whom data is collected or transferred to, business allocation plans, responsibility regulations
☒ Confirmed deletion after termination of the agreement
☒ Training / instruction of all authorized employees of the Processor
☒ Commitment of employees to confidentiality
☒ Maintaining records of processing activities in accordance with Art. 30 para. 2 GDPR

VI. Measures for ensuring the purpose limitation of personal data (Unlink ability)*

☒ Restriction of processing, utilization and transfer rights
☒ Omission or closure of interfaces in procedures and procedural components in terms of program technology
☒ Regulatory requirements for the prohibition of backdoors and quality assurance audits for compliance in software development
☒ Separation control
  ☒ Separation by organizational & department boundaries
  ☒ Separation by means of role concepts with scaled access rights based on identity management by the controller and a secure authentication method
  ☒ Separation of test and productive system
☒ Using purpose specific pseudonyms, anonymization services, anonymous credentials, processing of pseudonymous or anonymous data. We can anonymize the data if needed.
☒ Regulated procedures regarding change of purpose

VII. Data Protection by Design and Default (Art. 32 (1), 25 (1), (2) DSGVO)

Measures to ensure that Data Protection by Design & Default is taken into account, including transparency and intervernability (to take into account especially if the processor provides a technical system/solution):

1. *Data Protection by Design and Default (in general*

☒ Implementation of data protection principles (Art. 5 GDPR) & data protection by default (Art. 25 para. 2 GDPR)

- ☒ Regarding the amount of collected personal data,
- ☒ Regarding the scope of their processing,
- ☒ Regarding their retention period (deletion according to criteria and deadlines),

Data is retained while the contract with vFairs is active. We delete the data from the database and all the backups. After the data is deleted, we can also provide a data destruction certificate.

- ☒ Regarding their accessibility,
- ☒ Examination and documentation of the legal basis necessary for the processing
- ☒ Exclusive use and documentation of interfaces necessary for the fulfilment of the purpose
- ☒ Measures to ensure that the data are accurate and up-to-date
- ☒ Measures to anonymize personal data

☒ Examination and documentation of the legal basis necessary for the processing

☒ Data protection impact assessment has already been carried out by the Processor

☒ Proof of data origins (especially for personal data where it have not been obtained from the data subject

2. *Measures to ensure transparency*

☒ Provision of information according to Art. 13/14 GDPR

3. *Measures for ensuring the data subjects' rights (Intervenability)**

☒ Ensuring the feasibility of all affected rights in accordance with Art. 12 et seq. GDPR (especially right of access, right to data portability, right to restriction of processing, right to object)

- ☒ Creation of necessary data fields, e. g. for blocking indicators, notifications, consents, objections, counterstatements
- ☒ Documentation of consents and objections
- ☒ Differentiated options for consent, withdrawal and objection possibilities and channels
- ☒ Documented handling of malfunctions, problem-solving methods and changes to the procedure as well as to the protection measures of IT security and data protection
- ☒ Disabling options for individual functionalities without affecting the whole system
- ☒ Implementation of standardized interfaces for inquiries and dialogues for those data subjects to assert and/or enforce claims
- ☒ Traceability of the activities of the Controller for granting the data subject's rights
- ☒ Setting up a Single Point of Contact (SPoC) for data subjects
- ☒ Operational ability of compilation, consistent correction, blocking and deletion of all personal data stored about a person.

VIII. <u>Approved code of conduct/certification</u> (Art. 32 (3))

☒ Kindly refer to vFairs Code of Conduct.