spark • ignites ambition

Data Protection Policy

Policy owner: Nikolaos Koufos

Version	Date	Description of Version	Author
1	May 2018	Implementation	Nikolaos Koufos Todor Panovski Laura Brinks

Abbreviations

ICT Information and Communications Technology
MIS Management Information System
SIS Student Information System

Purpose

The purpose of this policy is to ensure that the privacy of natural persons whose data SPARK collects and processes is protected.

Scope

This policy is applicable to the collection and processing of data conducted by SPARK staff members, interns, volunteers and external consultants.

Further, this policy is applicable to the collection and processing of personal data. Personal data are defined as any information relating to an identified or identifiable natural person. An identifiable 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, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. This policy is also applicable to the collection and processing of sensitive data. Sensitive data are defined as information revealing the racial or ethnic origin, as well as the health of natural persons.

This policy is applicable to such data that SPARK collects and process from the following actors:

- SPARK staff members, interns and external consultants;

- SPARK local partners' staff members;
- SPARK beneficiaries, who are the participants to the organisation's programmes, including the applicants to its programmes;
- Applicants to the SPARK vacancies;
- Those that express complaints to SPARK;
- Those that receive the SPARK monthly newsletter;
- Various stakeholders, such as funding organisation's staff members, as well as local authorities' and organisation's staff members, who have been in contact with SPARK.

Moreover, this policy is applicable to the data collected and processed through the following SPARK ICT platforms:

- SPARK website: www.spark-online.org
- SPARK HE4S website: http://spark-syria.eu/home/
- SPARK Intranet: https://app.spark-online.org/
- SPARK Scholarship Enrollment System: https://www.he4s.eu/
- SPARK Student Information System: https://www.he4s.eu/
- SPARK Payroll: https://payroll.spark-online.org
- SPARK Vacancy: https://vacancy.spark-online.org
- SPARK Gmail accounts
- SPARK Salesforce platform: https://eu10.salesforce.com/home/home.jsp
- SPARK Pluriform bookkeeping platform
- SPARK cloud storage platform Z drive: https://drive.google.com/drive/folders/0BwFRXXwm_I49WU45dWlUWG1RSEk

Policy

SPARK for pursuing its mission is collecting and processing data from the actors as indicated above. The databases which contain these data, along with the links to them, their data types, their retention period and the lawful bases for maintaining them are stipulated in SPARK's Data Map. Overall, SPARK is collecting and processing these data for:

- Human resources recruitment and administration purposes;
- Financial administration purposes;
- Office administration purposes;
- Management of outsourced activities to its local partners purposes;
- Management, including planning, monitoring, evaluation, reporting and learning, of its programmes/projects purposes;
- Quality assurance of its programmes/projects purposes;
- External communication and outreach purposes;

Data collection and processing at SPARK takes place based on:

- Consensus provided by the data subject to the processing of his or her personal data for one or more specific purposes;

- Necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Necessity for the purposes of legitimate interests pursued by SPARK, namely the implementation of contracts/agreements it has with its donors.
- Necessity for compliance with a legal obligation to which SPARK is subject;

Access to the data that SPARK collects and processes is given to designed SPARK staff member, strictly responsible for handling them as per their roles within the organisation. This access is stipulated in SPARK's Permissions to Apps Policy. Externally to SPARK, access to specific types of programme/project related data is given to the donors that fund them, as well as to the organisation's local partners that implement them. The privacy of these external shared data is stipulated in SPARK's donor contracts and grant agreements, as well as in the partnership contracts and non-disclosure agreements.

Further, SPARK is implementing a Data Back-up Procedure for ensuring that no data are lost.

For databases containing large volumes of personal and sensitive data from vulnerable data subjects, SPARK is conducting data protection impact assessments. These assessments enable SPARK to identify privacy risks embedded in the processing of such databases, as well as measures for mitigating them.

All the data subjects, whose data are collected and processed by SPARK can:

- Receive further information on the data that SPARK collects and processes from them;
- Update their data;
- Receive their data in a machine-readable format;
- Have their data deleted at any time;

by sending an email with their specific request to data@spark-online.org. SPARK we will respond to this request within 4 weeks.

Additionally, all data subjects can express a complaint on the collection and processing of their data by SPARK, by sending an email with their complaint to spark@spark-online.org, indicating in the subject line *Complaint*. We will respond to this within 2 weeks. If the data subject is not satisfied with how his/her complaint has been handled by SPARK, then he/she can escalate the complaint to the Autoriteit Persoonsgegevens, which is the agency responsible for enforcing data privacy in the Netherlands.

In the case of a personal data breach, SPARK shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Autoriteit Persoonsgegevens.