DCAF Geneva Centre for Security Sector Governance

CHARTER GOVERNING DATA PRIVACY

Last updated on 7 October 2019

1. Introduction

1.1. The Geneva Centre for Security Sector Governance ("DCAF") is dedicated to improving the security of states and people within a framework of democratic governance, the rule of law, and respect for human rights.

1.2. DCAF must collect, process, use, and retain certain personal data for a variety of purposes. DCAF processes notably the personal data of its employees, visitors to its website, suppliers, and partners in connection with the provision of its services.

1.3. DCAF pays particular attention to confidentiality and privacy and takes data protection seriously. DCAF has therefore decided to:

- adopt this Policy whose purpose is to set out the key principles governing the collection, processing and storage of personal data within the organization (in Geneva and all Field Offices), in order to comply with applicable data protection law, in particular, the General Data Protection Regulation ("GDPR") and the Federal Act on Data Protection of 19 June 1992;
- allocate roles and responsibilities within the organization in order to ensure proper implementation of and compliance with this Policy and data protection law.

1.4. This Policy sets out the main data protection principles that DCAF employees – whether based in Geneva at DCAF headquarters or in DCAF's Field Offices – are expected to know and observe to ensure that DCAF complies with applicable data protection law.

1.5. This Policy will be accompanied by additional materials (such as Q&As) to address specific issues. The additional documentation will be updated on a regular basis and will provide employees with pragmatic information and guidance to respond to queries they may have regarding the principles set out in this Policy.

2. Data Protection Governance

2.1. DCAF Management shall be primarily responsible for ensuring compliance with and the implementation of the Policy and data protection law.

2.2. DCAF shall set up a Privacy Team with the following specifications:

- The Privacy Team shall include a "Focal Point" from the Resources Department, under the supervision of the Head of Resources.
- The Director shall designate the Head of the Privacy Team. The Focal Point cannot also hold the position of Head of the Privacy Team.
- The Privacy Team shall be responsible for ensuring compliance with and the coordinated implementation of the Policy and data protection law within the organization. In addition, the Privacy Team shall report to DCAF Management on a regular basis on all data protection issues concerning DCAF.

2.3 The Central Focal point shall be responsible for answering and verifying compliance with the Policy and data protection law within DCAF. Additional steps/measures may be implemented gradually to reinforce GDPR governance and implementation. The Head of the Privacy Team will set up a focal point system to ensure the Policy and data protection law is followed across DCAF.

3. Key Definitions

3.1. Personal data means 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 (IP address), or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

3.2. Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic or biometric data uniquely identifying a natural person, health data, or personal data relating to a natural person's sex life or sexual orientation is considered as sensitive data, the processing of which requires particular measures.

3.3. Within the context of GDPR, DCAF is the "controller", which means it is the organization that determines the purpose and means of processing personal data. DCAF is the controller of all personal data used in its non-profit and other activities. DCAF is also the controller in relation to the personal data of DCAF staff (including employees, contractors, temporary workers, and former members of staff), representatives of suppliers, and individuals whose personal data is collected as part of DCAF non-profit activities.

3.4. Data subjects are all living individuals about whom DCAF holds personal data, including staff, candidates, representatives of suppliers, and individuals whose personal data is collected as part of DCAF non-profit activities. All data subjects have legal rights in relation to their personal data.

3.5. The processing of personal data means any operation or set of operations performed upon personal data or sets of personal data, whether or not it is processed by automated means such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4. Types of Personal Data

4.1. As indicated above, DCAF processes a variety of personal data such as data about employees, visitors to its website, and representatives of suppliers and partner/donor organizations. Some of this is sensitive data, such as the location of individuals in conflict zones or the criminal records of employees.

4.2. This Policy applies to personal data in all its forms whether on paper or stored electronically. It applies throughout the lifecycle of the information from its creation through to its storage and utilization, and finally, to its disposal. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the GDPR or DCAF contractual obligations.

4.3. With regard to electronic systems, the Policy applies to the use of DCAF equipment and privately/externally owned systems when connected to DCAF's network, including but not limited to databases and emails.

4.4. Each Department within DCAF maintains one or several registers indicating the categories of data collected and processed within the Department.

5. Fair and Lawful Processing

A. In General

5.1. The GDPR is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2. For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out under the GDPR. These include the data subject's consent to the processing, the fact that the processing is necessary for the performance of a contract

with the data subject, compliance with a legal obligation to which the controller is subject, the legitimate interest of the controller or the party to whom the data is disclosed, or the protection of vital interests and public interest when exercising public authority.

5.3. e Regarding the concept of data subject consent more specifically consent means any freely given, specific, informed, and unambiguous indication of his or her wishes through which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data being processed.

5.4. It should be noted that personal data must be collected only for specified, explicit, and legitimate purposes. It must not be further processed in any manner incompatible with those purposes, and it cannot be used for new, different, or incompatible purposes from those disclosed when it was first obtained, unless the data subject has been informed of the new purposes, and he or she has consented (if necessary).

5.5. DCAF generally processes personal data during its activities on the basis that the processing is necessary for the performance of a contract with the data subject (whether that is a DCAF employee or partner). Regarding the processing of personal data necessary for staff administration and business efficiency purposes, DCAF processes personal data on the basis that is it is in its legitimate interests to do so, provided that such processing is not to the detriment of employees or any other relevant data subjects. In other instances, DCAF relies on the consent of the data subject to process personal data.

B. Marketing and Fundraising

5.6. Marketing – which includes the distribution of newsletters and similar measures, and fundraising activities based on personal data – requires, as a matter of principle, the consent of the data subjects. In any instance, a data subject's prior consent shall be required for unsolicited direct marketing by electronic means.

5.7. A data subject's objection to direct marketing must be honoured promptly. If a subscriber opts out of receiving DCAF newsletter or email notifications at any time, their details must be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

6. Transparency and Information to be Provided

6.1. According to the GDRP, data subjects must be informed about the collection and processing of their personal data.

6.2. In the course of its activities, DCAF may collect and process personal data received directly from a data subject (for example, by an employee providing bank details for remuneration purposes) and data received from other sources (for example, sub-contractors providing DCAF with technical website services).

6.3. If DCAF collects personal data directly from data subjects, it shall ensure that data subjects are aware that their data is being processed, and that they understand:

- The purpose of the processing and the lawful basis for the processing;
- The legitimate interests of DCAF or a third party, where applicable;
- Any recipient of his or her personal data;
- Details of transfers to third countries and safeguards in place;
- Retention periods or criteria used to determine the retention periods;
- The existence of each of the data subjects' rights;
- The right to withdraw consent at any time, where relevant;
- The right to lodge a complaint with a regulator;
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation, and possible consequences of failing to provide the personal data; and
- The existence of automated decision making, if applicable, including profiling and information about how decisions are made, the significance, and the consequences.

6.4. If DCAF collects personal data from a third party about a data subject, it will provide the data subject with the above information as soon as possible and provide any additional information as prescribed by the GDPR.

7. Management of Personal Data

7.1. According to the GDPR, personal data must be properly managed, which means in particular that rules and processes have to be defined with respect to the storage of personal data, the security surrounding personal data, the accuracy of personal data collected and processed by the organization, and the retention periods applicable to personal data.

A. Data Storage

7.2. Personal data should only be stored electronically whenever possible, and the recording of personal data in paper format should be kept to a minimum. In exceptional circumstances where personal data is recorded in paper format, it should be kept in a secure place to prevent unauthorized access to such personal data by unauthorized personnel.

7.3. With respect to the storage of personal data electronically, (i) only systems approved by the DCAF IT Department shall be used, and (ii) personal data shall be stored in the EEA or Switzerland.

B. Data Security and Data Breach

7.4. Together with its IT Department, DCAF will take appropriate security measures against the unlawful or unauthorized processing of personal data, and against the accidental loss of, or damage to, personal data. DCAF will put in place procedures and technologies appropriate to the size, resources, and amount of personal data that DCAF processes. These measures will maintain the security of all personal data from the point of collection to the point of destruction.

7.5. DCAF will regularly evaluate and test the effectiveness of these measures to ensure the security of its processing of personal data.

7.6. DCAF will maintain data security by protecting the confidentiality, integrity, and availability of personal data, defined as follows:

- Confidentiality means that only people who are authorized to use the data can access it (principle of access on a need-to-know basis).
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorized users should be able to access the data if they need it for authorized purposes. Personal data should therefore be stored on DCAF central computer system instead of individual PCs.

7.7. Any data breach, or suspicion of data breach, shall be immediately reported to the DCAF Focal Point.

C. Data Accuracy and Retention

7.8. DCAF will take all reasonable steps to ensure that personal data collected and held is accurate and kept up to date. DCAF will take all reasonable steps to destroy or amend inaccurate, incomplete, or out-of-date data.

7.9. DCAF will not keep personal data longer than is necessary for the purpose or purposes for which they were collected (principle of data minimization), and all personal data will be held in accordance with DCAF data retention policies and procedures.

8. Disclosing Personal Data to Third Parties

A. Processors

8.1. DCAF will only use processors (i.e. third parties processing personal data on behalf of and upon instructions given by DCAF) that agree to comply with the GDPR. DCAF will conduct adequate due diligence on all processors and take all steps required by the GDPR where it appoints a processor, including ensuring the processor:

- Enters a written agreement with DCAF that includes sufficient guarantees as to the security measures that the processor has in place;
- Imposes confidentiality obligations on all personnel who process the relevant data;
- Ensures the security of the personal data that it processes;
- Provides DCAF with all information necessary to demonstrate compliance with the GDPR;
- Either returns or destroys the personal data at the end of the relationship;
- Implements measures to assist DCAF in complying with the rights of data subjects; and
- Continues to comply with its data protection obligations when processing personal data (i.e. by monitoring its compliance).

8.2. In addition, where DCAF uses processors, it will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those processors to ensure that such processors' data protection obligations are of an equivalent standard to DCAF.

8.3. Where appropriate, DCAF will review the activities and processes of the processors it uses to check that they are processing personal data in line with DCAF requirements and the requirements of the GDPR and ensure that the processor confirms they regularly test their security measures to ensure they meet the applicable standards.

B. Governmental Agencies and Courts

8.4. DCAF may have to disclose personal data to governmental agencies and courts when required by law, upon valid court order, or if DCAF considers that disclosure is necessary to (i) investigate, prevent, or take action regarding suspected or actual illegal activities (including in relation the security or integrity of its website or dedicated pages on social media); (ii) investigate and defend itself against any third-party claims or allegations; or (iii) exercise or protect the rights and safety of DCAF personnel or others.

8.5. DCAF may dispute demands made governmental agencies and courts when it believes, in its discretion, that the requests are overbroad, vague, or lack proper authority, but DCAF does not systematically challenge every demand.

8.6. DCAF attempts to notify the persons concerned about legal demands for their personal data when this is judged appropriate and technically feasible, unless prohibited by law or court order, or when the request is an emergency.

9. Processing in Line with Data Subjects' Rights

9.1. Under the GDPR, data subjects have, in essence, the following rights: information about the processing of personal data; the access, update, and deletion of personal data; the rectification of personal data; the restriction of the processing of personal data; the withdrawing of consent regarding the processing of personal data; and data portability.

9.2. DCAF will process all personal data in line with data subjects' rights to and in connection with their personal data in accordance with the GDPR.

10. Transferring Personal Data to a Country Outside the EEA or Switzerland

10.1. DCAF may transfer personal data that it holds to a country other than the country in which the DCAF entity that has collected the personal data is located. These countries may be outside the EEA or Switzerland.

10.2. The transfer of personal data outside the EEA or Switzerland may take place provided that one of the following conditions applies:

- The country to which the personal data is transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
- The data subject has given his/her explicit consent (having been properly informed (for example, of potential risks, etc.)).
- The transfer is necessary for one of the reasons set out in the GDPR, including: the performance of a contract between DCAF and the data subject (or a third party, provided it is in the interests of the data subject); or to protect the vital interests of the data subject.
- The transfer is legally required on important public interest grounds or for the establishment, exercise, or defence of legal claims.
- The transfer is authorized by the relevant data protection authority where DCAF has adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

11. Policy Awareness and Responsibility

A. Policy Awareness

11.1. This Policy will be made available to all staff. Staff and authorized third parties given access to personal data will be advised of the existence of DCAF's relevant policies, codes of conduct, and guidelines that relate to the processing of personal data.

11.2. Training will be given to all staff when they first join DCAF. Additional training will also be provided on a periodic basis as necessary to refresh employees' knowledge – or where there has been a substantial change in applicable data protection law and this Policy – to ensure all staff are aware of their obligations under this Policy.

B. Responsibility

11.3. While DCAF is ultimately responsible for ensuring that DCAF meets its legal obligations under the GDPR, employees are responsible for compliance with this Policy.

11.4. This Policy will be made available to all employees upon implementation, to all new employees upon their recruitment, and to any other parties on a need-to-know basis. Revisions will be communicated to those affected by the changes.

12. Changes to this Policy

12.1. DCAF reserves the right to change this Policy at any time. DCAF will notify employees of those changes by mail or email.