CONCORDIA Data Protection Policy

Directly applicable all CONCORDIA social organisations which have subscribed to our Standard Contractual Clauses
Version 1.1 | 09.10.2023

Preliminary Conditions and Definitions, Related Documents

This document constitutes organisational measures for the group of CONCORDIA social organisations.

The CONCORDIA Data Protection Policy is closely related to the CONCORDIA IT Policy, which defines the technical measures (together: Technical and Organisational Measures; TOMs) that must be applied in all CONCORDIA social organisations for safeguarding personal (and other) data.

Further organisational measures that must be implemented by all participating organisations are defined in the CONCORDIA Code of Conduct (CoC) and the CONCORDIA Child Protection Policy (CPP).

This policy may be translated for easier local implementation, but the English text shall remain the decisive one.

Definitions:

The abbreviation GDPR refers to 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

Standard Contractual Clauses (SCCs) refers to a set of rules as defined by GDPR Article 46 (c).

The term group is used for the group of CONCORDIA social organisations which have subscribed to the CONCORDIA Standard Contractual Clauses. It consists of controllers (which must be EU-based) and processors. Together, they are called member organisations. The controller which has first subscribed to them (according to the sequence number) and is still active is called central controller. Organisations which are not part of the group are called outside organisations.

Member organisations governed by EU law are here called EU organisations, while member organisations in non-EU states are called non-EU organisations. Any country in which a member organisation is seated is called a member country.

The term employee is used for all people working for a member organisation, whether employed or voluntarily, who are processing personal data as part of that work.

The term data protection officer (DPO) is used here both to refer to the data protection officer of an EU organisation (as defined by GDPR Articles 37–39), and to the (main) employee responsible for data protection in a non-EU organisation. Legally, any tasks of a data protec-

tion officer that may not be delegated to non-EU employees are handled by the non-EU organisation's EU representative (GDPR Article 27). The central data protection officer is the DPO of the central organisation.

The term data protection authority (DPA) refers to the supervisory authority of an EU member country (GDPR Article 51), or to the national data protection authority of a non-EU member country. The central data protection authority is the supervisory authority responsible for the central controller. Legally, any tasks of a supervisory authority that may not be handled by a non-EU data protection authority are handled by the central DPA.

The abbreviation TOMs refers to Technical and Organisational Measures, especially to those defined on group level. The term audit refers to the mechanism established for ensuring the verification of compliance with the Standard Contractual Clauses, including its reporting and any correctional measures that are recommended afterwards.

The term directory refers to the records of processing activities (GDPR Article 30). The organisational records are called local directory, while records defined on group level are called central directory.

In addition, the definitions from GDPR Article 4 apply.

1. Data Protection Principles

1.1 Limitation of Purpose

The purpose(s) for which personal data have been collected must be documented in the directory. Should the need arise to use any personal data that was collected through one of these activities (or before the implementation of this policy) for another purpose, the following limitations apply:

a) In the case of a vital interest (Art. 6.1.d), the personal data may be used as far as necessary to resolve the emergency.

b) In the case of a legal obligation (Art. 6.1.c) or public interest / official authority (Art. 6.1.e), only as much as needed to fulfil those obligations.

c) In the case of a legitimate interest (Art. 6.1.f), only after the new purpose has been documented in the directory, including the reasoning why this interest is not overridden by the interests or fundamental rights and freedoms of the data subject.

1.2 Minimisation of Data

Personal data shall only be stored according to the procedures outlined in the directory.

In the case of a transfer to outside organisations, personal data shall only be transferred if it is necessary, and only as much as necessary. E.g. for reports, anonymised or statistical data is usually sufficient. If a transfer of personal data is deemed necessary, a data protection agreement must be in place before any transfer occurs, or they must be included in the standard contractual clauses as a sub-processor.

The CONCORDIA Code of Conduct lists further cases in which personal data must not be stored or transferred, especially with regard to children and programme participants.

1.3 Storage Periods

Entries in the directory must include a deadline for the storage of the personal data, usually relative to an event in a procedure (e.g. “at most three years after the last contact with the person”). Deadlines defined by the SCCs must be mentioned as such in the directory.

For creating an entry in the central directory, the involved organisations first check that their lists of purposes and data types are complete. Then, every organisation sends its intended storage period to the central DPO, who will try to find a common denominator that fits both the intended purposes and the national laws.

An extension to these deadlines is generally possible for backup procedures documented within a directory, as long as a DPO is involved in the restoration process. The backup procedures themselves must also mention the maximum storage periods.

Where national legislation (e.g. in the fiscal domain) demands it, storage periods for certain purposes and data types can be longer then specified in the central directory or in the SCCs. This fact must be mentioned in the local directory.

An annual review (at the change of the fiscal year) must identify data to be deleted or anonymised, according to the directory. Where a storage period requires deletion or anonymisation during a fiscal year, additional reviews must be scheduled for the affected processes as necessary.

1.4 Data Quality

Requests for corrections by data subjects shall be addressed independently of where they are received. If another organisation within the group is responsible for implementing them, the request will be passed on by the data protection staff. A reply that the correction request is handled shall be sent back as soon as possible, including the implementation deadline. The person who will respond to the data subject is established at the same time.

If a correction request comes from another source (from outside the group, but not from data subjects or their legal representatives), it is reviewed internally for plausibility before being processed.

1.5 Data Protection by Design and by Default

When exchanging personal data with data subjects or outside organisations, as little data as necessary (but as much as needed) is shared. In order to establish the validity of a request by a data subject, a confirmation question (usually regarding some other data we have collected from the same data subject before) is asked before any personal data is shared. An official identity document can replace this confirmation process.

Organisational hardware and software should be configured with data protection on by default, except where such options interfere with normal usability or the tasks of the employee. Where data protection options are switched off for these reasons (or where they are not available), the employee has to be informed about that fact.

All online and offline forms shall contain a valid data protection information including a link to the data protection policy (above the submit button / signature). Any checkboxes for communication not directly related to the form's purpose shall be unchecked by default.

1.6 Legal Basis

Personal data shall be processed only as allowed by Article 6 of the GDPR, both within the EU and outside. This restriction must also be passed on to sub-processors handling personal data stored by the group.

1.7 Data Security

The technical part of the Technical and Organisational Measures (TOMs) for the group are defined by the CONCORDIA IT Policy.

The central IT department must monitor the IT Policy regarding the state of the art, and inform the local IT departments regarding necessary security updates or changes. These changes must be implemented as soon as possible and should become part of the next version of the group's IT Policy. The central DPO must confirm the validity of the policy regarding these BCRs as part of the official adoption of a new version.

In cooperation with the local management, measures to restrict physical access to personal data (e.g. to servers or computers, but also to written or printed documents) should be implemented. These measures may include the locking of offices or shelves containing such information, with keys available only to the staff working with them or their backups.

1.8 Data Transfer to Outside Organisations

Transfers of personal data must be done either by inclusion in the SCCs as a sub-processor, or on the basis of a GDPR-conformant data processing agreement which honors the spirit of the SCCs, both within the EU and outside.

No personal data must be stored or transmitted through a cloud or online service without such a valid data protection agreement or SCC sub-processor agreement. In the case of services that may store or transfer personal data outside the EU, the implementation of GDPR-compatible safeguards must be ensured before any personal data is transmitted.

1.9 Accountability

Any data processing according to the SCCs must be documented in writing (including electronically) in the directory.

If any processing is likely to lead to high risk to data subjects' rights and freedoms, a data protection impact assessment must be carried out. If that assessment still indicates a high risk without mitigating measures, the competent DPA must be informed.

1.10 Third Country Legislation

On application to the SCCs, a joining non-EU organisation must document that its country's law, together with the SCCs and this policy, provides a suitable data protection level. This documentation must be written by a lawyer competent both in the country's law and in the domain of data protection.

Whenever local law contradicts either the SCCs or this policy, the central organisation must be informed about the case (unless local legislation or a law enforcement authority prohibits this information). The case should be handled as close to the spirit of the SCCs and this policy as it is possible under local legislation.

If local law or a local authority's request is likely to lead to high risk to data subjects' rights and freedoms, the central DPA must also be informed about it (unless prohibited).

Statistical data about local authorities' requests where communication was prohibited (e.g. number, frequency) should be communicated annually to the central DPA and, if permitted, to the central organisation; of course only in the case that such requests have actually happened in the reporting period.

Generally, where a third country's data protection law defines a different data protection level that does not contradict the SCCs or this policy, the higher level of protection shall be used.

2. Rights of Data Subjects

Requests by data subjects shall be addressed independently of where they are received. If another organisation within the group is responsible for implementing them, the request will be passed on by the data protection staff. A reply that the correction request is handled shall be sent back as soon as possible, including the implementation deadline.

Usually, the person who has received the original request will respond to the data subject in the originally used language. Exceptions may be made when a person is on vacation, not involved in data protection tasks, or doesn't speak that language.

2.1 Automated Processing, Including Profiling

Reports may be generated based on (semi-) automatic algorithms, but any decision based on such reports must be either made or reviewed manually (by a human being).

2.2 Right to Complaints, Redress, and Compensation

Data subjects may address any of the data protection staff (DPOs, persons responsible for data protection, EU representatives for non-EU organisations) within the group in order to

complain. Any negative response must include a detailed reason and mention the right to lodge a complaint before a DPA or a competent court.

Alternatively, or in the case of an inadequate or untimely response regarding a right under the GDPR, a complaint may be filed at a national DPA or at a competent court; either within the data subject's EU country of residence or in any EU country where one of the group members is based. In the case where national data protection law in a non-EU organisation is infringed, data subjects should instead file the complaint at their country's DPA or competent court.

3. Information Duties

A reference to the SCCs and the CONCORDIA Data Protection Policy (a copy, the attached document, or an online link) must be included in the local data protection policy of all member organisations that have signed them. A reference to either the SCCs and the CONCORDIA Data Protection Policy or the local data protection policy must be included in any initial communication with a natural person or outside organisation containing personal data, and on any online or offline forms used for collecting personal data by a member organisation.

4. Monitoring, Tasks of Data Protection Officers

Every EU based member organisation must nominate a DPO, who must be registered at the local DPA. If necessary, the DPO can have deputies (who don't have to be registered).

Similarly, every non-EU organisation must nominate a person who is responsible for data protection there and who shall have the tasks and responsibilities of a DPO according to the GDPR. Additionally, a person from an EU organisation is nominated who will be the organisation's EU representative. Both of these persons are to be registered at the DPA responsible for the EU organisation.

A DPO can be responsible for several member organisations, as long as that person is able to get there quickly if necessary.

The DPO leads the organisation's annual data protection audits (Section 6) and is also responsible for data protection training (Section 7).

5. Complaint Procedures

Complaints regarding data protection within the group or a in member organisation should be addressed to one of the DPOs, who act as national focal points. Ideally, a (non-formal) e-mail describing the complaint is sent, but other means of communications may be used as well.

Technically, a separate mail account / inbox / folder must be used for the e-mail addresses used for complaints or other data protection issues. These e-mail addresses must be published in the local data protection policy. A complaint address may be shared by several organisations.

A manual response that the e-mail has been received and is being addressed shall be sent back to the data subject as soon as possible. That e-mail must also mention a 30 days maximum response time (except where the law dictates a shorter period).

Internally, the request can then be passed on to the DPO in charge of the issue, but the final response must come from the initial contact person. Any negative response must include a detailed reason and mention the right to file a complaint before a DPA or a competent court.

Alternatively (or if this complaint procedure doesn't lead to the desired results), a formal complaint at an EU based DPA or competent court is possible as well, but may result in a longer response time (according to that agency's workload). In the case where national data protection law in a non-EU organisation is infringed, data subjects should instead file the complaint at their country's DPA or competent court.

6. Verification of Compliance

The DPO leads the data protection audits, in which the implementation of the data protection standards (Section 1) and the directory are reviewed and, if necessary, updated. The directory is reviewed based on a four-eyes principle, usually together with the department head responsible for each process. All review dates regarding any processing activity are to be documented in the directory (at least date, second reviewer, and signature). These internal reviews should be done annually. Where the workload would be too great for the organisation, the interval can be expanded to a maximum of two years.

The audit results shall be sent to the central organisation's board (the highest management level) and the central DPO. The central DPO makes sure that they are received and may specify a unified way of reporting the results. The central DPO may also specify a uniform method or further standards for the audits.

6.1 Documentation and Reporting

Every DPO shall document the results of their local audits. The central DPO shall also document the receipt of each organisation's audit results, including the measures recommended by the central DPO.

On request, the results of all data protection audits (including any recommended measures) are to be communicated to the (central or local) DPA. Any resulting advice must be followed.

7. Data Protection Training

Any employee has to receive a data protection training as part of the introduction period (within the first month). This training shall include the relevant sections of the SCCs and this policy, especially when and which data can be processed lawfully, and shall take at least half an hour.

An annual data protection group training shall be mandatory for every employee. The topics can include changes to data protection law or to the SCCs and this policy, current problems in

the data protection domain (e.g. processes that were handled problematically), or other data protection topics. It shall be organised by the local DPO and take at least half an hour. If a person is unable to attend to such a group training session, individual trainings or instructions in writing may replace the group training.

Exposed staff in contact with special categories of personal data can have more intensive training on a national level. This is decided by the local DPO on a case by case basis.

The DPOs need to stay up to date regarding the current data protection law. The central DPO organises periodic meetings in which training and updates concerning all data protection staff are discussed, which should be held on a yearly basis. These meetings can also be held in virtual conference rooms. Training information should be stored on a central server, in order to be accessible to all data protection staff.

8. Sanctions

In addition to the sanctions specified in the GDPR and local law (and applied by a DPA or competent court), the organisation(s) affected in any violations of the SCCs or this policy will conduct an examination in order to find out what went wrong, and who may have been responsible for it. Where more than one organisation is involved, the central organisation needs to be informed as soon as possible, and shall also receive the results of the examination. According to the GDPR Art. 33 and 34, the competent DPAs or the affected data subjects may also need to be informed.

In the case of a violation of the SCCs, this policy, or the GDPR by an employee, a disciplinary hearing will be held. According to the gravity of the violation, it might lead to disciplinary sanctions, including dismissal.