ANNEX 1

JOINT CONTROLLERSHIP ARRANGEMENT REGARDING THE FABO LEARNING PLATFORM

1. APPLICATION

1.1 This Joint Controllership Arrangement, entered into by DanChurchAid (CVR 36980214), Meldahlsgade 3, 1613 Copenhagen, Denmark (referred to as the "DCA" or "Party" unless something else is explicitly stated) and the member of the Fabo Charter (referred to as the "Fabo Member" or "Party" unless something else is explicitly stated), shall govern the relationship between these parties in regard to the Fabo Learning Platform (fabo.org).

2. PURPOSE OF THE ARRANGEMENT

2.1 The Fabo Learning Platform (the "Fabo Platform") has been established as a system to create and facilitate learning processes, and for member organisations (the "Fabo Member") and registered users (data subjects) to contribute to the sharing of methodologies, experiences, learning material, etc.

2.2 If a user (data subject) on the platform registers for or subscribes to a learning site (which can contain discussion forums, interactive learning experiences, etc.), the Fabo Member who owns the content on the learning site will process personal data of this user jointly with DCA.

2.3 This Arrangement lays down the responsibilities between the Fabo Member in question here and DCA as the host for Fabo and owner of The Fabo Learning Platform as required under Article 26 pf the General Data Protection Regulation (the "GDPR"). Concretely, this regards how they jointly process personal data of Learning Site Participants. These processing activities are described in Section 3.1 of this Arrangement.

3. SCOPE OF JOINT CONTROLLERSHIP & APPLICABILITY

3.1 The Parties are joint data controllers as they jointly determine the purposes and means of processing of personal data with regards to the following processing activities on the Fabo Platform:

3.1.1 All learning sites hosted by the Fabo Member on the platform, as these entail the processing of personal data of the Fabo Users registered on the learning site. This personal data includes organisation, department and other data directly related to the user profile.

3.1.2 Depending on what kind of activities have been added to the learning site, the parties will be able to process different kinds of personal learning data. This may include data based on activity completion (i.e. if activated, the parties will be able to see which activities any Participant has completed) and data based on Participants' own entries (i.e. all activities where Participants can interact with the learning site (i.e. survey, quiz, feedback, etc.) or with each other).

3.1.3 On any specific learning site not hosted by the Fabo Member, where the Organisation Learning Manager and any appointed Site Editors have been given access to personal data.

3.1.4 Data on Users' IP addresses and the learning sites they visit.

3.1.5 Cookie data of all users entering the platform are collected, but not accessible to the Fabo Member.

4. THE PARTIES' RESPONSIBILITIES UNDER THE ARRANGEMENT

	DCA is responsible	The Fabo Member is responsible
Legal basis for processing (section 4.1)	X	(X)
Drafting of a cookie consent declaration and obtaining cookie consent (section 4.2)	X	

Fulfilling the requirements for transparency laid down in Article 13-14 of the GDPR (section 4.3)	X	(X)
Notification to DCA upon receiving a requests or complaints from a data subject (section 4.4)		X
Responding to the data subjects' requests or complaints (section 4.4)	X	X
Implementation of appropriate technical and organisational security measures (section 4.6)	X	
Notification to DCA upon becoming aware of a personal data breach (section 4.7)		X
Investigation of the data breach, gather relevant documentation and mitigating the impacts (section 4.7)	X	(X)
Assessment of the personal data breach, notification to the supervisory authority and communication to data subjects (section 4.7)	X	(X)
Article 30 data inventory (section 4.8)	X	X
Erasure of user data not automatically deleted by the user (section 4.9)		X
Implementation of privacy by design and default principles (section 4.10)	X	
Undertaking Data Protection Impact Assessments (section 4.11)	X	(X)
Contracting with and auditing of data processors (if applicable) (section 4.12)	X	
Legal basis for international data transfers (section 4.14)	X	

(X) = supporting role

4.1 **Legal basis for processing:** DCA is responsible for deciding the legal basis for processing of personal data which takes place on the Fabo Platform to the extent this is necessary for providing the Fabo Platform to the registered users. The legal basis decided is:

- Article 6(1)(b) of the GDPR – i.e. processing takes place to the extent this is necessary for DCA or the Fabo Member to perform its obligations to deliver the Fabo Platform to the registered user.
- Article 6(1)(f) of the GDPR – i.e. the processing takes place to the extent DCA or the Fabo Member has a legitimate interest in the processing except where such

interests are overridden by the interests or fundamental rights and freedoms of the registered user.

- Article 6(1)(a) – i.e. consent, which mainly is used in relation to cookies (see section 4.2 below).

For any other use of personal data, each party is responsible for obtaining its own legal basis for the processing under the Articles 6, 9 and 10 of the GDPR, or under local privacy legislation. Each party may thus decide on its own whether further processing of personal data collected is allowed under the rules of the GDPR and whether obtaining consent from the data subjects in such case is necessary.

4.2 **Cookie declaration and consent:** The DCA is responsible for the drafting of a cookie consent declaration under the principles of the Privacy and Electronic Communications Directive 2002/58/EC ('ePrivacy Directive'), and the 'Danish Cookie Order', and to make sure that cookie consent is obtained from the users.

4.3 **Transparency and privacy notice:** DCA are responsible for fulfilling the requirements for transparency laid down in Article 13-14 of the GDPR or any other relevant privacy legislation – i.e. through a privacy notice available on the Fabo Platform. The Fabo Member is responsible for making sure that the content of the privacy notice reflects the collection and processing of personal data.

4.4 **Requests or complaints from data subjects**: If a Fabo Member has received a data subject request or complaint from a user, the Fabo Member is required to immediately notify DCA. The Fabo Member and DCA are jointly responsible for responding to the data subject without undue delay or within any given regulatory deadline with respect to the rules on data subject rights in Chapter III of the GDPR. Furthermore, the Fabo Member and DCA are jointly responsible for determining, if the request or complaint regarding the abovementioned rights or other relevant privacy rights, can be fully or partially met.

4.5 **The data subjects' rights:** This Arrangement does not restrict data subjects in effectively exercising their rights against any of the Fabo Members, including their rights to make a claim against any Fabo Member and file a complaint to a data protection agency.

4.6 **Data security:** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, DCA is responsible for implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk as required under Article 32 of the GDPR. The security measures at the time of entering this arrangement are specified in Annex 1.

4.7 **Data breaches:** If the Fabo Member becomes aware of a personal data breach, the Member is required to notify DCA immediately or at latest 12 hours after the breach has been detected. DCA is responsible for assessing if a personal data breach legally needs to be notified to the lead data protection authority ('The Danish Data Protection Agency'), and further assess if the breach also needs to be communicated to the affected data subjects, as required under Article 33-34 of the GDPR. All Fabo Members are required to cooperate with DCA in mitigating the impacts of a personal data breach, gather relevant documentation regarding the breach and, if necessary, make sure that a breach can be duly notified and communicated. DCA is responsible for internally documenting the data breaches through a list, an inventory or other relevant means.

4.8 **Data inventory:** Each Party is responsible for maintaining their own article 30 inventory. A suggestion for an article 30 inventory can be found in Annex 2.

4.9 **Deletion of personal data:** The user profile of an external user is erased, when the user deletes its user profile on the Fabo Platform. If not by the user, the personal data of external users (i.e. chat conversations, tests and e-learning results) are erased, when there is no longer a legitimate purpose for the processing of their personal data, as per the data retention principles for each Party. The Fabo Member is responsible for erasing personal data of external users, as these can register as participants for any open learning site on the Fabo platform.

4.10 **Data protection by design and by default:** In case of any changes to the Fabo Platform, DCA is responsible for implementing privacy by design and default principles into the changed solution.

4.11 **Data Protection Impact Assessment:** In case of any changes to the Fabo Platform that are likely to result in high risks for the rights and freedoms of the data subjects, DCA is responsible for the carrying out of a data protection impact assessment and, if necessary, consult the Danish Data Protection Agency. The other Fabo Members are required to assist with the data protection impact assessment and the consultation of the Danish Data Protection Agency if necessary. The other Fabo Members are required to make available any documentation needed for DCA to carry out its duties under this section. In case that any of the Fabo Members believe a legal obligation exists to carry out a data protection impact assessment, they shall notify DCA without undue delay.

4.12 **Data processors:** DCA is permitted and responsible to enter into data processing agreements with third party data processors if deemed appropriate. DCA is responsible for making sure that the data processors engaged in relation to the Fabo Platform are complying with its obligations, including conducting audits of third-party data processors

through the means considered necessary by DCA, e.g. through external third-party audits, questionnaires, physical inspections. An overview of third-party data processors is available to the Fabo Members at fabo.org/llab/fabodev. Members will be informed when any new data processors are engaged.

4.13 **Disclosure to third parties:** None of the Parties may disclose personal data to other third-party data controllers without mutual agreement between the Parties, unless required to do so by European Union law, Member State law or other relevant national regulation to which a Fabo Member is subject.

4.14 **International data transfers:** DCA is permitted to transfer personal data to third countries, territories and sectors outside the EU/EEA and to international organisations on behalf of the other Fabo Members if the conditions set forth in Chapter V of the GDPR are met. DCA is responsible for making sure that an international data transfer takes places according to said conditions.

5. FABO MEMBERS OUTSIDE THE EU/EEA

5.1 If the Fabo Member is located outside the European Union (EU) or the European Economic Area (EEA), or if a branch of the Fabo Member is operating outside the EU/EEA, the Standard Contractual Clauses (SCC) decided by the European Commission applies to all processing of personal data transferred to the Fabo Member or said branch. The SCC applicable can be found in Annex 3.

6. TERMS, GOVERNING LAW & DISPUTES

6.1 The Arrangement enters into force when the Fabo Charter has been signed by all Parties and stays in force for the duration of the Fabo Charter.

6.2 Changes to the purposes and means of data processing within the scope of this Arrangement must be communicated to the relevant contacts mentioned in the Fabo Charter for further assessment.

6.3 This Arrangement shall be governed by the laws of Denmark.

6.4 Any dispute or claim arising out of or in connection with this Arrangement or the breach, termination or invalidity hereof, shall be settled before the courts of law in Denmark.

ANNEX 1

Organisational security

The Platform Admin role on the Fabo Learning Platform is only given to two parties. The first party is staff in Fabo Learning Lab and only to staff that need it in order to complete their tasks related to their work on the platform. The second party is the developer from our service provider, with whom we have a Data Processing Agreement in place.
Any other role (e.g. Organisational Learning Manager), is only given to specific people upon request from the Member Organisation.

Technical security

In this section, we describe the relevant security settings employed on the Fabo Learning Platform. We have taken a point of departure in Google's "Web application security questionnaire" as it encompasses the central elements relevant to the security on the platform.

Basic security

HTTPS: The web application is reachable exclusively over HTTPS. Even if the user manually edits the URL to start with http://, it won't work, or it will redirect to https://
Cookies: As there is no sensitive information in our cookie data, they have not been decorated with the "htttpOnly" special key mechanism.

Session ID: The Fabo Learning Platform has a built-in session ID mechanism. The platform offers a "log out" button or link, when clicked, that not only terminates the session (deletes cookies from the client) but also invalidates the entire session ID.

Users and login

Our application requires regular users to log in. Very few features are available without logging in. In addition to an interface for regular users, our application provides an administration interface for users with permissions related to this (see Annex 1 for more on assignable roles). Some organisations are set up with single sign-on (SSO) for their users either through SAML 2.0 or LDAP / Active Directory.

For users without SSO, the Fabo Learning Platform employs username/password authentication. There are minimum password security requirements and passwords are stored using a secure cryptographic one-way hash function of the salted password. The users self-register and set their passwords online directly on the platform. The password can be changed and reset. The latter happens through a password reset link sent via email to the user's registered email address.

At user creation, the account is not prepopulated with any confidential information.

Authorisation

Restrictions on the Fabo Learning Platform related to data that should not be available to other users or should be restricted to certain roles are enforced on the server side. There are processes in place to make sure nothing is accessible for anyone without the right permissions.

Users are not able to gain privileges or perform unauthorised actions by loading pages or features that should only be available to users in a different role. Throughout the platform, we have ensured that users can perform only those actions that are appropriate for their roles.

Cross site request forgery (XSRF): As most actions on the platform are not high-risk, not all actions are protected against XSRF.

Cross-Site Script Inclusion: Our application does not use JSONP but another format that sets variables or calls functions with non-public information.

Clickjacking: As the nature of the platforms and possible actions does not require it, protection from this has not been implemented.

Cross-site scripting

We use a templating system that automatically escapes all user input before redisplaying it. Some of the pages escape user input. Part of the Fabo Learning Platform deals with user-provided HTML that is sanitised and re-displayed to the user. The platform sets a valid and appropriate content type and character set for each page (in the Content-Type HTTP header). We take great care to set this, knowing that otherwise we might be introducing XSS vulnerabilities. However, there might be some vulnerabilities related to DOM-based XSS.

Testing, QA and monitoring

We take great care to test and and ensure quality assurance (QA) on any new developments we make on the platform. Especially, when it comes to authorisation and permissions, we test to ensure that settings are correct before launch. As a standard, and especially related to a launch, we monitor performance and any spikes in crash rates or other large-scale anomalies.

Security contact

Fabo Admin, Christoffer Bengt Meier, cbjo@dca.dk, +45 4033 5552.

ANNEX 2 – ARTICLE 30 INVENTORY

This inventory contains all the activities related to the processing of personal data possible for the Fabo Member and has been added here as a suggestion for the member to use in their own inventory.

The overarching purpose for all data processing relates to learning – both related to user segments and on an individual level. Firstly, the Organisation Learning Manager and any Department Learning Supervisors of the Fabo Member can process personal data on users that are on the platform as a part of the specific organisation (Fabo Member Users), as these are technically all placed in the same cohort on the Fabo Platform. Furthermore, the Organisation Learning Manager, Site Creator and Site Editor of the Fabo Member can process data on users external to the Fabo Member that access a Learning Site hosted by the Fabo Member.

The data that the Fabo Member can process relates to two categories. One relates directly to the user profile, which is at least username, e-mail, country, city, organisation and department. If the Fabo User has added additional information to the user profile, this will also be accessible for processing. The second category relates to all data created by the User partaking in activities on a Learning Site. This includes:

- accessing and/or downloading files
- completed training exercises
- posting in discussion forums
- answering a quiz or survey

All data available for the Fabo Member is accessible through various dashboards directly on the Fabo Platform. This means that all personal data, as a starting point, is kept on the server it is generated on. The Fabo Member can, however, through some of the dashboards download data in a spreadsheet format (e.g. Excel), in which case the Member takes over full responsibility of how the data is processed.

The personal data on any User stored on a Learning Site is only accessible for the Fabo Member to process, if the User is registered on the Learning Site. Whenever a User is unregistered from a Learning Site, all data except for posts in discussion forums are removed as well.

Lastly, the Fabo Learning Platform and all personal data are stored on servers managed by DanChurchAid. The servers are hosted by Hetzner Online and physically placed in Germany (within the EU).

ANNEX 3 – STANDARD CONTRACTUAL CLAUSES

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Data Transfer Agreement

between

the Fabo Member (hereinafter "data exporter")

and

DCA (hereinafter "data importer")

each a "party"; together "the parties".

Definitions

For the purposes of the clauses:

(a) "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);
(b) "the data exporter" shall mean the controller who transfers the personal data;
(c) "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;
(d) "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

(a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

(b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

(c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

(d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

(e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

(a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

(b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

(c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

(d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

(e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

(f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

(g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

(h) It will process the personal data, at its option, in accordance with:

(i) the data protection laws of the country in which the data exporter is established, or

(ii) the relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data, or

(iii) the data processing principles set forth in Annex A.

Data importer to indicate which option it selects: *Option (iii)*
Initials of data importer: *Fabo Member*

(i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

(i) the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

(ii) the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

(iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact

that the countries to which data is exported may have different data protection standards, or

(iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

(a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

(b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

(a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

(b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means).

The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

(c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

(a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

(b) In the event that:

(i) the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

(ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

(iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

(iv) a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

(v) a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

(c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

(d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

ANNEX A: DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.
2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.
3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.
4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.
5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is

not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.
7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.
8. Automated decisions: For purposes hereof "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:
   (a) (i) such decisions are made by the data importer in entering into or performing a contract with the data subject, and (ii) (the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

   or

   (b) where otherwise provided by the law of the data exporter.

ANNEX B: DESCRIPTION OF THE TRANSFER

Data Subjects

The personal data transferred concern the following categories of data subjects:

- *Registered users to the Fabo Platform (as defined in section 1.1 to the Joint Controller Arrangement to which these Standard Contractual Clauses are annexed).*

Purposes of the transfer(s)

The Transfer is made for the following purposes:

- *To give the Fabo Member access to interact with the users of the Fabo Platform (as described in section 2 to the Joint Controller Arrangement to which these Standard Contractual Clauses are annexed).*
- *To give the data importer insights into the use of the Fabo Platform.*

Categories of data

The personal data transferred concern the following categories of data:

- *Is described in section 2 to the Joint Controller Arrangement to which these Standard Contractual Clauses are annexed.*

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients:

- *None (the data importer is not allowed to disclose personal data transferred under these Standard Contractual Clauses outside its own organisation).*

Sensitive data (if appropriate)

The personal data transferred concern the following categories of sensitive data:

- *None.*

Data protection registration information of the data exporter (where applicable)

- *None.*

Additional useful information (storage limits and other relevant information)

- *The data importer must delete all personal data transferred no later than at the termination of the Joint Controller Arrangement to which these Standard Contractual Clauses are annexed.*

Contact points for data protection enquiries

- *Contact information of the data importer and the data exporter may be found on the first page of the Joint Controller Arrangement to which these Standard Contractual Clauses are annexed.*