Annex 3 Template for transparency obligations

Note: The information in this Annex is to be provided by the Data Transmitter to the auditors, audited facility employees and contacts, Certification Body employees and system users ("Data subject") whose personal data is transmitted by the Data Transmitter to the Data Recipient. It is not intended to replace the Data Transmitter's own GDPR transparency information but can be provided in addition or integrated into an existing document. The Data Transmitter remains responsible for informing the Data subjects about its own processing of personal data according to GDPR requirements.

GDPR Transparency Information for IATF 16949 certifications

Processing of Personal Data in the IATF Systems

In order to manage IATF 16949 certifications, it is necessary for the IATF to process personal data of auditors, certification body employees, audited facility employees and contacts, and system user ("Data subject"). This is done by use of multiple databases, platforms, and systems. The IATF is committed to your privacy and the highest standards of data protection. Compliance with data protection laws, in particular the EU General Data Protection Regulation (GDPR), is of utmost importance to the IATF.

The following information serves to inform you about how the IATF processes your personal data in accordance with GDPR requirements.

1. Who is responsible for processing your personal data?

The members of the IATF have set up a common set of databases, platforms, and systems to manage IATF 16949 certifications (IATF Systems), which includes the processing of personal data by some members of the IATF. These members of the IATF are Joint Controllers regarding the personal data about the Data subject which they are processing using these common databases, platforms, and systems. As required by GDPR, they have entered into an agreement determining their respective responsibilities for compliance with their data protection obligations in this regard and for protecting the Data subject's personal data. This agreement between the Joint Controllers specifies in particular that each of the Joint Controllers is responsible to provide the Data subject with the required information about the processing of their personal data via the respective Certification Bodies it oversees, and that each Responsible Oversight Office, each one with respect to the system(s) for which it is responsible, shall act as a contact point and is primarily responsible for processing any requests by the Data subject for exercise of their data subject rights according to GDPR.

The Oversight Offices are responsible for the following IATF Systems:

Responsible Oversight Office	IATF System	Contact Information
IAOB	Auditor Development Process (ADP)	contact_us@iaob.org
IAOB	Audit and Non-Conformance Management Platform (AMP)	contact_us@iaob.org
IAOB	KPI Hub	contact_us@iaob.org
VDA QMC	Common Audit Report Application (CARA)	info@vda-qmc.de
SMMT	IATF Huddle	oversight@smmt.co.uk
IAOB	EthicsPoint	contact_us@iaob.org

The names and contact details of the Joint Controllers and where applicable of their Representatives or Data Protection Officers are:

Controller	Representative (Art. 27 GDPR)	Data Protection Officer
VDA QMC Behrenstr. 35 10117 Berlin, Germany	n/a	Nikolaus Bertermann Daspro GmbH Kurfürstendamm 21 10719 Berlin
IATF France 35 rue des Chantiers 78000 VERSAILLES, France	n/a	n/a
ANFIA Corso G. Ferraris 61 10128 Torino, Italy	n/a	Avv. Marco Mittone Via Assarotti, 9 Torino - Italy
SMMT 71 Great Peter Street London SW1P 2BN, United Kingdom	n/a	n/a
IAOB 4400 Town Center, Suite 200 Southfield, MI 48075 USA	n/a	n/a

To exercise your data subject rights or to address any questions or concerns regarding the processing of your personal data by the Joint Controllers, please contact the Responsible Oversight Office concerned as noted in the table above. Please note that you may also exercise your data subject rights in respect of and against each of the Joint Controllers.

2. For which purposes and on which legal basis is your personal data processed?

The Joint Controllers process your personal data for purposes of management of user access to the IATF Systems, management and monitoring of auditor activities including qualification/(re)qualification process, testing, ethics and performance, management of ongoing audits including auditor performance, as well as creation of reports and overviews regarding certifications, audits, audit results and performance. The legal basis for the processing of your personal data is Article 6 (1) point (f) GDPR. In this regard the Joint Controllers pursue their legitimate interests in effectively managing the global IATF 16949 certifications and audit activities related to those certifications and allowing for necessary traceability of auditor activities.

3. What categories of personal data are processed?

The personal data processed by the Joint Controllers for the above-mentioned purposes are as follows:

Responsible Oversight Office	**Global IATF System**	**Categories of personal data Transferred**
IAOB	ADP	Name, correspondence address, email address, online identifiers, photograph, account status, language, Certification Body employer, password, payment card account holder name, payor billing address, testing and training data, auditor identification number, test answers and results, test scores, education, and professional achievements
IAOB	AMP	Name, correspondence address, email address, online identifiers, phone number, password, Certification Body employer, auditor identification number, audit site contact name, and contact information
IAOB	KPI Hub	Name, correspondence address, email address, online identifiers, password, activation status
IAOB	EthicsPoint	Name of complainant, correspondence address, email address, online identifiers, title, potential unethical activity description, employment of complainant, name and contact information of involved persons
VDA QMC	CARA	Name, correspondence address, email address, online identifiers, auditor identification number, Certification Body employer, status
SMMT	IATF Huddle	Name, correspondence address, email address, online identifiers, password, photograph, phone number, activation status, comments

4. From what sources does your personal data originate?

As far as you do not provide your personal data to the Joint Controllers yourself, the Joint Controllers receive the above-mentioned personal data from the respective Certification Body or Certification Bodies on behalf of which the Data subject is participating in audits related to IATF 16949 certifications.

5. To which recipients is your personal data disclosed?

The above-mentioned personal data may be disclosed by the Joint Controllers to other Joint Controllers, Witness Auditors, as required by the IATF 16949 certification standards, and to service providers, processing the personal data only on behalf of and according to instructions from the Joint Controllers. Each of the Joint Controllers may also be legally required from time to time to disclose personal data to law enforcement or other government agencies. Each Party shall have the right to disclose transferred data, including reports, to affiliates or external advisors, representatives, and agents working for or on behalf of a Party in accordance with applicable data protection legislation and within the scope of the permitted processing purposes.

6. Is your personal data transferred to third countries outside the European Economic Area?

Your personal data is transferred by the Joint Controllers in the European Economic Area to the Joint Controllers in third countries outside the European Economic Area. For transfers to recipients in some third countries (United Kingdom), the European Commission has decided that the country provides an adequate level of data protection. For data transfers to recipients in third countries without such an adequacy decision (United States of America) the Joint Controllers have signed the appropriate Standard Contractual Clauses as provided by the European Commission and, where necessary, implemented additional safeguards to protect your personal data in these cases. To obtain a copy of the Standard Contractual Clauses and, where applicable, additional safeguards, please contact the Responsible Oversight Office concerned.

7. How long is your personal data stored?

The Joint Controllers store your personal data for as long as is necessary for the purposes for which the personal data is processed. Your personal data is deleted by the Joint Controllers when it is no longer required for the purposes pursued by the Joint Controllers (see above under 2.) and when no other legal bases, in particular statutory or contractual retention periods, apply.

8. What are your data protection rights?

You have these rights regarding the processing of your personal data by the Joint Controllers:

a. Right of access: You have the right to obtain from the Joint Controllers confirmation as to whether or not your personal data is being processed, and, where that is the case, access to the personal data and further information about the processing.
b. Right to rectification: You have the right to obtain from the Joint Controllers rectification of inaccurate personal data and to have incomplete personal data completed.
c. Right to erasure (right to be forgotten): Under certain circumstances, you have the right to obtain from the Joint Controllers erasure of your personal data. For example, you may have a right to erasure where the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, or if the personal data has been unlawfully processed.
d. Right to restriction of processing: Under certain circumstances, you have the right to obtain from the Joint Controllers restriction of processing of your personal data, meaning that the Joint Controllers will only store the personal data, process it with your consent or process it for the limited purposes allowed by the GDPR for restricted personal data. For example, you may have a right to restriction of processing if you have contested the accuracy of the personal data.
e. Right to data portability: You have the right to receive from the Joint Controllers the personal data that you have provided to the Joint Controllers for the performance of a contract, where the processing of your personal data is based on your consent or on the performance of a contract and the processing is carried out by automated means, in a common and machine-readable format. You have the right to transmit or have transmitted, where feasible, that personal data to another controller.
f. Right to withdraw your consent: Where the processing of your personal data is based on your consent, you have the right to withdraw such a consent at any time (without this being able to affect the legality of the processing previously undertaken on this basis).

Right to object: Where the Joint Controllers process your personal data to pursue their legitimate interests, you have the right at any time to object to the processing of your personal data on grounds relating to your particular situation. If you rightfully object to the processing of your personal data, the Joint Controllers will no longer process the personal data unless they demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or in the context of legal claims.

To exercise the above-mentioned data subject rights including the right to object or to address any questions or concerns regarding the processing of your personal data by the Joint Controllers, please contact the Responsible Oversight Office concerned. Please note that you may also exercise your data subject rights in respect of and against each of the Joint Controllers.

If you believe that the processing of your personal data by the Joint Controllers infringes the GDPR, you have the right to lodge a complaint with a supervisory authority in the country where you live, work or where you believe the infringement takes place.

9. Are you required to provide your personal data?

There is no statutory requirement for you to provide your personal data to the Joint Controllers. However, in order for you to fulfill your tasks for the IATF 16949 certification framework on behalf of a Certification Body or more generally to participate in audits related to IATF 16949 certifications, it is necessary that your personal data is provided to the Joint Controllers by yourself or by the Certification Body for the above-mentioned purposes.

10. Is your personal data used for automated decision making?

Your personal data is not used by the Joint Controllers for automated decision making.