Code of Conduct/Confidentiality and Data Protection Declaration

for Experts[1]

Code of Conduct
I declare that I avoid direct or indirect discrimination, in particular on the grounds of the ethnic origin, religion and belief, disability, age, sexual identity or gender. In case of immediate family relationships with a staff member of the FIBAA Head Office, I will refrain from acting as a FIBAA Expert for compliance reasons.

Confidentiality Notice
All facts, circumstances, and procedures relating to the operation of a company, which are not public and only known or available to restricted groups of personnel, and the non-distribution of which is a justifiable interest of the legal entity, are said to be business and trade secrets. This includes internal business processes, business, technical, financial or other information relating to FIBAA and its customers as well as all information coming under the above definition published by customers when submitting their self-documentation, during further correspondence or during on-site visits and phone or video conferences. Information, which is already generally known or can be made public without violating the confidentiality notice, is not classified as a business or trade secret.

Data Protection Notice
During your activities as expert you will come into contact with personal information of other experts, Committee members, project managers and other FIBAA staff and their customers. This type of information is subject to special legal protection (data privacy). It is forbidden to collect, process or use protected personal information for a purpose other than the purpose of lawfully completing the respective task. Passing on personal information to third parties is only permissible when the recipient has a right to it due to a legal provision or the affected party has given its prior permission.

Security Guidelines
Only the data required for completing the task at hand may be retrieved. All personal information, computer programmes and business and trade secrets must be stored, processed or distributed, protected from third party access and only duplicated for business purposes in line with the guidelines set by FIBAA. The necessary precautions must be taken whilst carrying out allotted tasks. Existing provisions on dealing with and securing information, computer programmes, business or trade secrets (e.g. password protection) must be observed. Confidential information made available in writing or electronically must be returned and deleted from all data storage devices upon request by FIBAA. Data storage devices or print outs, which are to be deleted or destroyed, containing personal information, computer programmes or business and trade secrets, are to be deleted or destroyed properly (irreversibly).

These obligations persist after the period of appointment as expert has ended.

[1] To facilitate the readability of this document, the male form will be used without further gender-sensitive differentiation. The document addresses anyone irrespective of gender.

These records can, at any time and without further reason, be presented or submitted to institutional customers, the German Accreditation Council, courts or, for good reason, to other institutions.

I hereby commit, as an expert appointed by FIBAA to permanently abide by the code of conduct, to maintain confidentiality and assessment and data privacy both now and beyond my period of appointment.

The applicable Sect. 17-19 of The Act Against Unfair Competition; Sect. 5, 43 and 44 of the Federal Data Protection Act; Sect. 106 of the German Copyright Law; Sect. 5, 202a-202c, 303a and 303b of the German Criminal Code, as well as the FIBAA Code of Conduct are attached to this notice.

The consent to data processing (appendix to CV) as part of the expert application process remains valid.

Name in print

Place, date

Signature

Legal excerpts

The Act Against Unfair Competition
Section 17: Disclosure of trade and industrial secrets
(1) Whoever as the employee of a business communicates, without authorisation, a trade or industrial secret with which he was entrusted, or to which he had access, during the course of the employment relationship to another person for the purposes of competition, for personal gain, for the benefit of a third party, or with the intent of causing damage to the owner of the business shall be liable to imprisonment not exceeding three years or to a fine.
(2) Whoever for the purposes of competition, for personal gain, for the benefit of a third party, or with the intent of causing damage to the owner of the business, acquires or secures, without authorisation,
1. a trade or industrial secret
a) by using technical means;
b) by creating an embodied communication of the secret; or
c) by removing an item in which the secret is embodied;
or
2. without authorisation, uses or communicates to anyone a trade secret which he acquired through one of the communications referred to in subsection (1), or through an act of his own or of a third party pursuant to number 1, or which he has otherwise acquired or secured without authorisation shall incur the same liability.
(3) An attempt shall incur criminal liability.
(4) In particularly serious cases the sentence shall consist in imprisonment not exceeding five years or a fine. A particularly serious case shall usually exist in circumstances where the perpetrator
1. acts on a commercial basis;
2. knows at the time of the communication that the secret is to be used abroad; or
3. himself effects a use pursuant to subsection (2), number 2, abroad.
(5) The offence shall be prosecuted upon application only, unless the criminal prosecution authority considers that it is necessary to take ex officio action on account of the particular public interest in the criminal prosecution.
(6) Section 5, number 7, of the Criminal Code shall apply mutatis mutandis.

Section 18: Use of models
(1) Whoever, acting without authorisation, uses or communicates to another person models or instructions of a technical nature, particularly drawings, prototypes, patterns, segments or formulas, entrusted to him for the purposes of competition or for personal gain shall be liable to imprisonment not exceeding two years or to a fine.
(2) An attempt shall incur criminal liability.
(3) The offence shall be prosecuted upon application only, unless the criminal prosecution authority considers that it is necessary to take ex officio action on account of the particular public interest in the criminal prosecution.
(4) Section 5, number 7, of the Criminal Code shall apply mutatis mutandis.

Section 19: Suborning and offering disclosure
(1) Whoever for the purposes of competition or for personal gain attempts to procure another person to commit a criminal offence pursuant to Section 17 or Section 18 or to incite the commission of such an offence shall be liable to imprisonment not exceeding two years or to a fine.
(2) Whoever for the purposes of competition of for personal gain offers, or accepts the offer of another person, or conspires with another person, to commit, or to incite the commission of, a criminal offence pursuant to Section 17 or Section 18 shall incur the same liability.
(3) Section 31 of the Criminal Code shall apply mutatis mutandis.
(4) The offence shall be prosecuted upon application only, unless the criminal prosecution authority considers that it is necessary to take ex officio action on account of the particular public interest in the criminal prosecution.
(5) Section 5, number 7, of the Criminal Code shall apply mutatis mutandis.

Federal Data Protection Act
Section 5 Confidentiality
Persons employed in data processing shall not collect, process or use personal data without authorisation (confidentiality). Such persons, when employed by private bodies, shall be obligated when taking up their duties to maintain confidentiality. The obligation of confidentiality shall continue after their employment ends.

Section 43 Administrative Offences
(1) (...)
An administrative offence shall be deemed to have been committed by anyone who, whether intentionally or through negligence,
1. collects or processes personal data which are not generally accessible without authorisation,
2. holds personal data which are not generally accessible ready for retrieval by means of an automated procedure without authorisation,
3. retrieves personal data which are not generally accessible or obtains such data for themselves or another from automated processing operations without authorisation,
4. obtains by means of incorrect information the transfer of personal data which are not generally accessible,
(...)
(3) Administrative offences shall be punishable by a fine of up to €300,000 (three hundred thousand euros) (...). The fine shall exceed the economic advantage gained by the perpetrator in carrying out the administrative offence. Should the figure given in item 1 not be sufficient, the fine can be increased.

Section 44 Criminal Offences
(1) Anyone wilfully committing an offence specified in Section 43 (2) of this Act in exchange for payment or with the intention of enriching himself or another person or of harming another person shall be liable to imprisonment for up to two years or to a fine.
(2) Such offences shall be prosecuted only if a complaint is filed. Complaints may be filed by the data subject, the controller, the Federal Commissioner for Data Protection and Freedom of Information and the supervisory authority.

German Copyright Law
Section 106 Unauthorised Exploitation of Copyrighted Works
Any person who, other than in a manner allowed by law and without the right holder's consent, reproduces, distributes or publicly communicates a work or an adaptation or transformation of a work shall be liable to imprisonment for up to three years or a fine.
(2) An attempt shall incur criminal liability.

German Criminal Code
Section 5 Offences committed abroad against domestic legal interests
German criminal law shall apply, regardless of the law applicable in the locality where the act was committed, to the following acts committed abroad:
7. violation of business or trade secrets of a business physically located within the territory of the Federal Republic of Germany, or of an enterprise, which has its seat there, or of an enterprise with its seat abroad and which is dependent on an enterprise with its seat within the territory of the Federal Republic of Germany and which forms a group with the latter;

Section 202a Data Espionage
(1) Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment of not more than three years or a fine.
(2) Within the meaning of subsection (1) above data shall only be those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable.

Section 202b Phishing
Whosoever unlawfully intercepts data (section 202a (2)) not intended for him, for himself or another by technical means from a non-public data processing facility or from the electromagnetic broadcast of a data processing facility, shall be liable to imprisonment of not more than two years or a fine, unless the offence incurs a more severe penalty under other provisions.

Section 202c Acts preparatory to data espionage and phishing
(1) Whosoever prepares the commission of an offence under section 202a or section 202b by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible
1. passwords or other security codes enabling access to data (section 202a (2)), or
2. software for the purpose of the commission of such an offence,
shall be liable to imprisonment of not more than one year or a fine.
(2) (...)

Section 303a Data tampering
(1) Whosoever unlawfully deletes, suppresses, renders unusable or alters data (section 202a (2)) shall be liable to imprisonment of not more than two years or a fine.
(2) The attempt shall be punishable.
(3) Section 202c applies accordingly when preparing a criminal act pursuant to paragraph 1.

Section 303b Computer Sabotage
(1) Whosoever interferes with data processing operations which are of substantial importance to another by
1. committing an offence under section303a (1); or
2. entering or transmitting data (section 202a (2)) with the intention of causing damage to another; or
3. destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier,
shall be liable to imprisonment of not more than three years or a fine.
(2) If the data processing operation is of substantial importance for another's business, enterprise or a public authority, the penalty shall be imprisonment not exceeding five years or a fine.
(3) The attempt shall be punishable.
(4) In especially serious cases under subsection (2) above the penalty shall be imprisonment from six months to ten years. An especially serious case typically occurs if the offender
1. causes major financial loss,
2. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of computer sabotage, or
3. through the offence jeopardises the populations supply with vital goods or services or the national security of the Federal Republic of Germany.
(5) Section 202c shall apply mutatis mutandis to acts preparatory to an offence under subsection (1) above.

Code of Conduct (Extract from the FIBAA Rules of Procedure)

Section 1 - Code of Conduct
(1) Committee members and experts carry out their work thoroughly and conscientiously.
(2) As experts in the area of quality assurance in higher education institutions they act and adjudicate exclusively in line with quality criteria and are not bound by instructions from third parties. They act and adjudicate in good faith and to the best of their knowledge and belief in the interests of FIBAA.
(3) They do not use their membership to pursue their own interests or those of third parties and will not misuse information gained through their appointment.
(4) They must not disclose, both during and after their period of appointment, confidential information and secrets, namely business and trade secrets, which come to their attention during their period of appointment. They must not disclose secrets of deliberations both during and after their period of appointment.
(5) Student Committee members and experts must immediately inform the administrative office upon completing or leaving their studies/doctorate and terminate their appointment.

Section 2 - Bias Committee for Committee members and experts
(1) Committee members and experts must possess the impartiality required for objective assessment of the subject areas.
(2) If an issue is being advised on which affects the interests of the individual, his spouse, his parents, children, siblings or a person represented by him by law or power of attorney, he may not participate in the consultancy and voting process. However, he can be heard as part of the decision making process.
(3) Bias towards an institution is irrefutable
a) when a person, at the time of assessment or up to five years prior, receives or has received a complaint due by decision of the institution which, in particular, comprises refused, rejected, denied, withdrawn or similar administrative files and criminal charges filed by the institution or a representative of the institution;
b) when an individual, at the time of assessment or up to five years prior, is involved or was involved in an employment relationship, or a doctorate, habilitation or appeals procedure at the respective institution;
c) when an individual, at the time of assessment or up to three years prior, was or is enrolled as a student at the respective institution, involved in joint research projects or other intensive cooperation projects, or;
d) when an individual or subject area to which the individual belongs, at the time of assessment or up to three years prior, is being or has been reviewed by employees of the institution.
(4) If an individual meets one of the bias criterion, or if he is suspected of being biased, this must be immediately made known and recorded without request. The biased party is to be excluded from consulting and voting.
(5) Committee members who have worked as experts do not take part in the vote on the respective accrediting process.