Information about Processing of Data

BACKGROUND AND PURPOSE

The “Customer” of FLOCERT wishes to receive a verification and certification against the EDGE Standards and, for this purpose, has entered into a certification agreement with FLOCERT in its capacity as an accredited EDGE Certification Body (“an Agreement”).

FLOCERT has been accredited by the EDGE Certified Foundation (https://edge-cert.org/) to be able to undertake and provide certification services in accordance with the EDGE Certification Requirements. EDGE is a global assessment methodology and business certification standard for gender equality. It measures where organizations stand in terms of gender balance across their pipeline, pay equity, effectiveness of policies and practices to ensure equitable career flows, as well as inclusiveness of their culture.

The certification services include the audit, verification, and certification that a company conforms with the EDGE Standard to one of the three EDGE Certification Levels.

METHODOLOGY

To perform the EDGE audit and certification, FLOCERT will conduct a remote Audit to verify that the data and information entered by the Customer in the EDGE Empower® Software is correct, has been derived from original organizational databases, is relevant to the chosen Reference Period and relates to all eligible employees (the “Employees”) included in the Audit scope.

During the online Audit interaction, the auditor will view a sample of employees’ personal information and cross-check the reported data against the Customer’s HR system or original data sources to confirm it is correct. The auditor will only view the employees’ data on the screen. The auditor will not be in possession, store or have direct access to any of the original data sources. Also, the auditor will not make screenshots, nor record or capture in any way the online interaction, so FLOCERT will not be able to use any personal data after the Audit or pass them on.

FLOCERT and its auditors are under strict obligation to respect the confidentiality of data e.g., Employee’s data. They have the awareness, the experience, and the technical and organisational measures in place to safeguard this and have confirmed so by entering into a respective non-disclosure agreement with FLOCERT.

Data shall therefore be made accessible by the Customer in an either aggregated or anonymized form, unless required otherwise to comply with the provisions of an Agreement.

ROLES AND RESPONSIBILITIES

When conducting an Audit, FLOCERT shall ensure it complies with applicable data protection laws, i.e. the General Data Protection Regulation "GDPR" (EU) 2016/679 ("Data Protection Laws") when processing personal data, as defined in applicable Data Protection Laws.

FLOCERT shall perform its activities pursuant to an Agreement, acting as processor on behalf of Customer. Customer shall remain the controller for all personal data,

FLOCERT agrees that when providing the services under an Agreement and in relation thereto acting as processor, it shall:

- only process personal data on the documented instructions of Customer (which shall include the performance of its obligations under an Agreement), unless required to process that personal data for other purposes by Data Protection Laws. Where such a requirement is placed on FLOCERT, it shall provide prior notice to Customer unless the relevant law prohibits the giving of notice on important grounds of public interest;
- inform Customer if, in its opinion, Customer's instructions would be in breach of Data Protection Laws;
- provide reasonable assistance to Customer to allow it to conduct privacy impact assessments and to respond to requests from individuals exercising their rights under Data Protection Laws;
- notify Customer immediately after becoming aware of any actual or reasonably suspected
  (i) accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed; or
  (ii) a breach of the technical and organisational measures (a "Security Breach"), regardless whether this Security Breach takes place in relation to personal data processed by FLOCERT or a sub-processor. The notification shall be in writing and shall be sent to Customer. FLOCERT shall maintain procedures aimed at continuously detecting, responding to and recovering from Security Breaches, including taking all adequate remedial measures;
- implement appropriate administrative, organisational, physical, and technical safeguards to protect the confidentiality, integrity, and availability of the personal data consistent with applicable Data Protection Laws, including, without limitation, to protect the personal data against destruction, loss, unauthorised disclosure or access, or any other form of unlawful processing. To clarify, FLOCERT shall consider the state of the art and implementation costs when considering the appropriateness of such administrative, organisational, physical, and technical safeguards, and ensure that such measures offer an appropriate level of security given the risks associated with processing and the nature of the personal data to be protected;
- not engage a sub-processor listed in an Agreement without Customer's prior written consent. Customer may attach reasonable conditions to its consent;
- not transfer personal data to other countries without Customer's prior written consent;
- promptly notify Customer if FLOCERT receives a request from a data subject attempting to exercise their rights under Data Protection Laws. The notification shall be in writing and shall be sent to Customer. FLOCERT shall assist Customer to respond to and fulfil such request and act in accordance with Customer's reasonable instructions when dealing with that request;
- ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

- following the end of the provision of the Audit and on Customer's request, return to Customer and/or permanently delete all personal data (including copies) in FLOCERT's possession or control.

PERSONAL DATA AND PROCESSING ACTIVITIES

The types of personal data, categories of data subjects and the purposes of the processing by FLOCERT are:

- Subject matter: The processing of personal data as further described in an Agreement.
- Duration: The personal data will be processed during the term of an Agreement.
- Nature and purpose: FLOCERT will provide Customer with audit services related to the Customer's EDGE certifications, as further described in an Agreement. The personal data will be processed for the purpose of performing the services under such Agreement. For clarification, the auditor does not have access to those data. The auditor will only be viewing the data.
- Types of personal data: contact details, name, title, position, compensation, career information, professional and leadership trainings, compensation. FLOCERT does not intend to process special categories of personal data pursuant to Art. 9 GDPR.

Categories of data subjects: Employees (incl. consultants and contractors), appointments, contact persons and shareholders of the Structure.

RIGHTS OF THE DATA SUBJECT

The data subject has the following rights:

- to request information about your personal data processed by us in accordance with Art. 15 of the GDPR. In particular, you may request information on the purposes of processing, the category of personal data, the categories of recipients to whom your data have been or will be disclosed, the planned storage period, the existence of a right of rectification, cancellation, restriction of processing or opposition, the existence of a right of appeal, the origin of your data if such have not been collected by us, and the existence of automated decision-making, including profiling and, if applicable, useful details regarding such data;
- to demand the correction of incorrect or incomplete personal data stored by us without undue delay in accordance with Art. 16 of the GDPR;
- to demand deletion of your personal data stored with us, unless the processing of such is necessary to exercise the right to freedom of expression and information, to fulfil a legal obligation, for reasons of public interest or to assert, exercise or defend legal claims in accordance with Art. 17 of the GDPR;
- to demand restriction of the processing of your personal data in accordance with Art. 18 of the GDPR if you dispute the accuracy of the data, if the processing is unlawful but you reject its being deleted and we no longer require the data, but you require it for the assertion, exercise or defence of legal claims or if you have lodged an objection to the processing pursuant to Art. 21 of the GDPR;
- to receive your personal data that you have provided us with in a structured, common and machine-readable format or to request that it be transferred to another responsible party in accordance with Art. 20 of the GDPR;

- to revoke consent you have previously granted us at any time in accordance with Art. 7 (3) of the GDPR. If you do so, we may no longer continue to process the data which have been based on this consent in the future and
- complain to a supervisory authority in accordance with Art. 77 of the GDPR.

RIGHT TO OBJECT

If your personal data are processed on the basis of legitimate interests in accordance with Art. 6 (1) (1) (f) of the GDPR, you have the right to object to the processing of your personal data in accordance with Art. 21 of the GDPR if there are reasons for doing so emanating from your particular situation or if the objection is directed against direct marketing. In the latter case, you have a general right of objection, which we shall abide by without your having to state any particular reason. If you wish to exercise your right of revocation or objection, simply send an e-mail to flocert@flocert.net.

INFORMATION ABOUT FLOCERT

Name and address:

FLOCERT GmbH, Bonner Talweg 177, 53129 Bonn, Germany

Legal Representative: Dr. Thorsten Niklas, Managing Director

Commercial Register: Bonn – HRB 12937

Contact Details: T: +49 (0)228-2493-0 F: +49 (0)228-2493-120 E: flocert@flocert.net

Data Protection Officer: dhpg IT-Services GmbH, Bunsenstr. 10a, 51647 Gummersbach, Germany

Contact Details: T: +49 (0)2261-8195-0 E: datenschutz@dhpg.de