

WHISTLEBLOWING

Reporting system for reporting breaches

Dear colleagues, former employees, job applicants, service providers, clients, and business partners ,

Greencells GmbH provides access to the reporting system "Proliance Whistle", through which breaches can be reported. At Greencells GmbH, the aim is to create a trusting and constructive whistleblowing culture that enables every reporting person to report breaches via secure communication channels. Below you will find all essential information on the reporting of breaches at Greencells GmbH.

If you have any questions, please contact our Compliance Officer for general questions on the reporting of breaches:

Ms Nicole Tsang, phone: +49 152 03145641, email: n.tsang@greencells.com

1. What is whistleblowing?

"Whistleblowing" is the reporting of a (possible) breach of certain legal provisions by a person who has become aware of the breach in a work-related context (= whistleblower or reporting person).

The EU Directive 2019/1937 on the protection of persons who report breaches of Union law ("EU Whistleblowing Directive") and the German Whistleblower Protection Act ("Hinweisgeberschutzgesetz") protect reporting persons from retaliations as a result of reporting a breach. It has always been an important concern of Greencells GmbH to promote open communication within the company and to prevent possible compliance breaches. The new legal requirements were therefore taken as an opportunity to set up an internal **reporting channel**, whereby reports can be submitted particularly easily and securely via the reporting system "Proliance Whistle" of the compliance service provider Proliance GmbH.

2. What must be considered when reporting?

As an employee of Greencells GmbH, you can report criminal offences and certain offences subject to fines as well as offences against sector-specific national and EU regulations. This includes the following topics or violations:

- Crimes
- Fined offences (limited)
- Money laundering and terrorist financing
- Product safety and compliance
- Road traffic safety (limited)
- Railway operational safety
- Maritime traffic safety (limited)
- Civil aviation security (restricted)
- Transport of dangerous goods (restricted)
- Environmental protection
- Radiation protection and nuclear safety
- Promotion of renewable energies etc.
- Food and feed safety, animal welfare, etc.
- Medicines, medical devices, patient care, etc.
- Tobacco products
- Consumer rights and consumer protection (limited)
- Protection of communications, harassing advertisements, etc.
- Protection of personal data
- Security in Information Technology (restricted)
- Shareholders' rights
- Audit of financial statements of companies in public interest
- Procurement of public contracts and concessions

- Accounting, including corporate accounting (limited)
- Infringement pursuant to § 4d I 1 Finanzdienstleistungsaufsichtsgesetz (restricted)
- Legal tax norms relating to corporations and commercial partnerships
- Abusive tax advantage for corporations and partnerships
- Impairment of competition or abuse of dominant position (in Germany or in the EU internal market) etc.
- EU internal market including competition and state aid
- Constitutional fidelity of civil servants
- Financial interests of the EU (limited)

In addition, you can submit a reporting in case of breaches of the following topics:

- Violations of internal compliance requirements
- Violations of company policies
- Violations of code of conduct

The legal protection of reporting persons against retaliations when using the internal reporting channel only applies if, at the time of the report, **there** was sufficient reason to believe that **the reported information on breaches was true and that this information falls within the scope of the EU Whistleblowing Directive or the German Whistleblower Protection Act.**

A violation can be reported by active employees (employees, persons employed for vocational training and persons similar to employees (e.g. temporary workers)), former employees, applicants, business partners, service providers and customers. Reports by other persons, such as interested parties and other persons, are not possible.

3. How can a breach be reported?

Breaches can be reported via the reporting system "Proliance Whistle". To access the reporting system, please use the following link:

<https://whistleblowersoftware.com/secure/greencells>

You can also scan this QR code to access the reporting system:



When preparing your reporting, please ensure that it designates Greencells GmbH as the **company concerned** and that it is **complete and comprehensible**. Your reporting will be received and processed **confidentially** by our service provider Proliance GmbH. **An anonymous** reporting is possible. You will receive further information before submitting a reporting via the reporting system "Proliance Whistle".

Breaches can also be reported to **external reporting channels**. The competent authority for this is in principle the German Federal Office of Justice (Bundesamt für Justiz). In certain cases, the German Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht) and the German Federal Cartel Office (Bundeskartellamt) are also competent external reporting authorities. With regard to the reporting procedure, we refer to the reporting channels of the respective bodies. In order to ensure immediate and effective processing of your report, we always recommend reporting a breach internally as a matter of priority.

For information on the processing of your personal data in the context of the reporting of a breach and the handling of your report, as well as the data subject rights to which you are entitled, please refer to the privacy information attached.

Annex: Privacy information for the whistleblower system of Greencells GmbH

Dear user of our whistleblower system,

In accordance with the requirements of Articles 13, 14 and 21 of the General Data Protection Regulation (GDPR), we hereby inform you about the processing of your personal data and your rights under data protection law in this regard. To ensure that you are fully informed about the processing of your personal data in the context of the use of our whistleblower system, please take note of the following information.

1. Data Controller in accordance with the data protection law

Greencells GmbH

Bahnhofstr. 28

66111 Saarbrücken

Phone: +49 (0) 681 992 669 10

E-Mail-Adresse: n.tsang@greencells.com

URL: <https://greencells.com/compliance/>

2. Contact data of our Data Protection Officer

PROLIANCE GmbH / datenschutzexperte.de

Data Protection Officer

Leopoldstr. 21

80802 Munich

Germany

E-mail: datenschutzbeauftragter@datenschutzexperte.de

3. Purposes and legal basis of processing

We process your personal data in accordance with the provisions of the European General Data Protection Regulation (GDPR) and the German Federal Data Protection Act (BDSG). The processing is carried out in order to fulfill our legal obligation within the meaning of Art. 6 (1) lit. c GDPR to receive and process reports in accordance with Directive (EU) 2019/1937 (Whistleblower Directive) as well as the German Whistleblower Protection Act (Hinweisgeberschutzgesetz). We process your data to the extent necessary and permissible to fulfill these legal obligations.

In addition, processing may be carried out to protect the legitimate interests of us or third parties and to defend and assert legal claims in accordance with Art. 6 (1) lit. f GDPR. If necessary, we will inform you separately, stating the legitimate interest, insofar as this is required by law.

4. Categories of personal data

We only process data that is related to the processing of your report. Unless you submit an anonymous report, this may be general data about you (name, contact details, etc.) and, if applicable, other data that you provide to us as part of the report, such as your relationship to us and to the person(s) reported. In addition, we process the further contents of your report (in particular descriptions of the facts and specific allegations of compliance violations) together with any attachments. If you send us your report by voice recording, we also process this.

5. Recipient of the data

Reports submitted via our whistleblower system are received and processed confidentially by our service provider PROLIANCE GmbH, Leopoldstr. 21, 80802 Munich, Germany. PROLIANCE GmbH acts as our data processor and carries out the data processing strictly in accordance with our instructions. If you do not make an anonymous report, we will only be informed of your identity by our service provider if you agree to this in order to ensure the best possible protection of confidentiality or if this is necessary to fulfill a legal obligation or to pursue our legitimate interests, such as the assertion or enforcement of legal claims or defense against a legal claim. Otherwise, we will only receive a summary of your report, which will not include any direct reference to your identity.

If we become aware of your identity or are provided with other personal data in connection with your report, we will maintain the required confidentiality by disclosing this data only to those departments and persons who need this data to fulfill legal obligations or to pursue legitimate interests.

Data will otherwise only be transferred to recipients outside our company if this is permitted or required by law, if the transfer is necessary to process your report, if you have given your consent or if we are authorized or obliged to provide the data. Under these conditions, recipients of personal data may be, for example:

- Tax consultants or lawyers
- Public authorities and institutions (e.g. public prosecutor's office, police, supervisory authorities, tax office) in the event of a legal or official obligation,
- Recipients to whom disclosure is directly necessary for processing your report,
- Other data recipients, for whom you may give us your consent to transfer data.

6. Transfer to a third country

A transfer to a third country is not intended.

7. Duration of the data storage

We process and store your personal data to the extent necessary for the processing of your report and any subsequent investigations and follow-up measures. The documentation of your report will generally be deleted three years after the conclusion of the proceedings. If the processing of your personal data is necessary for civil or criminal proceedings in connection with your report, we will store the data until the conclusion or until the decision has become final. The storage period is also based on the statutory limitation periods, which, for example, according to §§ 195 et seq. of the German Civil Code (BGB), are generally three years, but in certain cases can be up to thirty years.

8. Your Rights

Every data subject has the right of access pursuant to Art. 15 GDPR, the right to rectification pursuant to Art. 16 GDPR, the right to erasure pursuant to Art. 17 GDPR, the right to restriction of processing pursuant to Art. 18 GDPR, the right to notification pursuant to Art. 19 GDPR and the right to data portability pursuant to Art. 20 GDPR.

In addition, you have the right to lodge a complaint with a data protection supervisory authority pursuant to Art. 77 GDPR if you are of the opinion that the processing of your personal data is not lawful. The right to lodge a complaint with a supervisory authority shall be without prejudice to any other administrative or judicial remedy.

If the processing of data takes place on the basis of your consent, you are entitled to withdraw your consent to the use of your personal data at any time in accordance with Art. 7 GDPR. Please note that the withdrawal will only take effect in the future. Processing that took place before the revocation is not affected by this. Please also note that we may need to retain certain data for a period of time to comply with legal requirements (see Section 7 of this Privacy Policy).

Right to object

If your personal data is processed in accordance with Art. 6 para. 1 lit. f GDPR in order to safeguard legitimate interests, you have the right, pursuant to Art. 21 GDPR, to object to the processing of this data at any time for reasons arising from your particular situation. We will then no longer process this personal data unless we can prove compelling reasons for the processing. These must outweigh your interests, rights and freedoms, or the processing must serve the assertion, exercise or defense of legal claims.

To exercise your rights, please contact us using the contact details given in section 1.

9. Necessity of providing personal data

The provision of personal data for the submission of a report is voluntary. However, we can only process your report if you provide all personal data required for the processing of your report and any subsequent investigations.

10. Automated decision-making

In the course of processing your report, we do not use fully automated decision-making pursuant to Art. 22 GDPR. Should we use these procedures in individual cases, we will inform you about this separately or obtain your consent, if this is required by law.