Data protection declaration per Art. 13 General Data Protection Regulation (GDPR) for the Digital Reporting Channel

1. Name and address of responsible party

The responsible party pursuant to the General Data Protection Regulation and other national data protection legislation by Member States and other data protection regulations is:

Stern-Wywiol Gruppe GmbH & Co. KG
An der Alster 81
20099 Hamburg, Germany
E-Mail: info@stern-wywiol-gruppe.de
Telephone: 040 – 284 039-0
Fax: 040 – 284 039-76

Our attorney for data protection matters, Sven Naucke, can be reached at the above address or at data@stern-wywiol-gruppe.de

II. Data processing in connection with provision of the Digital Reporting Channel

1. Extent of data processing

Every time our Digital Reporting Channel is used, our system automatically records the following data and information from the computer system accessing it:

a. Partially anonymized IP address
b. Device
c. Operating system
d. Internet browser
e. Referring and exit pages
f. Date/time stamp

The data is also stored in our system's logfiles on servers in the EU, in order to ensure the functionality of the Digital Reporting Channel and the security of our IT systems. This data is not used or stored in conjunction with other personal data of the whistleblower (reporting party) (hereinafter also "user") in this context.

The data is deleted when it is no longer needed for the purpose of its collection. This is the case no later than after 14 days for data stored in logfiles.

“Partially anonymized” means that the IP address is captured when the site is accessed, but only at the proxy server level to ensure system security. There is no matching to individual users of the Digital Reporting Channel. The IP addresses are used only for the abovementioned duration in the LegalTegrity system, and not forwarded to the responsible party.

Matching these IP addresses to specific users is not readily possible for LegalTegrity either, and is only done when the Digital Reporting Channel has been misused, such as for a cyber attack, and it is necessary to determine which IP address such misuse came from.

2. Legal basis and purpose of data processing

The legal basis for the capture and temporary storage of data in logfiles is Art. 6 Para. 1 lit. f) GDPR. Access to the above information by the system is necessary in order to enable provision of the Digital Reporting Channel to the user’s computer. This is also the purpose for our justified interest in processing the data per Art. 6 Para. 1 lit. f) GDPR.

3. Objection and removal

Collection of data for the purpose of providing the Digital Reporting Channel and storage of the data in logfiles is necessary for its operation. Consequently, there is no option of objecting to it by the user.

4. The use of cookies

Our Digital Reporting Channel uses only the cookies technically necessary to make it usable, since it cannot function without them. This is also the purpose for our justified interest in processing personal data per Art. 6 Para. 1 lit. f) GDPR.

User data gathered by technically necessary cookies is not used to create user profiles.

III. Whistleblower account

1. Scope and purpose of data processing

Within the Digital Reporting Channel, whistleblowers have the option of voluntarily creating a whistleblower account where they can place and manage reports. This is not required for submitting a report.

If no account is created, when a non-anonymized report is submitted only the personal data described under II.1. will be captured, under the conditions there described.

In the course of creating such an account, the user must assign him- or herself a password and pseudonym. Optionally and voluntarily, users can give their names and e-mail addresses, if they wish to be kept informed of developments relating to their report.

2. Legal basis, duration of storage of personal data, removal option

The legal basis for processing of the personal data captured in account creation is the consent of the user per Art. 6 Para. 1 lit. a) GDPR. This consent may be revoked at any time without giving reasons, and without detriment to the user. If this is done no further personal data will be processed. The legal basis for processing until such revocation is not affected by it.

The personal data of the user captured in the process of creating a whistleblower account is stored until the user decides to delete the account, which also constitutes a revocation of consent. In this case the data relating to the account will be immediately deleted. This does not affect the storage of data already sent to us as part of reports.

IV. Data processing in connection with the report

1. Scope and purpose of processing of personal data

When non-anonymized reports are made to the Digital Reporting Channel, we process all data explicitly and wilfully provided to us in such reporting. In particular, this can involve the following:

a. Information on the personal identity of the whistleblower, such as given and family names, address, contact information, gender
b. Employment or other relationship of the whistleblower with our company
c. Information on the affected persons pursuant to the Whistleblower Protection Act (HinSchG), i.e. natural persons who in reports are designated as having committed the breaches in question, or are associated with such designated persons (i.e. name, address, contact information, gender, other information permitting identification)
d. Information on breaches that may allow identification of a natural person

We process such data for the purpose of investigating reports in order to prevent and/or uncover breaches of the law or company policies and/or take consequential measures (such as examining the truth of the assertions made in the report and if appropriate taking action against the reported breach, such as through internal investigation, punitive measures, withdrawal or revocation of funds, or conclusion of the process).

2. Legal basis

Processing of personal data rests on the following legal basis:

a. We process information on the identity of the whistleblower only if that person gives us their consent per Art. 6 Para. 1 lit. a) GDPR by providing the information wilfully.

b. We process information on employment relationship, affected persons and other information that allows identification of natural persons, based on Art. 6 Para. 1 lit. f) GDPR. Our required legitimate interest, depending on the specific case, consists of the processing of reports in order to take consequential measures, such as examining the truth of the assertions made in the report and if appropriate taking action against the reported breach, such as through internal investigation, punitive measures, withdrawal or revocation of funds, or conclusion of the process. Whether interests or basic rights and freedoms of affected persons conflict with such data processing is examined case by case, including in consideration of the respective breach.

c. We may process personal data of employees based on § 26 Para. 1 Clause 2 BDSG (Federal Data Protection Act) (need for data processing to uncover illegal acts).

3. Data deletion and retention period

As a rule data is stored until consequential measures resulting from a report are concluded. Depending on the subject of the report, other specific laws may be applicable that require longer data retention. This can also be the case if it is necessary to take further legal action (such as criminal or disciplinary action).

V. Recipients of personal data

1. Data connected with the Digital Reporting Channel

We work with LegalTegrity GmbH (“LegalTegrity”), Platz der Einheit 2, 60323 Frankfurt am Main, Germany, to provide the Digital Reporting Channel. That company developed the Digital Reporting Channel and hosts it for us. Therefore, LegalTegrity can be aware of the personal data described in this Data protection declaration.

LegalTegrity acts as an order processor for us. An order processing contract as required per Art. 28 Para. 3 GDPR has been concluded. In it, LegalTegrity is required to maintain confidentiality and to process only according to our instructions such personal data as falls under our data-protection responsibility in use of the Digital Reporting Channel.

2. Data from reports

Transfer of personal data to third parties takes place only if there is a legal basis for it. In particular, this is the case when transfer serves the fulfilment of legal responsibilities requiring us to report or transfer data, the user has given us their consent, or a balancing of interests justifies it.

For example, such a balancing of interests is necessary if persons named in a report demand information per Art. 15 GDPR on the personal data stored by us, including information on the source

from which we received the data. In this case, the interest of the affected person in this information and that of the whistleblower in remaining anonymous must be weighed against each other. The interest of the affected person will as a rule prevail when the whistleblower has falsely reported a breach wilfully or grossly negligently.

Depending on the main area of responsibility of the report and for the effective initiation of consequential measures, personal data may be transferred to our appropriate departments. In some cases we may transfer personal data to governmental authorities for prevention and/or criminal proceedings, or other responsible authorities and/or persons under confidentiality obligation, such as auditors/attorneys.

VI. No obligation to provide

Whistleblowers are under no legal or contractual obligation to give us personal data on this Digital Reporting Channel, since a complaint or report of a breach is voluntary.

However, we point out that the personal data under II.1. above is captured when the Digital Reporting Channel is accessed from the internet, since that is necessary for the site to be provided at all.

VII. Rights of affected persons

If personal data is processed by users, they are affected persons pursuant to GDPR and have the following rights as against us as the responsible party when the legal conditions apply:

a. Right to lodge a complaint (Art. 15 GDPR)
b. Right to rectification (Art. 16 GDPR)
c. Right to erasure (Art. 17 GDPR)
d. Right to restriction of processing (Art. 18 GDPR)
e. Right to data portability (Art. 20 GDPR)
f. Right to revocation of declaration of consent (Art. 7 Para 3 GDPR)

Per Art. 21 GDPR, users have the right to object to the use of personal data pertaining to them per Art. 6 Abs. 1 lit. e or f) GDPR at any time for reasons based on their circumstances; this includes profiling based on these provisions.

As the responsible party we will then no longer process the personal data of these users, unless we can prove compelling reasons for such processing that outweigh the interests, rights, and freedoms of the users, or the processing serves the assertion, exercise, or defence of legal claims.

Irrespective of other administrative or legal remedies, per Art. 77 GDPR users have the right to file a complaint to a supervisory authority if they are of the opinion that processing of the personal data pertaining to them is in violation of the GDPR.

Stern-Wywiol Gruppe GmbH & Co. KG

An der Alster 81
20099 Hamburg, Germany
Tel.: + 49 40 284039-0
Fax: + 49 40 284039-88
info@stern-wywiol-gruppe.de
www.stern-wywiol-gruppe.de