Privacy Notice

We appreciate your support in complying with laws, regulations, and internal company rules, standards, and instructions.

When you report incidents via the whistleblower system, we protect your personal data to ensure that no disadvantages arise from your report.

Here you can learn how we use your personal data when you use this website, **unless you choose to report an incident anonymously.**

1. **What does this privacy policy apply to?**

This privacy policy applies to the website https://app.legaltegrity.com/report/e61f5201-b193-4f6c-9aa2-f21c6baa552a (“**whistleblowing website**”) and the platform offered under this URL for reporting incidents of unethical, illegal, and irresponsible behavior ("Platform"), to the extent that we collect, process, or use ("use") your personal data therein.

2. **Who is responsible for data processing?**

The entity responsible for the use of personal data on the whistleblowing website is **Tyczka GmbH, Blumenstraße 5, 82538 Geretsried** ("**Company**" or "**we**" or "us**"**).

Tyczka GmbH centrally processes all incoming information concerning one or more companies of the Tyczka Group.

The operational management is carried out by die Firma LegalTegrity GmbH, Platz der Einheit 2, 60323 Frankfurt, which acts as a contractor under a data processing agreement with **Tyczka GmbH.**

3. **How can the data protection officer be reached?**

You can reach our data protection officer as follows:

Digital Compliance Consulting GmbH
c/o Dipl.-Ing. Arnd Fackeldey
Karl-Arnold-Str. 44
52349 Düren
fackeldey@digital-compliance-consulting.com

4. **What are personal and anonymous data?**

We use personal and anonymous data on the whistleblowing website and platform.

- **Personal data** are all details about a specific or identifiable natural person. You are identifiable as a person if you can be directly or indirectly identified with these details, such as by a phone or credit card number.
- **Anonymous data** are data that do not relate to a person (i.e., you cannot be identified as a person directly or indirectly) or where the personal reference can only be restored with disproportionate effort.

5. **What rights do I have regarding my personal data?**

You have the right to **access, rectify, delete,** or **restrict** the **processing** of your personal data, as well as the right to **data portability** and to **object** to the processing of your personal data.

If you have given us consent to process your personal data, you have the **right to withdraw your consent.** Processing carried out before the withdrawal remains unaffected. Please contact our data protection officer (see section 3) if you wish to withdraw your consent.

You also have the right to **lodge a complaint** with a data protection authority. However, we ask that you first contact our data protection officer (see section 3) with any questions or complaints.

6. **For what purposes and on what legal basis are my personal data used?**

You can use the whistleblowing website anonymously and without providing your personal data.

If you voluntarily provide personal data, we use it within the framework of the whistleblowing website and the platform offered solely for investigating the reported incident, provided there is a legal basis for this use. This is the case if the applicable data protection laws permit the use of the data you have provided or if you have given us your consent to use the data.

The following table shows the purposes for which we process the data you provide and the legal basis for each. You can find the text of the General Data Protection Regulation (GDPR) here.

Processing Purposes	**Legal Basis**
Central processing by Tyczka GmbH with regard to all information concerning companies of the Tyczka group of companies and, if necessary, transmission of data to companies of the Tyczka group affected by the information.	Art. 6 para. 1 GDPR (Processing for the purpose of a legitimate interest). The legitimate interest consists of internal administrative purposes.
Your name, email address, phone number, and contact details to contact you for follow-up questions after your report.	Art. 6(1)(a) GDPR (Consent) Art. 6(1)(f) GDPR (Processing for the purpose of a legitimate interest; the legitimate interest is the efficient investigation of the incident you reported)
Details of the incident you reported (e.g., subject of your concern, time and duration of the incident, business unit, circumstances of becoming aware of the incident, uploaded documents)	Art. 6(1)(a) GDPR (Consent) Art. 6(1)(f) GDPR (Processing for the purpose of a legitimate interest; the legitimate interest is the efficient investigation of the incident you reported)

Processing Purposes	Legal Basis
Any other personal data you provide to us in the context of individual communication (e.g., by email, fax, phone, or via provided online forms) to respond to general inquiries or other concerns you have raised.	Art. 6(1)(a) GDPR (Consent)
Disclosure to professionals bound by confidentiality (lawyers, auditors) or other third parties contractually obligated to confidentiality (e.g., detectives) for further clarification of the reported incident and, if necessary, to assert civil claims against the reported persons.	Art. 6(1)(c) GDPR (Fulfillment of legal obligation) Art. 6(1)(f) GDPR (Legitimate interest; the legitimate interest is the enforcement of legal interests and the obtaining of professional and legal support in establishing a lawful state)
Disclosure to law enforcement authorities for the purpose of criminal prosecution in the event of criminally relevant actions by the reported persons.	Art. 6(1)(c) GDPR (Fulfillment of legal obligation) Art. 6(1)(f) GDPR (Legitimate interest; the legitimate interest is to support law enforcement authorities in investigating and prosecuting the incident)
Operation of the platform (processing) by LegalTegrity GmbH under a data processing agreement	Data processing agreement pursuant to Art. 28 GDPR Art. 6(1)(f) GDPR (Legitimate interest; the legitimate interest is the operation of the whistleblowing website by a specialized provider)
Pursuit of abusive reports; you will not suffer any disadvantages if you use the platform in good faith. In the event of abusive use of the platform to harm reported persons, we reserve the right to take action against the whistleblower.	Art. 6(1)(f) GDPR (Legitimate interest; the legitimate interest is to protect good faith whistleblowers and to protect the platform from abusive use)

We process your personal data only within the specified purposes and to the extent necessary for these purposes.

7. Consent

By submitting your report via the **platform**, you agree that Tyczka GmbH processes and stores your personal data provided therein for the purposes stated in this privacy policy. You also agree that Tyczka GmbH processes the personal data beyond the conclusion of an

investigation as long as necessary for a proper assessment of the incident regarding further action.

You can withdraw your consent at any time with effect for the future. Please address the withdrawal to

- the Chief Compliance Officer, Mr. Christoph Rupp, christoph.rupp@tyczka.de, Fon 08171 627-258

8. Is the provision of personal data required?

Whistleblowers who report unethical, illegal, and irresponsible behavior are not informants. However, please note that the information you provide about yourself, your colleagues, or any other aspect of company operations can lead to decisions that affect other people. Therefore, please only provide information that you believe to be correct to the best of your knowledge. Although you will not face sanctions if you provide information in good faith, even if it later turns out to be incorrect, the intentional provision of false or misleading information will not be tolerated.

You are neither legally nor contractually obligated to provide your personal data when using the whistleblowing website. However, providing your personal data allows us to ask follow-up questions and investigate the reported incident more quickly. If you do not provide personal information, we may have to discontinue the investigation of the incident due to incomplete or incorrect information.

9. To which recipients or categories of recipients are personal data disclosed?

Unless otherwise required by law, the processed personal data may only be read and used by persons who need access to the data to perform their professional duties related to the investigation of the incident. These persons may include responsible employees of the compliance, human resources, audit, legal, data protection, or security departments, or the management of Tyczka GmbH and companies of the Tyczka group (as far as they are affected by the reported incident), or technical employees of LegalTegrity GmbH. We generally do not disclose your data to third parties and will only transfer it to third parties without your consent if we are legally required to do so or due to a court or administrative decision. Additionally, we may disclose your personal data to the following recipients on a case-by-case basis:

- Law firms or tax advisors or auditors instructed by us
- Detective agencies

10. Are personal data transferred to third countries outside the European Union / European Economic Area?

All information stored in the platform database by LegalTegrity GmbH is hosted by a subcontractor (Telekom Deutschland GmbH, Landgraben 151, 53227 Bonn) of LegalTegrity GmbH.

A transfer to third countries (countries outside the European Union and the European Economic Area) generally does not take place. As an exception to this:

- we transfer personal data in the event of a report from a third country to the location in the third country where the incident occurred to conduct investigations on-site.

11. How long are personal data retained?

Tyczka GmbH processes personal data as long as it is necessary to fulfill legal obligations. It should be noted that reported incidents may need to be retained for documentation and audit purposes for a reasonable period. We process your personal data only as long as necessary for the purposes of the investigation and any subsequent civil or criminal actions against involved parties. In this regard, we follow the statutory civil and criminal limitation periods in individual case assessments.

Furthermore, we store your personal data as long as there are legal retention periods in connection with a report. This may be particularly relevant for tax-related matters, for which § 147 of the German Fiscal Code (AO) provides a retention period for business letters, including emails, of ten years.

Thank you for reading our privacy policy.