Privacy Notice

The company takes the protection of personal data very seriously. This privacy notice explains which personal data we collect from you when using the whistleblower system and how we use it. We ensure compliance with applicable data protection regulations through appropriate technical and organizational measures.

Controller and Data Protection Officer
The entity responsible for processing personal data is:

Domino's Pizza Deutschland GmbH
Am Sandtorkai, Hamburg, Hamburg, 20457, Germany

The company's Data Protection Officer can be reached at datenschutz@dominos.de.
The technical implementation of the whistleblower system is carried out on our behalf by EQS Group AG ("EQS").

Personal Data
In principle, the use of the whistleblower system is possible without providing personal data, as far as legally permissible. However, you may voluntarily disclose personal data during the whistleblower process, particularly information about your identity, first and last name, country of residence, telephone number, or email address.

We generally do not request or process special categories of personal data, such as information about racial and/or ethnic origin, religious and/or philosophical beliefs, union membership, sexual orientation, or health-related data. However, due to free text fields in the reporting form, such special categories of personal data may be voluntarily disclosed by you.

The report you provide may also contain personal data of third parties referenced in your report. Affected individuals will be given the opportunity to respond to the report. In such cases, we will inform the affected individuals about the report. Your confidentiality will be maintained, as no information about your identity will be disclosed to the affected person, as far as legally permissible, and your report will be used in a way that does not compromise your anonymity.

Purpose and Legal Basis of Processing
The whistleblower system allows you to contact us and report compliance and legal violations. We process your personal data to review the report you submitted via the whistleblower system and to investigate the alleged compliance and legal violations. We may need to ask you follow-up questions. For this purpose, we use only the communication channel provided by the whistleblower system. Confidentiality of the information you provide is our top priority.

The processing of your personal data is based on your consent given when submitting the report via the whistleblower system (Art. 6(1)(a) GDPR).

Additionally, we process your personal data to fulfill legal obligations, particularly in relation to criminal, competition, and labor law matters (Art. 6(1)(c) GDPR).

Finally, we process your personal data where necessary to protect the legitimate interests of the company or a third party (Art. 6(1)(f) GDPR). We have a legitimate interest in processing personal data to prevent and detect violations within the company, to review internal processes for legality, and to maintain the integrity of the company.

If you disclose special categories of personal data, we process them based on your consent (Art. 9(2)(a) GDPR).

We also use your personal data in anonymized form for statistical purposes.

We do not intend to use your personal data for purposes other than those listed above. If we do, we will obtain your prior consent.

Technical Implementation and Data Security
The whistleblower system includes an option for anonymous communication via an encrypted connection. Your IP address and current location are never stored during use. After submitting a report, you will receive login credentials for the whistleblower system mailbox to continue secure communication with us.

To ensure data protection and confidentiality, we maintain appropriate technical measures. The data you provide is stored in a specially secured database by EQS. All data stored in the database is encrypted by EQS according to the latest technical standards.

Disclosure of Personal Data
To fulfill the aforementioned purpose, it may be necessary to disclose your personal data to external parties such as law firms, criminal or competition authorities, possibly including entities outside the European Union.

When we disclose your personal data externally, we ensure a consistent level of data protection through appropriate contractual agreements. In all cases, the company remains responsible for data processing.

Finally, we transfer your personal data to EQS for technical implementation as described above. We have entered into a data processing agreement with EQS to ensure data protection.

Data Retention Period
We store personal data only as long as necessary to process your report or if we have a legitimate interest in retaining your personal data. Storage may also occur if required by European or national

legislation to fulfill legal obligations, such as retention requirements. Afterwards, all personal data will be deleted, blocked, or anonymized.

Your Rights
If you have provided personal data, you have the right to access, rectify, and delete your personal data. You may also restrict processing or request the transfer of your data to another controller.

Additionally, you have the right to object to the processing of your personal data at any time for reasons arising from your particular situation.

You have the right to withdraw your consent at any time. Withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

You may exercise these rights by sending an informal request to the controller or our Data Protection Officer mentioned above. If you have exercised your right to rectification, deletion, or restriction of processing, we are obliged to inform all recipients to whom we have disclosed your personal data, unless this proves impossible or involves disproportionate effort. Upon request, we will inform you about these recipients.

Finally, you have the right to lodge a complaint with a supervisory authority, without prejudice to any other administrative or judicial remedy, particularly in the Member State of your residence, workplace, or the place of the alleged infringement, if you believe that the processing of your personal data violates the GDPR.