

Privacy Notice – Information on processing of personal data related to the Speak Up Policy

This notice governs the processing of personal data of individuals who (i) report, (ii) are mentioned in a report, (iii) contribute to the investigation in any capacity (including as Speak Up Officers, Investigators, witnesses, etc), or (iv) are otherwise mentioned during the scope of the investigation of a Concern under BSEMEA’s Speak Up Policy (jointly, the “**Data Subjects**”). This notice applies to investigations of Concerns submitted through the BridgeLine, both as the group reporting and the local reporting channels established by the Bridgestone group entities listed in Appendix 2 to the Policy. This notice is an integral part of the Policy; any capitalised terms used in this notice which are not specifically defined herein have the meaning attributed to them in the Policy.

Who is responsible for the data processing?

For Concerns reported via the group reporting channel, Bridgestone Europe NV/SA with registered office at Da Vincilaan 1, 1930 Zaventem, Belgium (“**HQ**”) processes personal data as Data Controller, pursuant to the data protection laws. For Concerns reported through any of the local reporting channels referred to Appendix 2 of the Policy, Bridgestone Europe NV/SA and the Bridgestone entity to which the Concern is addressed are joint Data Controllers.

What Personal Data are processed?

Within the scope of an internal investigation, the following personal data may be submitted by the Reporter, or otherwise collected by the investigation team from (i) witnesses, (ii) other persons who may be asked to provide information relevant to the investigation, or (iii) the person(s) against whom the Concern was raised (“**Personal Data**”):

- ❖ Name, job title, relationship with Bridgestone and any other identification data;
- ❖ Recording of reported Concern (if the Concern is reported via phone);
- ❖ Any facts which, according to the Reporter, any witnesses, or the investigation team have occurred in connection with a Data Subject, including any potential sanctions they will be subject to.

Personal Data may also include special categories of data such as information on race or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health, sex life or relating to criminal convictions or offences (“**Sensitive Data**”). There is no obligation for the Reporter to submit Sensitive Data.

No IP addresses, MAC addresses, locations, or any other information are captured or stored by the Controller. We do not use technological means to determine the identity of a Reporter who choose to stay anonymous.

Our purpose and legal basis for the processing

We process the Personal Data to the extent necessary to investigate a Concern and define mitigating actions. In some jurisdictions, Bridgestone is obliged under applicable legislation to implement an internal reporting system to receive and investigate Concerns. In these situations, the processing of the Personal Data collected in connection with the concern reported via local reporting channel is necessary for compliance with a legal obligation to which the given data controller is subject, which arises in particular from the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons

who report breaches of Union law and legislation implementing this Directive into the local laws, as well as from the other laws. Where there is no such obligation, Bridgestone has a legitimate interest to investigate any Concerns, with the aim of deterring and stopping any violations of law or internal policies, and preventing such violations in the future.

To the extent that any Sensitive Data is processed, the exemption we rely on is the necessity of its processing for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject, or consent (as the case may be).

How long do we keep the personal data?

Personal Data shall be kept for at least five years from the receipt of the Concern and, regardless of such period, during any pending judicial or administrative proceedings relating to the reports. After that period, all personal data are either anonymised, i.e., all information that can be used to identify persons involved is removed or deleted irreversibly if they are no longer necessary to meet the requirements of applicable laws. For Local Concerns reported through a local reporting channel, other retention periods may apply, as described in Appendix 2 of the Policy. In said cases, the retention period set forth in Appendix 2 prevails.

With whom do we share the data?

Depending on the Concern, Personal Data can be processed by and transferred to any subsidiary, branch office or affiliate of Bridgestone worldwide. When Bridgestone requires the support of professional service providers and advisors to perform an internal investigation (including external lawyers, accountants, or other specialised service providers), said third parties may also access the personal data, acting as data processors of Bridgestone.

Personal Data can also be disclosed and transferred to any public and governmental authorities, including regulatory authorities, law enforcement, public bodies and judicial bodies. Any international transfer of Personal Data is covered by the appropriate legal and/or contractual measures. To request a copy and/or further information on such measures, please contact Bridgestone using the contact information below.

BridgeLine is operated by EQS Group AG, located at Talacker 41, 8001 Zurich, Switzerland (hereinafter referred to as “**EQS Group**”). EQS Group acts as a contracted data processor on behalf of Bridgestone. For all data storage purposes, EQS Group uses server systems of Swisscom AG, Alte Tiefenaustrasse 6, 3050 Bern, Switzerland (hereinafter referred to as “**Swisscom**”). These servers are located exclusively in Switzerland. Switzerland is recognized by the European Commission as a country that ensures an adequate level of protection for data transfers. The servers are protected from unauthorised access by various technical security measures. All data are transmitted and stored with encryption. Only employees of Bridgestone involved in the investigation have access to these data. Neither EQS Group, Swisscom nor third parties can view the stored information.

Data Subject Rights

You have the following rights with respect to the processing of Personal Data relating to you:

- ❖ request access to your Personal Data, and ask for rectification of inaccurate data;
- ❖ request the erasure of your Personal Data when (i) no longer needed by us, (ii) you objected to the processing (unless we have an overriding interest) or (iii) we have processed unlawfully;

- ❖ request the restriction of the processing of the Personal Data relating to you when (i) you contest the accuracy of the data, (ii) our processing is unlawful but you do not want the data to be deleted, (iii) we no longer need the data but you require it for a lawsuit, or (iv) pending the verification of our overriding legitimate interest when you have objected to our processing;
- ❖ object to the processing of the Personal Data relating to you on the grounds of your particular situation, and except where we have an overriding interest;
- ❖ request portability, to the extent applicable;
- ❖ lodge a complaint with the competent supervisory authority, in particular in the country of your habitual residence, place of work or place of the alleged infringement.

Contact the Data Controller

If you have any question in relation to the processing of your Personal Data, or want to exercise the above listed rights, you can contact Bridgestone's Data Protection Organisation via privacy@bridgestone.eu.