

Information on Data Protection in the Whistleblower System of Boll & Kirch Filterbau GmbH

<https://boll.online-hinweisgeber.de/en>

In the following, we would like to inform you about the collection, processing and use of personal data if you report information to us about a violation of laws or company rules within the meaning of the Whistleblower Protection Act, which you have obtained in connection with or in the run-up to your professional activity, and use our online whistleblower portal at <https://boll.online-hinweisgeber.de/en> in doing so. Please therefore read this data protection information very carefully before submitting an online report.

INTRODUCTION

Data protection is very important to Boll & Kirch Filterbau GmbH and the whole group of Bollfilter companies. We also understand that data protection is very important to you. In this data protection notice, you will learn how we protect and use information that we collect via our online whistleblower portal and, in certain circumstances, disclose excerpts relating to the content of the report.

Certain information – which may also include personal data – that we collect is necessary for us to fulfil our legal obligations under the Act for the Better Protection of Persons Providing Information (Whistleblower Protection Act – HinSchG), while other information is necessary to enable us to technically operate the online portal we have set up for this purpose and which provides you with an internal reporting channel within the meaning of the Whistleblower Protection Act.

Until the aforementioned Whistleblower Protection Act (HinSchG) comes into force, implementing the EU Whistleblower Directive into national law, we invoke our legitimate interest within the meaning of Article 6(1)(f) GDPR in the detection and prevention of malpractice in the companies of our group that is punishable by penalties or fines or that violates EU or national law. Another legitimate interest is to prepare ourselves for the upcoming entry into force of the Whistleblower Protection Act and to provide an appropriate and functional whistleblower system at that time.

1. Responsible entity and data protection officer

The responsible entity for this web-based whistleblower portal is

Boll & Kirch Filterbau GmbH
Siemensstraße 10 – 14
50170 Kerpen (Germany)
Phone: +49(0)2273-562-0
Fax: +49 (0)2273-562-223
E-mail address: datenschutz@bollfilter.com

You can contact our data protection officer by e-mail at kinga.moeller@vuv-consult.de ((in person) oder dsb@vuv-consult.de (team of data protection officers).

If you report a breach that does not concern Boll & Kirch Filterbau GmbH, but rather another company of the Bollfilter Group, this other company shall be jointly responsible with us for the data processing within the meaning of Article 26 GDPR.

2. System provider

We provide our online whistleblower system <https://boll.online-hinweisgeber.de/en> from the provider iComply GmbH, Große Langgasse 1A, DE-55116 Mainz, telephone +49 6131 27626 80, e-mail kontakt@iwhistle.de, via OK MEDIA Webconsulting UG (limited liability), Untergasse 2, 65474 Bischofsheim, with hosting in the Open Telekom Cloud (ISO/IC 27001) under the strictest security precautions and exclusively in Germany.

Data that is processed to provide the online reporting portal

a. What data is processed and for what purpose?

Each time our online whistleblower system is accessed, our system (i.e. the web server) automatically records information from the system of the user's accessing computer or terminal device that may enable identification. The following data is recorded and temporarily stored:

- Date and time of access
- User IP address
- Host name (Internet server provider) of the accessing computer
- The website from which the website was accessed (so-called referrer URL).
- Websites accessed via the website
- Visited page on our website
- Message whether the retrieval was successful
- Amount of data transmitted
- Information about the browser type and version used
- Operating system of the user's terminal device

The temporary storage of data during the course of your visit to our online portal is technically necessary in order to enable the provision of the portal. This data is not used for any other purpose and is immediately deleted or completely anonymised after the end of your visit to the portal.

b. On what legal basis is this data processed?

The data is processed on the basis of Article 6(1)(f) GDPR to protect our legitimate interests in providing a user-friendly, easily accessible and functional internal pathway for our employees and other persons entitled to report violations under the Whistleblower Protection Act. In this context, the provision of the internal reporting channel is in itself a legal obligation to which we are subject as an employer under the Whistleblower Protection Act, and the implementation of this obligation by providing an online whistleblower portal is in line with our aforementioned legitimate interest in a simple internal reporting facility.

c. Are there any other recipients of the personal data besides the responsible entity?

The parties mentioned under point 2 "System providers" have the theoretical possibility of viewing the personal data collected and processed by us via <https://boll.online-hinweisgeber.de/en>. However, access is expressly not provided for, indeed is even excluded, by contract and is secured via a processing contract in accordance with Article 28 GDPR. During transmission, there is end-to-end TLS encryption of the data, including the metadata of files, whereby neither system operators nor third parties have access to the encryption key.

d. How long is the data stored?

The data is deleted as soon as it is no longer required for the purpose for which it was collected. The data is deleted as soon as it is no longer required for the purpose for which it was collected. In the case of the provision of an online portal, this is the case when the respective session has ended.

The log files are stored for a maximum of seven days and are directly and exclusively accessible only to the administrators of the portal provider. After that, they are only indirectly available via the reconstruction of backups and are permanently deleted after a maximum of four weeks. Storage beyond this period is possible, but in this case the IP address of the user is deleted or masked in a way that it is no longer possible to assign it to the retrieving client and the data contained therein no longer contains any personal reference.

Data collected and (further) processed by a whistleblower during and on the basis of a personalised report in the online whistleblower portal (personalised report)

e. What data is processed and for what purpose?

The whistleblower portal is our internal reporting office. You can report information about violations of laws or company rules that you have obtained in the run-up to or in connection with your professional activity at our group of companies or with us to this portal via the indicated reporting form.

When submitting a personalised report, the following personal data is processed:

- **the company of the Bollfilter Group to which your message refers**
- **surname and first name**
- **relationship of the whistleblower to us or another company of the Bollfilter Group**
- **e-mail address**
- **text of notices submitted and information communicated in this context**
- **communication with the whistleblower and internal and external parties involved**

If you send such a report to our internal reporting office, you will receive an acknowledgement of receipt within seven days to the e-mail address from which you made the report or which you provided to us. No later than three further months later, you will receive a response including information on planned and already taken follow-up measures and the reasons for these.

The personal data submitted with the report (whistleblower data) will be stored with the report within the whistleblower system. This data will be used exclusively for processing your report. The purpose of the processing is therefore to enable the transmission of the acknowledgement of receipt and to maintain contact with you as a whistleblower and, if necessary, to be able to request further information.

The internal reporting office examines all incoming reports to determine whether they fall within the material scope of the Whistleblower Protection Act and whether they are substantiated enough to take appropriate follow-up measures (such as conducting internal investigations or handing over the proceedings to the competent department or authority). In this context, the identity of the whistleblower may only be disclosed to the persons responsible for receiving reports or taking follow-up action, as well as to the persons assisting them in the performance of these tasks.

f. On what legal basis is this data processed?

The data is processed on the basis of Article 6(1)(c) GDPR to fulfil our legal obligations under the Whistleblower Protection Act, to which we are subject as a company, whereby Section 10 HinSchG expressly permits the processing of personal data required for this purpose.

According to Section 12(1) sentence 1 of the HinSchG, we as an employer are obliged to set up and operate at least one internal office to which employees can turn to report information on violations subject to the material scope of the Whistleblower Protection Act which they have obtained in the run-up to or in connection with their professional activities. With our online portal, we provide our employees and other persons eligible to submit reports with such an internal reporting channel and process the information reported via this channel in accordance with Sections 10, 13 et seq. of the Whistleblower Protection Act.

Until the aforementioned Whistleblower Protection Act (HinSchG) comes into force, we invoke our legitimate interests within the meaning of Article 6(1)(f) GDPR as described in

paragraph 3 of the introduction to this Data Protection Notice as the legal basis for data processing.

g. Are there any other recipients of the personal data besides the responsible entity responsible for data processing?

The parties mentioned under point 2 "System providers" have the theoretical possibility of viewing the personal data collected and processed by us via <https://boll.online-hinweisgeber.de/en>. However, access is not expressly provided for in the contract and can, at most, occur within the scope of technical support processing on our express instruction; this is secured via an order processing contract in accordance with Article 28 GDPR. During each transmission, there is end-to-end TLS encryption of the data, including the metadata of files, whereby neither system operators nor third parties have access to the encryption key.

h. How long is the data stored?

The data is deleted as soon as it is no longer required for the purpose for which it was collected. In the case of personal data transmitted to us within a person-specific report, this is the case when the respective communication with the whistleblower has ended.

The dialogue is ended when it is clear from the circumstances that the matter in question has been finally clarified. From this point in time (usually when the whistleblower is given feedback), the processing of this data can be restricted. However, deletion only takes place after the respective retention period has expired.

All reports received by the reporting office must be documented in a permanently retrievable manner in compliance with the confidentiality requirement of the Whistleblower Protection Act, and this documentation must be deleted three years after the conclusion of the process.

Rights of the data subjects

a. Right to information

In accordance with Article 15 GDPR, you can request information about the personal data we process.

b. Right of rectification

If the information concerning you is not (or is no longer) correct, you may request correction in accordance with Article 16 GDPR. If your details are incomplete, you can request that they be completed.

d. Right to erasure

In accordance with Article 17 GDPR, you have the right to have your personal data deleted.

e. Right to restrict processing

Pursuant to Article 18 GDPR, you have the right, if the criteria are fulfilled, to request restriction of the processing of your personal data.

f. Right of appeal

If you believe that the processing of your personal data violates data protection law, you have the right to complain to a data protection supervisory authority of your choice in accordance with Article 77(1) GDPR. This includes the data protection supervisory authority responsible for the responsible entity: State Commissioner for Data Protection and Freedom of Information of North Rhine-Westphalia, Postfach 20 04 44, 40102 Düsseldorf, +49 (0)211/38424-0, poststelle@ldi.nrw.de.

g. Right to data portability

In the event that the requirements of Article 20(1)GDPR are met, you have the right to have data that we process automatically on the basis of your consent or in fulfilment of a contract released to yourself or to third parties. The collection of data for the provision of the website and the storage of log files is absolutely necessary for the operation of the website. This is therefore not based on consent pursuant to Article 6(1)(a) GDPR or on a contract pursuant to Article 6(1)(b) GDPR, but is justified under Article 6(1)(f) GDPR and therefore does not meet the requirements for data portability.

[Right to object under Article 21\(1\) GDPR](#)

You have the right to object at any time, on grounds relating to your particular situation, to the processing of your personal data by us pursuant to Article 6(1)(f) GDPR, i.e. processing that we base on our legitimate interests. The responsible entity will then no longer process the personal data unless it can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or the processing is carried out for the purpose of asserting, exercising or defending legal claims. The collection of data for the provision of the website and the storage of log files is absolutely necessary for the operation of the website.

[Amendment and updating of the data protection notice](#)

We reserve the right to update our data protection notice from time to time if changes in the data processing we carry out make this necessary or if the legal framework or its interpretation and application practices that form the basis of our data processing change.

We therefore ask you to inform yourself about the content of our data protection information at regular intervals.