**Specific data protection information in accordance with Art. 13 GDPR on the whistleblower system of the Lapp Group**

As a responsible company or operator of the website, we take the protection of your personal data very seriously. Insofar as it arises in the context of your notification and communication via the platform provided by us, we treat your personal data confidentially and in accordance with the statutory data protection provisions and this privacy policy.
In the interest of transparency under data protection law, the following policy serves to explain the reporting platform we use and to inform whistleblowers using this system about the handling of whistleblower reports received and about the type, scope and purpose of the collection and use of data.

**Information on the controller**

Lapp Holding SE
Oskar-Lapp-Str. 2
Stuttgart 70565
0711 7838-01
www.lappgroup.com

- hereinafter referred to as **Company/we** -

If you have selected one of the following national companies of the Lapp Group on the platform, this company is the controller with regard to those personal data that you enter on the platform and provide with a reference to this company. With regard to this data, Lapp Holding SE will act as a processor. A corresponding contract has been concluded These companies are:

- U.I. Lapp GmbH

- Lapp Service GmbH

- Lapp Mobility GmbH

- Lapp GmbH Kabelwerke

- Contact GmbH Elektrische Bauelemente

- Lapp Systems GmbH

- Lapp Austria GmbH

- Lapp Benelux B.V.

- Cableries Lapp S.a.r.l.

- Lapp France S.a.r.l.

- Lapp Muller S.A.S.

- Lapp Czech Republic s.r.o.

- Lapp Automaatio Oy

- Lapp Connecto Oy

- Lapp Hungaria KFT

- Lapp Sistemi Italia S.R.L.

- KU Distribution S.r.l.

- Unika S.p.A.

- Lapp Italia S.r.l.

- Camuna Cavi S.r.l.

- CEAM Cavi Speciali S.r.l.

- Policabos S.A.

- Lapp Romania SRL

- Lapp, d.o.o.

- Lapp Miltronic AB

- Fleximark AB

- Lapp Holding NA Inc.

- Lapp USA Inc.

- Lapp Cable Works Inc.

- Lapp Tannehill Inc.

- hereinafter referred to as **National Company** -.

Unless otherwise stated, the information below also applies with regard to the national company.

The controller is the natural person or legal entity who alone or jointly with others determines the purposes and means of the processing of personal data (e.g. names, email addresses or similar).
For this purpose, the controller uses a service provider who provides the reporting platform as a data processor. otris software AG (hereinafter referred to as the operator) operates the reporting platform of our whistleblower system as a neutral, trustworthy and secure entity. The data collected and stored here is transmitted to us in encrypted form.

**Description of the processing process**

For companies, internal grievances, especially crime within the organization, can have threatening consequences. To support the establishment of whistleblower systems and the protection of whistleblowers, the EU Directive 2019/1937 on the protection of persons who report breaches of Union law entered into force on October 23, 2019. The whistleblower system enables anonymous communication with whistleblowers via a secure, web-based reporting platform.
We are convinced that a whistleblower system helps us to quickly identify weaknesses and grievances and thus directly contributes to sustainable corporate success.

**What personal data are collected?**

Only personal data that the whistleblower consciously provides are collected:

* Name
* Email address
* Other personal data arising in the context of the description of the information

**Lawfulness of the processing**

We have a legitimate interest in processing the personal data you knowingly provide to prevent and detect breaches within our organization, to verify the lawfulness of internal procedures, and to protect our integrity. The lawfulness of the processing of personal data (of the whistleblower as well as of the person affected by the report) thus results from Art. 6 (1) sentence 1 f) GDPR in conjunction with Section 26 (1) sentence 2 of the German Federal Data Protection Act [BDSG], Art. 88 GDPR:

* Furthermore, the processing of personal data results from a legal obligation pursuant to Art. 6 (1) sentence 1 c) GDPR in conjunction with Section 25a (1) sentence 6 no. 3 of the German Banking Act [KWG].
* Insofar as the whistleblower wishes to disclose his or her identity intentionally or knowingly, the legal basis for such disclosures is consent pursuant to Art. 6 (1) sentence 1 a) GDPR (conscious removal of anonymity in the reporting form). You have the right to revoke your consent at any time pursuant to Art. 7 (2) GDPR, although this would in fact only be effectively possible up to one month after the report has been made, as the accused person must be informed of the processing of his or her data and of the identity of the whistleblower pursuant to Art. 14 (3) a) GDPR no later than one month after the report.

**Purpose**

The whistleblower system is available to employees of our company and third parties (e.g., customers, business partners, suppliers, employees of affiliated companies) for whistleblowing.
The whistleblower system serves to receive and clarify serious suspicions of breaches of EU law in accordance with EU Directive 2019/1937, in particular criminal acts that could endanger our company, as well as to record general process deficiencies and weaknesses that require appropriate action.
These include, but are not limited to, breaches in the areas of:

* Accounting, audits, and internal financial controls (e.g., accounting, financial reporting, and auditing irregularities, financial misconduct in internal controls)
* Corporate integrity (e.g.: bribery, corruption and fraud, gifts and hospitality, falsification of documents, conflicts of interest, competition and antitrust, confidentiality and data protection breaches).
* Environment, health and safety (e.g.: breaches of environmental regulations and occupational health and safety regulations; including bodily injury and abuse).
* Human resources, diversity and respect in the workplace (e.g.: discrimination, (sexual) harassment and bullying, human rights violations, compensation, general personnel matters, misconduct or inappropriate behavior)
* Misuse/embezzlement of assets or services (e.g., unauthorized use of company-owned resources or equipment for non-business reasons, theft of company property, labor fraud)
* Other (other breaches of regulations, laws and guidelines, general suggestions for improvement and new ideas)

The aim is to process whistleblowers' data while preserving their anonymity. The whistleblower system collects data on the type of general system usage. These include the number of messages for specific categories and message processing information. The whistleblowing system does not allow any statistical evaluations to be carried out that would allow conclusions to be drawn about an individual user. The whistleblower system is an Internet-based alternative to the usual communication channels and/or internal company functionaries and therefore does not necessarily request personal data from the whistleblower. The whistleblower's personal data is entered into the whistleblowing system on a voluntary basis.

**Storage of the whistleblower's personal data**

Anonymity guarantee: User behavior is recorded anonymously by the whistleblower system. Voluntarily provided personal data can be viewed by whistleblowers at any time via the whistleblower tracking system.
Further information about the personal data stored in the whistleblower system (reporting platform) is technically not possible. All data entered by the whistleblower is stored individually encrypted in a database. Neither administrators, website operators nor other persons have the possibility to gain access to the content of the personal data deposited by the whistleblower.

**Storage of personal data of the person affected by the notice**

In the event that personal data is stored, the person affected by this will be informed about the processing and use of this data as soon as there is no risk to the clarification of the facts. In this case, the person affected by the report also has a right to information about the personal data stored about them. Subject to the above provisions, the identity of the whistleblower shall be excluded from this right to information.

**Disclosure of personal data**

When breaches of conduct are reported, the designated department (e.g. Internal Audit, Compliance and any Group companies involved) receive the personal data for further internal processing.
Please keep in mind that pursuant to Art. 14 GDPR, within one month after whistleblowing without the knowledge of the data subject, the data subject must be informed, if necessary, disclosing the identity of the whistleblower.
In addition, the operator of the reporting platform of our digital reporting system processes your personal data as a data processor used by us (Art. 28 GDPR). In this context, the operator shall provide sufficient guarantees that appropriate technical and organizational measures are implemented in such a way that the processing is carried out in compliance with the requirements of the GDPR and the protection of the rights of the data subjects is ensured.
For its part, the operator uses the service providers bytemine GmbH and gridscale GmbH, whereby the subcontracted processors only have the possibility of becoming aware of personal data and the data is pseudonymized or even cleansed of any personal reference (anonymized) to this extent.
Disclosure and processing of the data to an employee in the company affected by the report, insofar as this is necessary for clarification, requires the prior consent of the whistleblower. We would like to point out that in the case of such consent, the recipient may be obliged pursuant to Art. 14 GDPR to inform the person affected by the report also of the identity of the whistleblower one month after becoming aware of it, at the latest, however, if such information would not jeopardize an effective investigation of the allegation or the collection of the necessary evidence. If a whistleblower gives consent to the disclosure of his or her identity, they may revoke this consent in accordance with Art. 7 (2) GDPR up to one month after the report has been made.
Freedom from seizure cannot be guaranteed. By order of the Bochum Regional Court dated March 16, 2016, a seizure by the public prosecutor's office for the purpose of investigating the identity of a whistleblower was expressly permitted.

**Data Transfer with Non-EU countries (Third Countries)**

Insofar as the national company, which is the controller in your case, has its registered office outside the EU, data will be transferred back to it by the processor. For data protection purposes, we have concluded an order processing agreement that also includes the standard contractual clauses. We have carried out the required Transfer Impact Assessment (TIA), i.e. identified and implemented measures that ensure the required level of data protection.

**Safeguarding the rights of data subjects**

According to European data protection law, you and the persons named in the report have the right to information, correction, deletion, restriction of processing, as well as the right to object to the processing of your personal data. Under Art. 15 GDPR, the data subject, both the whistleblower and the accused person, has the right to information about the data stored about them, also insofar as it relates to the origin and recipient. However, there is no obligation to provide information if the information would disclose information that must be kept secret due to overriding legitimate interests of a third party, Section 29 (1) sentence 2 BDSG. If the right to object is exercised, we will immediately check the extent to which the stored data are still required; in particular for processing a report. Data that is no longer required will be deleted without undue delay. For further questions and the possibility to assert your rights, you can contact us at any time at the address indicated on page 1 (controller).
Furthermore, you have the right to lodge a complaint with the competent supervisory authority.

**Deletion & Change**

Whistleblowers and data subjects have the right to have incorrect data corrected, changed, blocked or deleted if the legal requirements are met. The statutory deletion periods shall apply. If whistleblowers have transmitted personal data in the course of the dialog, this data will be retained for as long as is necessary to clarify and conclusively assess the facts reported. After completion of the report processing, these data are deleted in accordance with the legal requirements.
To maintain the integrity of the data, the application and the database are backed up on a regular basis. The retention period of a backup is a maximum of one calendar month. Older backups and all corresponding copies are automatically deleted.

**SSL or TLS encryption**

This site uses SSL or TLS encryption for security reasons and to protect the transmission of confidential content that you send to us as the site operator. You can recognize an encrypted connection by the fact that the browser address bar changes from "http://" to "https://" and by the lock symbol in your browser bar. If SSL or TLS encryption is activated, the data you transmit to us cannot be read by third parties.

**Data protection officer/ supervisory authority**

Data protection officer of Lapp Holding SE:

Matthias Walliser Dipl.-Ing. (BA)
*geprüfter Datenschutzbeauftragter (udis)*
**walliser consulting gmbh**
Altenwaldstr. 8
72768 Reutlingen
Geschäftsführer:
Finn-Lucas Walliser, Matthias Walliser

Meine Bürozeiten: **Di. - Mi. - Do**. von 8:30 – 15:30 Uhr
Freitags ist unser Büro nicht besetzt
Tel.     07121/ 69 702 – 27
Mail   beratung@walliser-datenschutz.de

Internet:  [www.walliser-datenschutz.de](http://www.walliser-datenschutz.de/)

This function is also the point of contact with regard to the national companies.

Controller’s competent supervisory authority

Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg

Postfach 10 29 32, 70025 Stuttgart

Lautenschlagerstraße20, 70173 Stuttgart

Tel.: 0711/61 55 41 – 0

Fax: 0711/61 55 41 – 15

E-Mail: poststelle@lfdi.bwl.de

Internet: [http://www.baden-wuerttemberg.datenschutz.de](http://www.baden-wuerttemberg.datenschutz.de/)