GREIF DATA PRIVACY POLICY

(Version May 18, 2018)

Data privacy laws safeguard information about individuals – their personal data. At Greif, we respect the privacy rights of our employees, customers, suppliers and business partners. We are committed to managing personal data in a professional, lawful and ethical way.

Personal data are broadly defined as any information relating to an identified or identifiable individual such as name and contact details. Some private information, such as race or ethnic origin, health data, sexual orientation, criminal behaviour or trade union membership is sensitive personal data and subject to more stringent requirements. Processing of personal data means any action involving personal data, including collecting, using, accessing, viewing and even deleting them.

As personal data are everywhere, privacy rules apply to virtually every business process in Greif. If we do not comply with privacy rules, we risk causing harm to individuals, being ordered to cease any processing, and potential fines or litigation. We are also putting Greif's reputation at risk. Therefor, all our employees and suppliers using personal data, are required to abide by the law and the below key principles on data privacy and do's and don'ts (see next page).

Questions & Communication: For further information, please refer to Inside Greif / Data Privacy. For any questions, please refer to your HR Department or IT contact as appropriate, or contact Greif's Data Privacy Team at:

DataPrivacyTeam@Greif.com

Greif Key Principles on Data Privacy and dos and don'ts:

1. Comply with privacy laws. Always follow the Greif Code of Conduct and Greif's Guidelines on Data Privacy Topics as published on Inside Greif/Data Privacy page when processing personal data.

2. Only process personal data for specific, defined, legitimate business purposes.

3. Do not excessively process personal data; do not process more personal data than necessary; do not access more personal data than strictly necessary for the performance of your job.

4. Do not keep personal data longer than necessary, and then ensure they are securely and irreversibly deleted.

5. Treat personal data as confidential and use appropriate physical and IT security safeguards. Tell Greif immediately if you know of or suspect any security breach, and use the Data Security Breach Procedure on Inside Greif/Data Privacy.

6. Inform individuals, using clear and easy to understand language, about why you are collecting their personal data, what you are going to do with their data and for how long. In some cases, you will need to get their prior consent.

7. Safeguard personal data before disclosing or sharing them with third parties, by entering into proper contracts.

8. Respect the rights of individuals to access, correct, restrict and remove their personal data.

9. Identify privacy risks before processing personal data, such as in a new IT system, business process or service.

10. Be transparent about the personal data that you process. Do not process personal data without individuals being aware of you doing so.

11. Don't process any sensitive data (for example medical data, data on race, religion or sexual preference) unless you have been explicitly authorized to do so and this processing has been confirmed to be compliant with the law.

12. Do ask questions about privacy and think about how you can help ensure personal data is kept safely and processed legally in our company. Compliance is a team effort.