Data Privacy Statement Relating to The Dover Hotline

Prepared on September 11, 2019

Updated on February 21, 2020

1. Introduction

Dover Corporation (the "**Company**") is committed to protecting your personal data, and intends to process your personal data in a transparent and lawful way. Personal data is any information relating to an identified or identifiable natural person. Your name, address, phone number, and bank account number are examples of personal data. In all circumstances the Company aims to process personal information according to the following principles:

a. Transparency: Personal data is used fairly, lawfully, and transparently.

b. Limited Use: Personal data is collected for a specific and legitimate business purpose and used in a manner that is compatible with for that purpose. We securely dispose of it when it is no longer needed.

c. Data Minimization: Only relevant data – not excessive amounts – is collected and used.

d. Accuracy: We aim to keep personal data accurate and up-to-date.

e. Security and Limited Access: Personal data is stored securely and is shared only with those individuals who need the data to accomplish a business objective.

This Data Privacy Statement is intended to provide you with some information regarding how your personal data may be collected, used, shared, protected and otherwise processed within the Dover Global Hotline and related reporting process (the "**Hotline**") that will be deployed by the Company, which is described in greater detail in the sections below. You can find the latest version of this Data Privacy Statement on: www.thedoverhotline.com. The Company may change this Statement from time to time by updating this page.

2. Who is the relevant "controller" of your personal data?

The Hotline is implemented by Dover Corporation. Our intention is for the implementation of the Hotline to comply with applicable data protection laws, including the EU General Data Protection Regulation ("**GDPR**") and applicable local laws. Dover Corporation is the data controller of the personal data collected via and contained in the Hotline, and can be contacted here: 3005 Highland Parkway, Suite 200 Downers Grove, Illinois 60515 USA, privacy@dovercorp.com. If you would like to contact the data protection officer responsible for your OpCo and need assistance locating the officer, you may contact privacy@dovercorp.com.

3. What data is being collected or gathered?

With regard to the Hotline, the Company processes your personal data in order to address concerns ("**Reports**") made through the Hotline, whether made by employees of Dover Corporation or its Operating Companies ("**Employees**"), vendors, suppliers, and business partners and those of its subsidiaries, or other third parties who may file such reports (collectively, "**Reporters**"), as described further in Section 5 below.

We do not collect personal data revealing racial or ethnic origin, political opinions, religious, or philosophical beliefs, trade-union membership, genetic data, biometric data or data concerning health or sex life and sexual orientation.

With regard to the Hotline, the Company may obtain the following categories of personal data, from the following source(s):

a. Reporters. Reporters are asked but are not required to provide:

    a. Reporters' name and contact details (optional).

    b. Reporters' relationship to the Company (optional).

    c. A description of the concern and circumstances of the incident.

    d. Personal data of persons named in the Report ("Named Person"), including name, title, and contact details (optional).

    e. Any details which may be valuable in the evaluation and resolution of the Report (e.g. dates and time, witnesses, and location).

Please note that the use of the Dover Hotline is entirely voluntary, and the above data will be gathered only if a Reporter elects to use the Dover Hotline to make a report.

b. Dover Systems. If the Reporter is a current or former Employee, information may be obtained from Dover Systems (e.g. HR Central, Active Directory), including job title, manager's name, the Dover segment or Operating Company ("OpCo")/Business Group that the Reporter works/worked in, business contact details (e.g. business address, phone, email), and the functional area of the Reporter's job.

c. Other Company Systems. If the Reporter is not a current or former Employee, for purposes described in section 5 below, information may be obtained from Company systems (e.g. CRM), including title, relationship to the Company, or business contact details (e.g. business address, phone, or email).

4. How is the data being processed?

Dover has established the Hotline to provide Reporters with an additional, electronic method (e.g. phone and web) of making a Report relating to ethical matters and concerns, including suspected violations of Company policies, financial reporting standards, or laws and regulations. The intake and centralized database for the Hotline is operated by a third party vendor, located in the United States (NAVEX Global, Inc.)

We will not use your personal data for decisions based solely on automated processing if the decision produces legal effects concerning you or significantly affects you, unless you gave your explicit consent for this processing.

With regard to the Hotline, the Company will be processing the personal data described above in the following manner:

a. Stored. Personal data will be stored centrally so the Dover Corporate Compliance Department can ensure Reports are reviewed and, as needed, investigated. The information stored in the NAVEX database can only be accessed by the Dover Corporate Compliance Department and Dover Corporate Legal Department.

b. Transmitted. Personal data will be transmitted to individuals for purpose(s) listed in Section 6.

c. Retrieved. If required, a qualified Company Employee or third party (e.g., an independent investigator) will be provided personal data relating to a Report in order to conduct a fair and unbiased investigation and prepare a summary of findings which includes (1) identity and function of Named Person, (2) objective description of facts, (3) additional information collected during the investigation, (4) summary of the steps taken to investigate, and (5) the outcome. Qualified Company business, legal and HR leadership may be provided with some or all of the data captured in those summary of findings reports. See Section 6 below for further information on the categories of recipients who may be provided access to personal data from the Hotline.

Your personal data may also be processed in connection with any legal proceedings or prospective legal proceedings, in order for the Company to establish, exercise or defend its legal rights, or in order to fulfill legal obligations, including but not limited to responding to a request from a competent administrative or judicial authority or in any circumstance where such processing is requested pursuant to applicable laws.

5. Why does the data need to be processed?

Processing personal data in the Hotline will always be based on lawful grounds. With regard to the Hotline, the Company will process the personal data described above for the following purpose(s):

a. To comply with business and legal requirements to have a reporting mechanism and process to address concerns relating to ethical matters and concerns, including suspected violations of Company policies, financial reporting standards, and laws and regulations, which protects employees, the Company, and its' stakeholders. Such legal requirements include the Sarbanes-Oxley Act of 2002 ("SOX"), as well as other countries' whistleblower and anti-corruption laws, such as The Bribery Act 2010 ("UK Anti-Bribery Act") and Sapin II.

b. To address Reports, including reviewing the accuracy of the reported facts and, if necessary, conducting an investigation.

The Company is relying on one or more of the following legitimate grounds for this processing:

a. **Legitimate Interests:** The processing described is necessary to administer and facilitate your employment relationship with us. Specifically, it is in the Company's legitimate interest to process data in the Hotline to ensure Reports are addressed. The Company has weighed these legitimate interests against your fundamental rights and freedoms, and concluded that the processing outlined here is legitimate, proportionate and appropriate. Further information can be provided regarding this analysis upon request. If you are located within a jurisdiction where GDPR applies: This processing will rely on Art. 6 (1) f) GDPR.

   Please note that you have a right to object to the processing of your personal data where that processing is carried out for Company's legitimate interests. However, Company may not be able to fulfil this request in all instances.

b. **Legal Obligation:** The processing described in this Privacy Statement may be necessary to satisfy certain legal obligations of the Company including, without limitation its obligation to comply with business and legal requirements to have a reporting mechanism and process to address concerns relating to ethical matters and concerns, including suspected violations of Company policies, financial reporting standards, and laws and regulations, which protects employees, the

Company, and its' stakeholders. Such legal requirements may include the Sarbanes-Oxley Act of 2002 ("SOX"), as well as other countries' whistleblower and anti-corruption laws, such as The Bribery Act 2010 ("UK Anti-Bribery Act") and Sapin II. If you are located within a jurisdiction where GDPR applies: This processing will rely on Art. 6 (1) c) GDPR.

c. **Collective Agreements:** The processing described may be carried out in accordance with applicable works council agreements. If you are located in Germany: This processing will rely on Art. 88 GDPR, § 26 (4) German Data Protection Law (*Bundesdatenschutzgesetz*) and the respective works council agreement applicable for your OpCo.

6. Who has access to your personal data?

The Company limits who has access to the personal data in our possession to only those who need it for a legitimate business purpose. Personal data is shared on a "need to know" basis. Only those individuals and third parties who need the data to accomplish a business and/or other legitimate objective should have access to the personal data, and only for as long as they need it to accomplish the objective. Individual recipients are not authorized to share personal data with other employees or third parties unless that sharing is authorized and complies with all applicable Company policies and procedures. To the fullest extent possible, Reports will be handled confidentially, including the Reporter's identity. If a person listed below is a Named Person in a Report, they will not be given access to data from that particular report. For the Hotline, we anticipate that the following recipients will have access to your personal data, for the purposes listed below:

a. Dover Corporate Compliance Department, including the Chief Compliance Officer; Director, Ethics & Compliance; and Compliance Manager(s), are responsible for implementing and maintaining a retaliation-free internal reporting process (e.g. the Hotline) to ensure the Company operates with the highest ethical standards and can address violations of Company polices, financial reporting issues, or laws and regulations, which, left unaddressed, would be detrimental to the Company and its' stakeholders. Accordingly, this role has access to the centralized database and to all data relating to Reports to (1) ensure compliance with the procedures of the Hotline, (e.g. non-retaliation, fair and unbiased reviews, and confidentiality), (2) provide data in Reports to individuals in sections b through h to be reviewed and addressed, and (3) monitor that all Reports are reviewed and addressed.

b. Dover Corporate Law Department, including the General Counsel; VP & Associate Counsel, Labor & Employment; Assistant Counsel, Labor & Employment; Assistant Counsel, Litigation; and VP & Deputy General Counsel are responsible for all legal and legal-related matters. Accordingly, these roles have access to the centralized database and data relating to Reports to provide consultation and legal advice to those individuals investigating Reports and making decisions based on the outcome of Reports, as needed, to ensure that Reports are addressed.

c. Outside Counsel and Investigatory Resources, including designated and appropriately retained outside legal counsel and independent investigators, may be selected on a case-by-case basis to assist with investigating certain Reports. Accordingly, these individuals will be provided with access to data relating to Reports as needed to assist with investigations.

d. **Dover Corporate Senior Vice President, Human Resource,** is responsible for the executive leadership and direction of the Dover-wide Human Resources function. The Company's Hotline activity is an indicator of culture and employee concerns, accordingly, Dover Compliance provides this role with data from Reports. Accordingly, this role has access to data relating to Reports to provide consultation to those individuals investigating Reports and making decisions based on the outcome of Reports, as needed, to ensure that Reports are addressed.

e. **Dover Corporate Controller and Vice President, Internal Audit** are responsible for the oversight of all financial matters of the Company. Accordingly, if a Report contains financial concerns (e.g. fraud, intentional wrongdoing, or significant error relating to accounting, internal control over financial reporting, or auditing matters), Dover Compliance provides data from the Report to this role to ensure the Report is confidentially reviewed and addressed promptly, thoroughly, and without bias.

f. **Segment Chief Financial Officer** is responsible for the segment-wide financial matters of the Company. Accordingly, if a Report is within their area of responsibility and contains financial concerns, Dover Compliance provides data from the Report to this role to ensure the Report is reviewed and addressed promptly, thoroughly, and without bias.

g. **Segment Vice President Human Resources** are responsible for the segment-wide Human Resources function. The Company's Hotline activity is an indicator of culture and employee concerns, accordingly, Dover Compliance provides this role with data from Reports. Accordingly, these roles have access to data relating to Reports to provide consultation to those individuals investigating Reports and making decisions based on the outcome of Reports, as needed, to ensure that Reports are addressed.

h. **Local OpCo Human Resources Leadership**, including the OpCo Vice Presidents of Human Resources and their local Human Resources management and leadership teams, are responsible for the Human Resources function within their OpCo. Accordingly, if a Report is regarding their OpCo and area of responsibility, Dover Compliance provides this role with data from the Report to confidentially review and address promptly, thoroughly, and without bias.

i. **Local OpCo Business Leaders are** responsible for oversight of OpCo operations. Accordingly, if the Report is within their OpCo and area of responsibility, these roles may be provided with data from the Report to confidentially review and address the Report promptly, thoroughly, and without bias (i.e. financial reporting issues would be shared with local OpCo finance leaders).

j. **Dover Corporate Board of Directors,** for the benefit of all stakeholders, is responsible for the oversight of the Company, including ensuring adequate measures are in place to address ethical matters and concerns, including suspected violations of Company policies, financial reporting issues, or laws and regulations at the Company. Accordingly, these roles have access to a summary of Reports which includes data such as title, OpCo, and a description of the concern and outcome.

Some of the recipients noted above are located in the United States or otherwise outside of the European Economic Area ("**EEA**") and the UK, in countries which are not considered to provide an adequate level of data protection including, in the United States, India, China. As described in

Section 7 below, all such transfers to recipients will be compliant with all applicable laws and regulations.

The Company may engage third party vendors to assist in processing personal data from time to time. The Company will pass on to any such vendor its obligations under the applicable data privacy law, require that the vendor secure the data, and provide additional notice as required by law. We will not sell, distribute or lease your personal data to third parties unless we have your permission or are required by law to do so.

7. Where is the data being transferred? On what legal grounds?

For employees of EU/UK OpCos, your personal data will be transferred outside the EEA/UK for the purposes listed above pursuant to EU Standard Contractual Clauses, the EU-US Privacy Shield, or another legally binding and permissible arrangement. Such transfers will be compliant with all applicable laws and regulations. Specifically, we anticipate that for purposes of the Hotline, your data may be transferred to the following jurisdictions: any country where Dover and its operating companies perform business. Relevant additional details regarding the basis for transfers of your personal data can be provided upon request.

8. Data Security.

We are committed to ensuring that your personal data is secure. In order to prevent unauthorized or unlawful access to personal data or accidental loss, destruction, or damage to personal data, we have implemented and maintained reasonable, appropriate technical and organizational measures to safeguard and secure the personal data we process. The Company also maintains an inventory of personal data and evaluate the protections that we have in place for that data to ensure that our security measures are tailored to the sensitivity of the data.

For example, with regard to the Hotline, related data will be stored using secure servers, training will be provided to data recipients regarding proper and safe use, and outside vendors will be obligated to deploy appropriate data security measures. As described in Section 6 above, the Company has carefully limited access to your personal data only to those individuals who need access to it in order to fulfill their assigned roles, and only to the extent that they need such access.

9. Data Retention.

The Company strives to only store your personal data for as long as is necessary for the purpose for which we have processed it, and to dispose of it securely once that purpose has been fulfilled. How long we retain your personal data depends on the type of data and the purpose for which we process your personal data. In these efforts, the Company adheres to the Dover Records Management Policy when determining how long we retain personal data. The retention periods are established considering legitimate business purposes, according to the local regulations, and further details can be provided upon request.

10. Data Subject Rights.

Employee rights vary based on your local law. However, you can always ask the Company for more information about the people who will be able to see and access the personal data that relates to you. If you are aware of inaccurate data, it is your responsibility to request that such personal data to be updated and corrected.

If you are located within the jurisdiction of the GDPR, you also have the right (subject to certain limitations) to:

a. Request access to and rectification or erasure of your personal data.

b. Receive your personal data in a structured, commonly used, and machine-readable format, and request that Company transmits this to another controller.

c. Restrict the processing of your personal data or object to the processing of your personal data.

The Company is committed to ensuring your data is protected from misuse. If you think your data and information have been used in violation of the laws, regulations, or the applicable data protection provisions, please alert the Company and it will assist you.

Furthermore, you have the right to lodge a complaint with the supervisory authority, if you believe that your data have been processed unlawfully. Any requests, including those regarding the exercise of such rights, and questions can be directed to your local Human Resources representative or privacy@dovercorp.com. If you would like to contact the data protection officer for your company and need assistance locating the officer, you may contact privacy@dovercorp.com.

11. What company policies relate to my personal data?

We observe the requirements set out in Dover Corporation's Global Privacy Policy, Acceptable Use Policy, Data Security Incident Response Plan, Records Management Policy, and other related policies and standards. All of these policies are available for your review at www.integritycounts.com.