| | |
|---|---|
| IDEX CORPORATION | **POLICIES & PROCEDURES** |
| **Subject:**<br>**IDEX Data Protection Policy** | **Number:**<br>LGL-WW-50-150 |
| **Scope:**<br>All IDEX Business Units | **Initial Release:**<br>April 2020 |
| **Administration:**<br>This document is maintained and updated by the IDEX Corporate Compliance Department. Inquiries regarding interpretation of, or revisions to, the Policy should be made to the Chief Compliance Officer. | |

**POLICY CONTENTS:**



**POLICY:**

## 1.0 Applicability and Policy Definitions

"IDEX Corporation" refers to all IDEX's subsidiaries, affiliates and Business Units ("BU" or "BUs") around the world (collectively, "the Company" or "IDEX"). Local laws governing data protection may vary depending on country; should there be a conflict between this Policy and local law, then local law applies.

The IDEX Data Protection Policy ("the Policy") refers to the Company's commitment to treat information of employees, customers, and other interested parties with the utmost care and confidentiality. Although this Policy is intended to address general data privacy and data protection laws around the world, it most specifically addresses obligations set forth under the General Data Protection Regulation ("GDPR") (EU 2016/679).

The Policy specifically applies when IDEX processes personal data: (i) at an IDEX BU within the European Union ("EU") and/or the European Economic Area ("EEA") **and/or** (ii) at an IDEX BU *outside* the EU or EEA where such processing is connected to the business of an IDEX BU *within* the EU and/or EEA. This Policy also applies when the personal data processed is related to data subjects who are residents within the EU and/or EEA **and** where the processing activities are related to ***either***: (a) the offering of goods or

services to such data subjects; ***or*** (b) the monitoring of behaviour that takes place within the EU and/or EEA.

Below are definitions under privacy laws, most specifically as defined under the GDPR:

| Term | Definition |
|---|---|
| Anonymize | Anonymizing is the changing of Personal Data in such a way that the individual details about personal or factual circumstances can no longer be assigned to an identified or identifiable person or only with a disproportionately high expenditure of time, costs and manpower. |
| Consent | Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he/she, by a statement or by a clear affirmative action, signifies agreement to the specific processing of his/her Personal Data. It has to be a clear affirmative act ("Opt-In"). Silence or inactivity are not sufficient. Consent may be withdrawn at any time with effect for the future. |
| Data Breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. |
| Data Controller | The natural or legal person, public authority, agency or other body which alone, or jointly with others, determines the purposes and means of the Data Processing. |
| Data Processing | Any operation, or set of operations, which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |
| Data Processor | A natural or legal person, public authority, agency or other body, which processes Personal Data on behalf of the Data Controller (Article 28 GDPR). |
| Data Protection Impact Assessment ("DPIA") | A risk assessment for a data processing activity (Article 35 GDPR) *only* for certain high-risk processing activities. This may include a description of: (a) the envisaged processing operation along with the purpose of the processing; (b) the legitimate interest pursued by the controller; (c) an assessment of the necessity and proportionality; (d) an assessment of risks to the rights and freedoms of Data Subjects; and (e) the measures envisaged to address the risks to ensure the protection of Personal Data and to demonstrate compliance with GDPR. |
| Data Protection Procedures | Any IDEX or local BU internal policies/procedures supplementing this Policy. |
| Data Protection Law | All applicable state, local and federal/national laws related to data protection including, but not limited to, GDPR. |
| Data Subject | Any person to whom the respective Personal Data refers. |
| Joint Controller | Two or more Data Controllers who determine the purposes and means of the Data Processing (Article 26 GDPR). |
| Personal Data | Any information relating to an identified or identifiable natural person (Article 4 GDPR) or as further described in Section 3 of this Policy. |
| Records of Processing Activities ("ROPA") | A document required by Article 30 GDPR with inventory and analysis purposes, which must reflect data processing tools and procedures and which precisely |

| | |
|---|---|
| | identifies: (a) the actors involved (Controller, Processors, representative, Joint Controller, etc.) in the Data Processing; (b) the categories of data processed; (c) the purpose of the processing; (d) who has access to and who are the recipients of the Personal Data; (e) how long the Personal Data is retained; and (f) the technical and organizational security measures implemented. |
| Responsible Person | The person responsible for the compliance of a particular processing activity with Data Protection Law as determined by the Data Protection Procedures. |
| Sensitive Data | Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union memberships, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (Article 9 GDPR). |
| Supervisory Authority | An independent public authority, which is established by a European Union Member State (Article 51 GDPR) or any other public authority which is responsible for monitoring the application of Data Protection Law. |
| Third Party/Parties | Any legal entity (whether an IDEX BU or not) that is different from the party processing the Personal Data as further described in Section 8 of this Policy. |

## 2.0 General Rules of Data Protection

This Policy represents a component of a comprehensive data protection compliance strategy and establishes a framework for the lawful handling of Personal Data. The Policy is designed to ensure that all processing of Personal Data at IDEX is in compliance with any relevant Data Protection Law.

The general rules for data protection for employees to follow are:

- Data protection concerns every IDEX employee.
- Data Protection Law applies to all Personal Data, including Sensitive Personal Data, concerning natural persons, whether employees, applicants, business partners, website users, etc.
- Any use of the Personal Data without statutory permission or Consent of the Data Subject and for the specific predetermined purpose for which it was required is prohibited.
- Use caution with regard to Sensitive Data as it may only be processed under limited conditions.
- New or modified Data Processing activities must be consistent with Data Protection Law and be included in the ROPAs.
- The Global Privacy and Data Protection Team (as defined below) must be notified immediately of any potential or actual Data Breach.
- Exercise caution in data exchanges with third parties as tests and/or documentation may be necessary and special contracts/addendums to existing contracts will likely need to be put in place.

A negligent or deliberate violation of this Policy or Data Protection Law may result in discipline, up to and including termination of employment, with or without notice. In addition, employees may be personally liable under local laws, civil, criminal or Data Protection Law for damages to Data Subjects.

## 3.0 Scope and Implications of this Policy

### *Relevant Data*

This Policy applies solely to the handling of Personal Data. Information constitutes Personal Data only if it can be assigned to a person *(e.g., the e-mail address "pparker@idexcorp.com").* However, it is also considered Personal Data if the respective data can be linked to a person by indirect identifiers, including a telephone number, an address, or a personnel number *(e.g., the information that five employees with the personnel numbers 9375, 9376, 9377, 9378 and 9379 were involved in workplace accidents is Personal Data because the Company can easily identify the employees).*

In comparison, information or data which has been Anonymized is no longer subject to Data Protection Law and, therefore, this Policy does *not* apply *(e.g., if the personnel numbers are deleted in the previous example, the remaining information that five employees were involved in an accident cannot be linked to an identifiable person anymore).*

This Policy does *not* relate to information about companies or entities generally. For example, IDEX may possess or receive certain information from or about other companies that may be considered confidential information. While this Policy does not apply to those situations, our Code of Business Conduct and Ethics may apply regarding the handling of confidential or sensitive business information.

### *Publication of this Data Protection Policy and Updates*

This Policy should be made available to all employees, including new employees upon hire. This Policy will be reviewed regularly by the Corporate Compliance Department and employees will be informed in a timely and appropriate manner of any substantive changes.

## 4.0 Data Protection Concerns Everyone

### *Employees Must Observe Data Protection*

All employees who have access to Personal Data may only process Personal Data as authorized and in accordance with the instructions of the respective Responsible Person. All areas must comply with Data Protection Law; however, in particular, employees in Marketing, Human Resources (HR), and Information Technology (IT) should be especially aware of data protection requirements as they more regularly handle Personal Data and Sensitive Data.

### *Privacy and Data Protection Governance Structure*

IDEX maintains a governance program led by the Global Privacy and Data Protection Team comprised of members of multiple corporate functions. Each IDEX BU located in the EU and/or EEA has a named local Privacy Lead, who is an extension of the Team. Additionally, certain BUs have appointed Data Protection Officers, as is required by certain local law. Their roles are described in more detail below.

| Role | Description |
|---|---|
| Global Privacy and Data Protection Team ("Team") | The Team that directs activities relating to data protection broadly, not only those related to the GDPR. The Team is responsible for ensuring overall GDPR compliance at an enterprise-wide level and will work with the local Privacy Leads regarding key activities related to privacy governance and program management, policies and procedures, privacy regulatory compliance, business enablement, privacy breach and incident response, and communication and training. The Team can be contacted directly or also via a dedicated email address at: LFOPrivacy@idexcorp.com.<br><br>Additionally, the Team acts as the point of contact for regulators during inquiries and general communications. By contrast, the local Privacy Leads remain the first point of contact for local employees, except in matters of urgency or great importance. |
| Privacy Lead | Personnel situated locally at each IDEX BU, whose responsibilities include supporting data protection initiatives in their respective local BUs. The Privacy Leads are the local coordinators for all data protection matters and also serve as the point of contact for the Team. They also manage all data protection documents for an IDEX BU, e.g., policies, procedures, templates and data protection statements. |
| Data Protection Officer ("DPO") | Only certain IDEX BUs (only if required by law) will appoint a Data Protection Officer in accordance with Article 37 GDPR and/or national Data Protection Law. His/her tasks will include at a minimum to inform and advise on and monitor compliance with Data Protection Law and internal policies and procedures on data protection. Before any BU appoints a DPO, please contact the Team. |

***Notification of Privacy and Data Protection Issues***

Questions regarding this Policy, or the correct handling of Personal Data in general, should be communicated to the local Privacy Lead and/or the Team. If employees have questions regarding compliance with relevant Data Protection Law during the execution of their duties, they should consult with the Responsible Person for the individual Data Processing, the BU Privacy Lead and/or the Team. In addition, employees should also immediately report any actual or suspected violations of this Policy or Data Protection Law to the Responsible Person for the specific Data Processing, the BU Privacy Lead and/or the Team.

## 5.0 Principles Relating to the Processing of Personal Data

Below are the general guidelines relating to Data Processing for which IDEX and the BUs are individually responsible.

***The Processing of Personal Data is Prohibited Unless it is Exceptionally Permitted***

The processing of Personal Data is lawful only if an explicit legal basis applies. Such legal basis can either be: (i) a statutory permission to process the data; or (ii) Consent by the Data Subject. The accepted statutory permissions are:

**Performance of or taking steps to enter a contract**: When the Data Processing is necessary to fulfill a contract with the Data Subject or a contract requested by the Data Subject *(e.g., the Human Resources Department collects bank details of employees for salary payment).*

**Compliance with legal obligations**: When a certain Data Processing is requested by law *(e.g.,* a *court orders the release of certain information for legal proceedings).*

**Legitimate interest**: When the Data Processing is in the legitimate interest of IDEX or a third party and the interests and rights of the Data Subject do not take precedence*.*

If there is no statutory permission for Data Processing, then **Consent** must be obtained from the Data Subject. The law places high demands on the effectiveness of such Consent; it must be declared freely, for the specific case, in an informed manner and unequivocally (*e.g., a business contact agrees to the subscription of a newsletter by clicking "subscribe now")*. Consents may be withdrawn at any time by the Data Subject with effect for the future. The Responsible Persons must ensure the Consents used meet the applicable legal requirements.

Consent is specifically required for the processing of **Sensitive Data** *(e.g., employees agree to the statistical use of Sensitive Data like their ethnicity, religious beliefs or sexual orientation by signing a Consent form explaining the planned Data Processing).* Only in exceptional cases do statutory provisions allow the Sensitive Data to be processed without Consent.

***Principles of Purpose Limitation, Data Minimization and Storage Limitation***

Personal Data must be processed for a specific purpose. Before any Data Processing occurs, it must be determined, whether and to what extent, the Data Processing is necessary in order to achieve the purpose for which it is undertaken *(e.g., if a special contact form is used for job applicants, the hiring company will require the applicant to provide certain data needed to process and/or respond to the job application, such as e-mail address, telephone number or postal address).*

If such purpose is changed, special legal requirements apply, meaning that the Data Subject must consent or Data Protection Law must allow such change of purpose *(e.g., business contact sends an e-mail regarding certain product information; the e-mail address is collected to respond and take steps to enter into a contract - the e-mail address may not be used for other non-related purposes, such as a marketing newsletter).*

In addition, Personal Data shall be deleted, once it is no longer necessary for the purpose for which it was collected, unless otherwise required by law. The Responsible Person for that particular data procedure is responsible for deleting the data. If Personal Data is stored with external Data Processors, IDEX must take steps to ensure that data is also irrevocably deleted (in partnership with local IT).

***Principle of Transparency***

Data Subjects must be informed about how their Personal Data is being handled. Article 13 GDPR requires every Data Controller provide specific information to the Data Subjects. Every Responsible Person ensures that Data Subjects are informed adequately and in a timely manner (usually at the time when the Personal Data is collected).

*As an example, a user visits the IDEX website. The Website Data Protection Statement must be made available to the user by inserting a direct link on the homepage. This Data Protection Statement must*

*inform the website user about the specific Data Processing, about the identity of the Data Controller, the data categories, the purpose(s) of Data Processing and about to whom the Personal Data might be transmitted.*

***Principle of Factual Accuracy and Currency***

The Responsible Person for the Data Processing has to take all adequate steps to remove, supplement or update Personal Data that is inaccurate or incomplete. The Data Subject has the right to request erroneous data about him/her be deleted or rectified in a short timeframe *(e.g., an employee gets married and changes his or her last name, he/she has the right to request the employer change the last name in the Company database).*

***Principle of Data Integrity, Confidentiality and Accountability***

The security of all data must be properly maintained at all times. Personal Data must be kept safe and protected against unauthorized or unlawful processing and against accidental loss, destruction or damage. Technical and organizational measures must be taken to ensure a level of protection appropriate to the risk of processing. Such measures often include measures of access control, i.e., to the data processing equipment itself and access controls in databases and measures of availability control, *(e.g., backup strategy (online/offline; on-site/off-site))*.

## 6.0 Specific Required Data Protection Measures and Processes

The following data protection measures and processes are required. However, this Policy also may be supplemented by more specific local BU Data Protection Procedures. In case of inconsistencies between this IDEX Data Protection Policy and any local policies and procedures, this Policy prevails.

***Data Protection By Design and By Default***

Data protection principles (as stated in Section 5.0) are required to be implemented by the appropriate technical and organizational measures into all processing of Personal Data. And, when introducing new procedures for processing Personal Data, the Responsible Person must ensure this procedure is permissible under Data Protection Law. The review should take place as early as possible, and before the respective Processing of Personal Data starts. The legal basis must be documented and retained with local BU program documents, if applicable. The type and scope of these measures depend on the: (i) state of the technology; (ii) implementation costs; (iii) type, scope, circumstances and purposes of Data Processing; and (iv) probability of occurrence and severity of the risk for the rights and freedoms of natural persons.

As an example, data protection-friendly technologies (*e.g., designing a customer contact form)* and data protection-friendly pre-settings (*e.g., a new Customer Relationship System is set up and IT ensures that the checkbox for receiving the newsletter is not pre-selected*) shall be implemented from the design phase, when processing Personal Data.

***Record of Processing Activities***

IDEX must document and retain a ROPA relating to Personal Data in accordance with Article 30 GDPR. Such record is the central tool to the management of data processing activities. Every data processing activity in which Personal Data is processed must be listed in the ROPA and ensure all information is

correct and complete before implementing the new processing activity. The same applies if a data processing activity is changed as new data categories are processed or new software is used.

***Data Protection Impact Assessment***

If a planned Data Processing is likely to entail a high risk to the freedoms or rights of the Data Subjects, the Responsible Person in each case shall contact the Privacy Lead and the Team to determine whether a DPIA is necessary before the Data Processing is put into operation (Article 35 GDPR). A high risk to the freedoms or rights of a Data Subject exists when Sensitive Data is processed on a large scale, publicly accessible areas are monitored on a large scale and/or when personal aspects of people are systematically and extensively evaluated with a significant effect on the Data Subject.

## 7.0 Violations of the Protection of Personal Data

A Data Breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. Data Breaches may, in particular, include:

- improper transmission of Personal Data to third parties *(e.g., e-mails containing Personal Data were sent to the wrong recipients);*
- improper access by third parties to Personal Data *(e.g., access controls in the HR-systems failed and employees had access to personnel files); and/or*
- loss of Personal Data *(e.g., notebooks or a storage device were lost).*

If a Data Breach has occurred or is suspected, the Team must be informed immediately. Communication with the parties concerned or the Supervisory Authority will be done as a joint effort between the Team and the local IDEX BU. Under certain circumstances, the Data Breach may have to be reported to the Supervisory Authority without undue delay, and not later than **72 hours** (including weekends and holidays). The Team shall be contacted **before** any contact is made with the Supervisory Authority. In addition, when the Personal Data breach is likely to result in a high risk to natural persons, the Data Subjects are also to be informed. The Team and the BU will partner to determine whether this is the case.

## 8.0 Cooperation with Third Parties

***General Guidance***

IDEX Corporation, or an IDEX BU, may choose, or may be contractually required, to provide Personal Data to Third Parties. In this case, legal requirements apply to the lawfulness of the Data Processing. They apply even if only the possibility exists that a Third Party may access the Personal Data. Importantly, such legal requirements include special data protection contracts, as well as certain technical and organizational measures, to document the Third Party's compliance with Data Protection Law.

In principle, the GDPR establishes three types of contractual relationships:

**Data Processing:** When a Third-Party processes Personal Data on behalf of the Data Controller (i.e., only following the Data Controller's instruction), such entity is a Data Processor. If IDEX Corporation itself or an IDEX BU is the Data Controller, it is responsible for the Personal Data. However, a contract, or an addendum to an existing contract, fulfilling the requirements set out in Article 28 GDPR must be put in place.

**Controller-to-Controller Transfer**: Personal Data could be transferred to a Third Party who shall independently process such Personal Data (for purposes determined by the latter entity). In this case, the Third Party itself becomes the Data Controller and, thus, responsible for the Data Processing. In such a case, the transfer of data must be allowed under Data Protection Law either by Consent or a statutory permission.

**Joint Controllership**: A Third Party and IDEX Corporation or an IDEX BU may jointly determine the purposes and means of Data Processing. In this case, IDEX Corporation or the IDEX BU and the Third Party are **Joint Controllers.** Also, in this case, a special data protection contract fulfilling the requirements of Article 26 GDPR is required.

***Transfer of Data from the EU/EEA to Third Countries***

Additional restrictions exist for data transfers out of the EU and/or EEA to recipients in third countries. In the event that Personal Data is planned to be transferred to such a third country (whether to a Data Processor, another Data Controller or a Joint Controller), the Responsible Person must ensure the appropriate contractual terms are in place.

IDEX Corporation, or the IDEX BU, must ensure that the recipient of the Personal Data outside the EU and/or the EEA has an adequate level of data protection within the meaning of Article 45 GDPR or that there are suitable guarantees within the meaning of Article 46 GDPR.

## 9.0 Data Subjects' Rights

Data Subjects have the right to request information about how the Company handles their personal information. Privacy Leads and employees are required to report requests by Data Subjects to the Team immediately. The Team will work with the local IDEX BU for handling and appropriate responses.

In addition, Data Subjects have various legal rights with regard to the data stored concerning them:

**Right of Access:** Every Data Subject has the right to receive information regarding the data stored about him/her; the information shall be complete as specified by Article 14 GDPR and in a form and language comprehensible to the person concerned.

**Right to Rectification and Erasure:** Personal Data must be factually correct and incorrect data must be rectified at the request of the Data Subject; irrespective of this, Personal Data are to be regularly checked for their correctness and necessity and deleted if the data are no longer required to fulfil the purpose pursued in each case.

**Right to Restriction of Processing:** In certain cases, Data Subjects have the right to obtain a restriction on the Data Processing of their Personal Data; the data concerned shall be blocked for further Data Processing.

**Right to Data :** The Data Subject has the right to receive the Personal Data concerning him/her in a structured, current and machine-readable format or to be transferred to another location directly.

**Right to Object:** In certain circumstances, the Data Subject may have a right to object to the processing of his/her Personal Data (Article 21 GDPR) – in this case, the Data Processing may not be continued.

## 10. Amendment History

| CP | Rev. | Date | Description of Change | Originator | Approved By |
|---|---|---|---|---|---|
| LGL-WW-50-150 | 0 | April 2020 | Initial Release | T. Gainer, Senior Compliance Counsel | A. Roche, Chief Compliance Officer / R. Sharma, Vice President, Information Security |