Data Protection Policy

Linde Material Handling (Ireland) Ltd is committed to comply the General Data Protection Regulation (GDPR). The GDPR applies to all organisations that process data relating to their employees, as well as to others including customers, contractors and clients. It sets out principles which should be followed by those who process data; it gives new and extended rights to those whose data is being processed.

To this end, the organisation endorses fully and adheres to the six principles of data protection, as set out in Article 5 of the GDPR.

1. Data must be processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. Data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. Data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

These principles must be followed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, the organisation will:

- observe fully the conditions regarding the fair collection and use of information including the giving of consent
- meet its legal obligations to specify the purposes for which information is used
- collect and process appropriate information only to the extent that it is needed to fulfil our operational needs or to comply with any legal requirements
- ensure the quality of information used
- ensure that the information is held for no longer than is necessary
- ensure that the rights of people about whom information is held can be fully exercised under the GDPR (ie the right to be informed that processing is being undertaken, to

access one’s personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as incorrect)

- take appropriate technical and organisational security measures to safeguard personal information
- publicise and abide by individuals' right to appeal or complain to the supervisory authority (Office of the Data Protection Commission (DPC)) in the event that agreement cannot be reached in a dispute regarding data protection
- ensure that personal information is not transferred abroad without suitable safeguards.

Status of this Policy

The Policy does not form part of the formal contract of employment for our employees, but it is a condition of employment that they will abide by the rules and policies made by the company from time to time. Any failure to follow the Data Protection Policy may lead, therefore, to disciplinary proceedings. This Policy was approved as per implementation signature section. It will be reviewed at least every 2 years. This policy replaces all previous Data Protection policies of the organization.

Designated Data Protection Officer and Data Coordinators

The Data Protection Officer for LMHI is the Financial Controller. The Designated Data Coordinator is the Financial Accountant.

The above mentioned will deal with day-to-day matters. Any member of staff, or other individual who considers that the policy has not been followed in respect of personal data about himself or herself should raise the matter with one of the above-named persons.

Staff Responsibilities

All staff are responsible for:

- checking that any information that they provide to the organisation in connection with their employment is accurate and up to date
- informing the organisation of any changes to information that they have provided, e.g. changes of address, either at the time of appointment or subsequently. The organisation cannot be held responsible for any errors unless the employee has informed it of such changes.

Data Security

All staff are responsible for ensuring that:

- any personal data that they hold is kept securely
- personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter and may, in some cases, be considered gross misconduct. Personal information should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly

backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Disaster Recovery

1. All data that is in My Company Data folder on laptops & desktops is backed up daily offsite to a Cloud hosted in a KION-Group contracted data centre within the EU.

2. All data on the Network drives is backed up every day and is replicated to an offsite server in the KION-Group contracted Data Centre in Germany. A log of backups is kept for auditing purposes.

3. Backups are verified regularly by KION Group IT.

4. Firewalls and anti-virus software are kept up to date and running, and employees are educated constantly in dealing with Phishing, spam mails.

5. All data traffic over company networks are encrypted and secure.

6. Computers are protected from physical harm, theft or damage, and from electrical surges using protective plugs.

7. The organization has sufficient plans for how to deal with loss of electricity, external data links, server failure, and network problems.

Subject Consent

The GDPR sets a high standard for consent and requires a positive opt-in. Neither pre-ticked boxes nor any other method of default consent are allowed. As required by the GDPR, the organisation takes a "granular" approach i.e. it asks for separate consent for separate items and will not use vague or blanket requests for consent. As well as keeping evidence of any consent, the organisation ensures that people can easily withdraw consent (and tells them how this can be done).

It should be noted, however, that consent is only one of the lawful bases on which data processing depends. In brief, the others include the following.

- Contract: if processing someone’s personal data is necessary to fulfil the organisation's contractual obligations to them (eg to provide a quote).

- Legal obligation: if processing personal data is necessary to comply with a common law or statutory obligation.

- Vital interests: not one that will occur often as it refers to processing personal data to protect someone’s life (and even then, it cannot be relied on with regard to health data or other special category data if the individual is capable of giving consent.

- Legitimate interests: the most flexible lawful basis for processing and one which applies when data is used in ways people would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

Note that the GDPR provides for special protection for children’s personal data and the organisation will comply with the requirement to obtain parental or guardian consent for any data processing activity involving anyone under the age of 16.

Subject Access

An employee may request details of personal information which the organisation holds about him or her under the GDPR. A small fee may be payable and will be based on the administrative cost of providing the information if persistent or vexatious requests are made. If an employee would like a copy of the information held on him or her, they should write to accounts@linde-mh.ie. The requested information will be provided within one month. If there is any reason for delay, that will be communicated within the four-week time period. A request which is manifestly unfounded or excessive may be refused. The person concerned will then be informed of their right to contest this decision with the supervisory authority (the ICO).

If an employee believes that any information held on him or her is incorrect or incomplete, then they should email to accounts@linde-mh.ie as soon as possible. The organisation will promptly correct any information found to be incorrect.

Data breaches

The loss, misuse or unlawful disclosure of personal information can bring harm and distress to the individuals concerned, as well as the possibility of significant damage to the Company's reputation. A breach of the Act is likely to be regarded as gross misconduct. It is also a criminal offence to knowingly or recklessly obtain, disclose or procure the disclosure of personal data unlawfully, as is selling, or offering to sell, personal information which has been unlawfully obtained.

A data breach can happen for a number of reasons, including:

- loss or theft of data or equipment on which data is stored;
- inappropriate access controls allowing unauthorised use;
- equipment failure;
- human error;
- unforeseen circumstances such as fire or flood;
- cyber-attack (Hacking); or
- "blagging" offences where information is obtained by deceiving the Company.

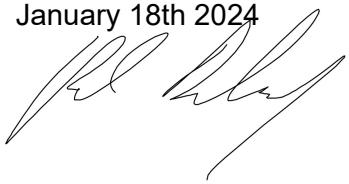
All breaches must be reported to the Data Coordinators or the Data Protection Officer of Linde Material Handling (Ireland) Ltd. as soon as an incident has been identified. Timelines of reporting is key to ensuring that the Company can put in place the necessary measures to contain the damage and begin the recovery process.

Conclusion

This policy sets out this organisation's commitment to protecting personal data and how that commitment is implemented in respect of the collection and use of personal data.

Signed: **Paul Delaney, QHSE Manager**

Date: January 18th 2024



Appendix 1

Definitions

The Data Protection Act 2018 applies, subject to certain exemptions, to the *processing* of *data* that are deemed to be *personal data.* The 2018 Act uses these terms to determine **who** and **what** fall within its provisions.

Data

This means information which is processed or is intended to be processed by means of automatic devices such as IT systems or as hard copy data.

Data Controller

This means the person(s) who determine(s) the purposes and manner in which any personal data are, or are to be, processed. ‘Person’ in this sense means legal person and so, as well as individuals, includes organisations such as companies.

'LMH IRL Ltd' therefore is a data controller.

Data Processor

This means any person (other than an employee) who processes data on the Company’s behalf (e.g. the Company pension provider). The Act imposes a higher duty of care upon data controllers when the processing of personal data is carried out on their behalf by data processors.

Data Subject

This means an individual who is the subject of the personal data.

Personal Data

This means data from which it is possible to identify a living individual, either directly from that information or from additional information which is in the possession of anyone processing that data. Both factual information and expressions of opinion (e.g. references) about the individual are relevant. Personal data includes original or copies of paper documents or correspondence, photographs, video or audio recordings.

With regard to employment, personal data will be that relating to current and former employees, job applicants, agency, casual and contract workers, volunteers, apprentices and students.

Processing

This term has very wide scope and covers almost any conceivable use of data, including obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, using, disclosing, blocking, erasing or destroying the information or data. This means, for example, that simply having data in one's possession or reading it on a webpage constitutes processing for the purposes of the Act.

Sensitive personal data

This means personal data consisting of information as to a person's racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life or the commission or alleged commission of any offence (or proceedings for those offences) by that person or details used to comply with any Irish or European legislation .

Subject access

This means the right of any individual to have access to personal information about themselves held by a data controller.

Third party data

This term is used in relation to data subject access requests and refers to data that identifies another party. For example, an employee is unable to view or have a copy of references we receive in the course of recruitment, as these are directly attributable.

Appendix 2

Data Protection Breach Handling Process