LEITHS
Built on Quality

GENERAL DATA PROTECTION REGULATION- GDPR

SCOPE OF POLICY

Leiths (Scotland) Limited is fully committed to compliance with the requirements of the General Data Protection Regulation (GDPR) and all other data protection legislation currently in force. The Regulation applies to anyone processing personal data and sets out principles which should be followed and gives rights to those whose data is being processed.
To this end, Leiths endorses fully and adheres to the Data Protection Principles as in the guidelines listed below.

GUIDELINES

When processing data we will ensure that it is:

- processed lawfully, fairly and in a transparent way ('lawfulness, fairness and transparency')
- processed no further than the legitimate purposes for which that data was collected ('purpose limitation')
- limited to what is necessary in relation to the purpose ('data minimisation')
- accurate and kept up to date ('accuracy')
- kept in a form which permits identification of the data subject for no longer than is necessary ('storage limitation')
- processed in a manner that ensures security of that personal data ('integrity and confidentiality')
- processed by a controller who can demonstrate compliance with the principles ('accountability')

These rights must be observed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, Leiths will:

- observe fully the conditions regarding having a lawful basis to process personal information
- 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 necessary to fulfil operational needs or to comply with any legal requirements
- ensure the information held is accurate and up to date
- 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 (i.e. the right to be informed that processing is being undertaken, to access personal information on request; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as wrong information)
- take appropriate technical and organisational security measures to safeguard personal information
- ensure that personal information is not transferred outside the EU, to other countries or international organisations without an adequate level of protection.

EMPLOYEES PERSONAL INFORMATION

Throughout employment and for as long as is necessary after the termination of employment, Leiths will need to process data about you. The kind of data that Leiths will process includes:

- any references obtained during recruitment details of terms of employment
- payroll details
- tax and national insurance information
- details of job duties
- details of health and sickness absence records
- details of holiday records
- information about performance
- details of any disciplinary and grievance investigations and proceedings
- training records
- contact names and addresses
- correspondence with Leiths and other information that you have given Leiths

Leiths believes that those records used are consistent with the employment relationship between Leiths and yourself and with the data protection principles. The data Leiths holds will be for management and administrative use only but Leiths may, from time to time, need to disclose some data it holds about you to relevant third parties (e.g. where legally obliged to do so by HM Revenue & Customs, where requested to do so by yourself for the purpose of giving a reference or in relation to maintenance support and/or the hosting of data in relation to the provision of insurance).

In some cases, Leiths may hold sensitive data, which is defined by the legislation as special categories of personal data, about you. For example, this could be information about health, racial or ethnic origin, criminal convictions or religious beliefs. This information may be processed not only to meet Leiths legal responsibilities but, for example, for purposes of personnel management and administration, suitability for employment, and to comply with equal opportunity legislation. Since this information is considered sensitive, the processing of which may cause concern or distress, you will be asked to give express consent for this information to be processed, unless Leiths has a specific legal requirement to process such data.

ACCESS TO DATA

You may, within a period of one month of a written request, inspect and/or have a copy, subject to the requirements of the legislation, of information in your own personnel file and/or other specified personal data and, if necessary, require corrections should such records be faulty. If you wish to do so you must make a written request to the HR Department. Leiths is entitled to change the above provisions at any time at its discretion.

DATA DISCLOSURES

Leiths may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- any employee benefits operated by third parties
- disabled individuals - whether any reasonable adjustments are required to assist them at work
- individuals' health data - to comply with health and safety or occupational health obligations towards the employee
- for Statutory Sick Pay purposes
- HR management and administration - to consider how an individual's health affects his or her ability to do their job
- the smooth operation of any employee insurance policies or pension plans.

These kinds of disclosures will only be made when strictly necessary for the purpose.

DATA SECURITY

You are responsible for ensuring that any personal data that you hold and/or process as part of your job role is stored securely.
You must ensure that 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.
You should note that unauthorised disclosure may result in action under the disciplinary procedure, which may include dismissal for gross misconduct. Personal information should be kept in a locked filing cabinet, drawer, or safe. Electronic data should be password protected 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.
When travelling with a device containing personal data, you must ensure both the device and data is password protected. The device should be kept secure and where possible it should be locked away out of sight i.e. in the boot of a car. You should avoid travelling with hard copies of personal data where there is secure electronic storage available. When it is essential to travel with hard copies of personal data this should be kept securely in a bag and where possible locked away out of sight i.e. in the boot of a car.

BREACH NOTIFICATION

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of Leiths becoming aware of it and may be reported in more than one instalment.
Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual.
If the breach is sufficient to warrant notification to the public, Leiths will do so without undue delay.

TRAINING

New employees must read and understand the policies on data protection as part of their induction.
All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.
The nominated data protection officer for Leiths is trained appropriately in their role under the GDPR.
All employees who need to use the computer systems are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and Leiths of any potential lapses and breaches of Leiths policies and procedures.

DATA PROTECTION OFFICER

Data Protection Officer: James Bell – Group Finance Director.
Head Office, Rigifa, Cove. AB12 3LR