Heronstone Engineering LTD

T/A Harlech Tools

GDPR & Privacy Policy

GDPR Background Information and Description

The General Data Protection Regulation (25th May 2018)

The GDPR's focus is the protection of personal data, Individuals must be informed that they have the following (non-exhaustive) rights:

- To complain to supervisory authorities. (ICO in the UK)
- To withdraw their consent to processing of their personal data.
- To access their personal data and have it rectified or erased. (The right to be forgotten)
- To be informed of the existence of any automated personal data processing.
- To object to certain types of processing.
- To be told how long their personal data will be held for.
- To be provided with details of any appointed data protection officer.

Where consent from the individual is required, consent must be given by affirmative action, i.e. a signed statement from the individual specifying what data has been collected and what it is to be used for. This means that separate consents are required for different data processing operations.

Finally, it must be easy for an individual to withdraw their consent at any time. Previous consents should be revisited to make sure they comply with the new regulations.

Scope of GDPR

Heronstone provides secure system of storage for each employee and customer data through the SAGE system, secure computer and server systems with power supply back up as to not lose or corrupt data in the event of a power failure. The server is backed up nightly and monitored by our IT providers to ensure that we can recover data in the event of a system failure or cyber-attack. User accounts are Password protected and passwords should not be shared/disclosed to other users. The ICT system is further protected by antivirus and group policy enforcement to prevent the running of unauthorized software . The establishment, maintenance and continuous improvement of a safe working system to handle Employee and customer data from being collected to being stored and to provide easy, hassle free communication regarding the relevant data held by Heronstone. Tailored consent forms are produced to suit the needs and inform the recipient of what information is collected and used for. Risk assessments carried out prior to the collection and storage of data in the form of a Data Documentation Controller.

Collection of data

Each category of data that Heronstone holds or collects must be entered into the Data Controller Document. The Document identifies processing activities which require a risk assessment, If the Document cannot be filled in fully then the data cannot be collected or processed.

- The Data Controller Document must be filled in fully.
- Based on the Data Controller Document the data might (such as requirement for contract) may not need consent but classified as a legitimate interest. Some data is required by law.
- There must be a lawful basis for collection of the data.
- There must be secure storage (locked under 2 keys / stored on protected computer system).
- If required, consent must be given freely and without detriment.

What data is collected

The data Heronstone collects is as follows:

- Company and personal contact details, this can include but is not limited to, Email, Address, Name and phone number.
- Bank, pension and tax details, for payment purposes and to be able to fulfil contract terms with employees.
- Inhouse and external training is recorded for the purposes of ISO standard and Health and Safety.
- Health surveillance is undertaken for the improvement of working conditions within the company.
- Emergency contact details are recorded.
- Annual leave details and sick leave details are recorded.
- CCTV for the detection and investigation of criminal activity and safe working practices.

Use of collected data

Each regular processing activity must be input into the Data Controller Document, This Document specifies the use of the data. Personal Data cannot be used for a different purpose other than stated in the Controller Document.

- Heronstone does not undertake marketing campaigns.
- Contact details are required for the ease of communication, Fulfilment of contract terms and information transfer about jobs and tasks the company undertakes.
- Bank, Pension, Sick leave and tax details are required by law, (HMRC and Payee)
- Bank / payment details are used to pay companies.
- Annual leave details are recorded for contract purposes.

Storage of collected data

The majority of personal and company data is stored electronically. Although Heronstone still utilizes paper-based storage systems.

The electronically stored data is protected by multiple steps:

- A group user policy, restricting the running of programs on individual computers.
- Antivirus systems protecting the central server and individual computers.
- Password protected user accounts.
- Administrator locks on changes to programs.
- Daily backups of data carried out automatically.
- SAGE with restricted user accounts to handle vast majority of data.
- ITCS as IT support specialist (GDPR Compliant)
- SAGE Support (GDPR Compliant)

The paper-based system is as follows:

- Paper-based data is stored within offices.
- The “2 Key“ System putting two locks between data and accessing it.
- Filling systems are in place to easily find stored data.
- Restricted access to offices with personal information.

Who the data is shared with

Heronstone does not sell or send data to a 3rd party.

- Heronstone does not sell any data.
- Heronstone only shares data if required by law. (HMRC, HSE etc)
- Heronstone enlists the help of 3rd parties to protect data but does not give access to it.
- Heronstone needs a written request or consent from the owner of the data to share it with a 3rd party.

Your rights regarding your data

Your rights are outlined by GDPR and covered in the background information, although some data is required to be kept by Heronstone so that we can comply with current legislation.

If you would like to request what information Heronstone holds on you, or have any other questions, please contact us at: info@harlech-tools.co.uk

Rectification and Erasure Policy

Information and Description

The data subject has the right to request all information held by the company for viewing. They also have the right to have information corrected or erased in certain circumstances.

Requests for any of the above actions much be made via email to the address Info@harlech-tools.co.uk

Once a request has been received it must be checked for validity, I.E. an employee cannot request the information held about the company they work for unless accompanied by consent from the company's data controller or director.

Once validated, data must be shared within 1 month of request. Heronstone must inquire how they want to receive the data I.E. Via email, Post or a visit to the site.

Extreme caution must be taken when providing information from a subject access request that you do not inadvertently breach another data subjects rights when providing the information.

Rectification

If information is to be rectified Heronstone must receive all new / rectified data from the data subject with valid consent from the data controller or director of the data subjects company.

With valid consent Heronstone can rectify the data within the company's systems and send a completion notification to the data subject. Usually this task will be undertaken by the general manager.

Erasure

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

Under the GDPR, this right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

There are some specific circumstances where the right to erasure does not apply and you can refuse to deal with a request.

You can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defense of legal claims.

Once validated Heronstone is obliged to notify the data subject the consequences or erasure. After this has been agreed the data subject's data will be purged from company's systems.

Notification will be sent by email after this has been complete.

Data Breach Policy

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Information and Description

In the event of a data breach the company's system must be secured ASAP to prevent further any further loss of information.

By law the company must inform the ICO within 72 hours of becoming aware and notify them of the data breach. The company may also have to inform data subjects if it suspects their data was lost and is likely to result in a high risk to the rights and freedoms of the data subject.

The company will work with the ICO on identifying the breach and move forward with any suggested improvements as soon as practically possible.