Date: 21/05/2018
Date Reviewed:

Data Protection Policy

Employer: Mueller Europe Ltd, Oxford St, Bilston, West Midlands. WV14 7DS

Purpose and Scope

Mueller Europe Limited is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, contractors, and former employees, referred to as HR-related personal data.

Mueller Europe Limited has appointed their Financial Controller as data protection controller. Their role is to inform and advise the organisation on its data protection obligations. Questions about this policy, or requests for further information, should be directed to the data protection controller.

Definitions

"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

Mueller Europe Limited processes HR-related personal data in accordance with the following data protection principles:

- We process personal data lawfully, fairly and in a transparent manner.
- We collect personal data only for specified, explicit and legitimate purposes.
- We process personal data only where it is adequate, relevant and is limited to what is necessary for the purposes of processing.
- We keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- We keep personal data only for the period necessary for processing.

- We adopt appropriate measures to make sure that personal data is secure, protected against unauthorised or unlawful processing, accidental loss, destruction or damage.

We tell individuals the reasons for processing their personal data, how we use such data and the legal basis for processing in our privacy notices. We will not process personal data of individuals for other reasons. Where we rely on our legitimate interests as the basis for processing data, we will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

We will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered during the employment and contractor relationship is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which the organisation holds HR-related personal data are contained in its privacy notices to individuals.

Mueller Europe Limited will keep a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, we will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

We will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

To make a subject access request, the individual should send the request to the HR Manager. In some cases, we may need to ask for proof of identification before the request can be processed. We will inform the individual if we need to verify his/her identity and the documents we require.

We will normally respond to a request within a period of one month from the date it is received.

If a subject access request is manifestly unfounded or excessive, we are not obliged to comply with it. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the we have already responded. If an individual submits a request that is

unfounded or excessive, we will notify him/her that this is the case and whether or not we will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the employer to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the employer's legitimate grounds for processing data (where the employer relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the employer's legitimate grounds for processing data.

To ask the organisation to take any of these steps, the individual should send the request to the HR Manager.

Data security

We take the security of HR-related personal data seriously. Mueller Europe Limited has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties

Where we engage third parties to process personal data on our behalf, we will always ensure that they do so subject to privacy and security obligations consistent with our practices and with applicable laws.

Data breaches

If we discover that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner within 72 hours of discovery. We will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International data transfers

HR-related personal data may be transferred to countries outside the EEA i.e. to our head office in America (Mueller Industries). Data is transferred outside the EEA using appropriate safeguards to ensure that your personal data is treated securely and in accordance with data protection legislation.

Individual responsibilities

Individuals are responsible for helping us keep our personal data up to date. Individuals should let us know if data provided to us changes, for example if an individual moves house or changes his/her bank details.

Individuals may have access to the personal data of other individuals in the course of their employment. Where this is the case, we rely on individuals to help meet our data protection obligations.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the employer) who have appropriate authorisation;
- to keep data secure
- not to remove personal data, or devices containing or that can be used to access personal data, from our premises without adopting appropriate security measures, not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the employer's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Signed on behalf of Mueller Europe:

Date of Policy Agreement:

21/05/218