

| | | | |
|----------------------|----------------------------------|---|---------|
| FILE: | HQ-58 - Central Personnel Manual | | |
| POLICY TITLE: | Data Protection Policy | | |
| NUMBER: | 58-0528 v4.0 | ISSUED: | 22-5-18 |
| AUTHOR: | Tony Alcock | TRAINING REQUIRED ON THIS VERSION: | false |
| SITE(S): | All Sites | | |

Yeo Valley People Data - Data protection policy (compliant with the GDPR)

Introduction

Purpose

Yeo valley 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 Yeo Valley's 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 and former employees, referred to as HR-related personal data.

Questions about this policy, or requests for further information, should be directed to your HR Advisor.

Definitions

"Personal data" is any information that relates to an 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

Yeo Valley processes HR-related personal data in accordance with the following data protection principles, Yeo Valley:

- Processes personal data lawfully, fairly and in a transparent manner.
- Collects personal data only for specified, explicit and legitimate purposes.
- Processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- Keeps personal data only for the period necessary for processing.
- Adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

| | |
|----------------------|------------------------|
| POLICY TITLE: | Data Protection Policy |
| NUMBER: | 58-0528 v4.0 |
| ISSUED: | 09 Aug. 19 |

Yeo Valley informs individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing it.

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

Personal data gathered during employment, is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR Dynamics systems. The periods for which Yeo Valley holds HR-related personal data are contained in the HR personal data register. Personal files will normally be destroyed 6 years after termination dates.

Yeo Valley keeps 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, Yeo Valley 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 Yeo Valley has failed to comply with his/her data protection rights; and

Where requested, Yeo Valley 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.

Yeo Valley 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, Yeo Valley is not obliged to comply with it. Alternatively, Yeo Valley can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which Yeo Valley has already responded. If an individual submits a request that is unfounded or excessive, Yeo Valley will notify him/her that this is the case and whether or not it will respond to it.

| | |
|----------------------|------------------------|
| POLICY TITLE: | Data Protection Policy |
| NUMBER: | 58-0528 v4.0 |
| ISSUED: | 09 Aug. 19 |

Other rights

Individuals have a number of other rights in relation to their personal data. They can require Yeo Valley 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 Yeo Valley's legitimate grounds for processing data (where Yeo Valley 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 Yeo Valley's legitimate grounds for processing data.

To ask Yeo Valley to take any of these steps, the individual should send the request to their HR Advisor.

Data security

Yeo Valley takes the security of HR-related personal data seriously. Yeo Valley has internal 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 Yeo Valley engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Data breaches

If Yeo Valley discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. Yeo Valley 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, it 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

Yeo Valley will not transfer HR-related personal data to countries outside the EEA.

| | |
|----------------------|------------------------|
| POLICY TITLE: | Data Protection Policy |
| NUMBER: | 58-0528 v4.0 |
| ISSUED: | 09 Aug. 19 |

Individual responsibilities

Individuals are responsible for helping Yeo Valley keep their personal data up to date. Individuals should let Yeo Valley know if data provided to Yeo Valley 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 and of our customers and consumers in the course of their employment. Where this is the case, Yeo Valley relies on individuals to help meet its data protection obligations to staff, to customers and consumers.

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 Yeo Valley) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from Yeo Valley's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

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

Training

Yeo Valley will provide training to all individuals about their data protection responsibilities as part of the induction process.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.