wiser

Data protection policy

30 April 2020

Contents

1 Purpose

Wiser 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 Wiser's commitment to data protection and individual rights and obligations in relation to personal data.

This policy helps to protect Wiser from some very real data security risks, including:

- Beaches of confidentiality;
- Failing to offer choice;
- Reputational damage

This policy applies to the personal data of job applicants, employees and former employees ("**HR-related personal data**"). This policy does not apply to the personal data of clients or other personal data processed for business purposes.

Wiser has appointed Ben Buffone as its Data Protection Officer ("**DPO**"). His role is to inform and advise Wiser on its data protection obligations and he can be contacted at dpo@wearewiser.com.

Questions about this policy, or requests for further information, should be directed to the DPO.

2 Definitions

"**Criminal Records Data**": information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

"**Employees**": Anyone who works for Wiser, including freelancers.

"**Personal Data**": 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**": 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.

3 Data protection principles

Wiser processes HR-related Personal Data in accordance with the following data protection principles:

- Personal Data will be processed lawfully, fairly and in a transparent manner;
- Personal Data is collected only for specified, explicit and legitimate purposes;
- Personal Data is only processed where it is adequate, relevant and limited to what is necessary for the purposes of processing;
- All reasonable steps will be taken to ensure that only accurate Personal Data is kept and that inaccurate Personal Data is rectified or deleted without delay;
- Personal Data is kept only for the period necessary for processing
- Appropriate measures are adopted to ensure that Personal Data is secure and protected against unauthorised or unlawful processing, accidental loss, destruction or damage.
- Individuals will be notified of the reasons for Wiser:
    - processing their Personal Data;
    - using such data;
    - the legal basis for processing this data
- Where there is a legitimate interest for processing data, Wiser will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals;
- Where Wiser processes Special Categories of Personal Data or Criminal Records Data to perform obligations or to exercise rights in employment law, this is done in accordance with Wiser's policy on Special Categories of Data and Criminal Records Data;
- All HR-related Personal Data will be promptly updated if an individual advises that his/her information has changed or is inaccurate;

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

Wiser 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 2018 (GDPR).

4 Individual rights

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

4.1 Subject access request

Individuals have the right to make a subject access request.

If an individual makes a subject access request, Wiser will notify 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 Wiser has failed to comply with his/her data protection rights;
- Whether or not Wiser carries out automated decision-making and the logic involved in any such decision-making.

Wiser 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.

If the individual wants additional copies, Wiser will charge a fee, which will be based on the administrative cost to Wiser of providing the additional copies. To make a subject access request, the individual should send the request to dpo@wearewiser.com for making a subject access request.

In some cases, Wiser may need to ask for proof of identification before the request can be processed. Wiser will inform the individual if it needs to verify his/her identity and the documents it requires.

Wiser will normally respond to a request within a period of one month from the date the request is received. In some cases, such as where Wiser processes large amounts of the individual's data, it may respond within three months of the date the request is received. Wiser will write to the individual

within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, Wiser is not obliged to comply with it. Alternatively, Wiser 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 Wiser has already responded.

If an individual submits a request that is unfounded or excessive, Wiser will notify him/her that this is the case and whether or not it will respond to it.

4.2 Other rights

Individuals have a number of other rights in relation to their Personal Data. They can require Wiser 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 Wiser's legitimate grounds for processing data (i.e. where Wiser relies on its legitimate interests as a reason for processing data);
- Stop processing or erase data if processing is unlawful;
- 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 Wiser's legitimate grounds for processing data.

To ask Wiser to take any of these steps, the individual should send the request to dpo@wearewiser.com.

Wiser processes HR-related Personal Data in accordance with the following data protection principles:

5 Data security

5.1 Internal policies

Wiser takes the security of HR-related Personal Data seriously.

Wiser 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.

Details of how Wiser handles this area can be found in Wiser's suite of Information Management Security Systems policies. This can be found on the Wiser Group Drive. All cyber related policies are also on CyberSmart.

Where Wiser 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.

5.2 Data storage

Personal Data is of no value to Wiser unless the business can make use of it. However, it is when Personal Data is accessed and used that it can be at the greatest risk of loss, corruption or theft.

The following guidelines help to limit this risk:

- When working with personal data, Employees must ensure the screens of their computers are always locked when left unattended;
- Personal Data must not be shared informally;
- Employees must not save copies of Personal Data to their own computers.

5.3 Data accuracy

The law requires Wiser to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible:

- Data will be held in as few places necessary. Employees must not create any unnecessary additional data sets;
- Employees must take every opportunity to ensure data is updated;
- Data must be updated as inaccuracies are discovered.

5.4 International data transfers

Wiser will not transfer HR-related Personal Data to countries outside the EEA.

5.5 Employee responsibilities

Everyone who works for or with Wiser has some responsibility for ensuring data is collected, stored and handled appropriately ("**Employees**").

Employees who have access to Personal Data are required to:

- Access only data that they have authority to access and only for authorised purposes;
- Not disclose data except to individuals (whether inside or outside Wiser) who have appropriate authorisation;
- 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 remove Personal Data, or devices containing or that can be used to access Personal Data, from Wiser's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- Not store Personal Data on local drives or on personal devices that are used for work purposes;
- To report data breaches of which they become aware by emailing dpo@wearewiser.com.

However, these people have key areas of responsibility:

- Ben Buffone, CTO, is ultimately responsible for ensuring that Wiser meets its legal obligations;
- Ben Buffone, DPO, is ultimately responsible for:
    - Keeping the management team updated about data protection responsibilities, risk and issues;
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule;
    - Arranging data protection training and advice for the people covered by this policy;
    - Handling data protection questions from team member and anyone else covered by this policy;
    - Checking and approving any contracts or agreements with third parties that may handle company's sensitive data;

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards;
- Performing regular checks and scans to ensure security hardware and software is functioning properly;
- Evaluating any third-party services the company is considering using to store or process data (e.g. cloud computing services);
- Approving any data protection statements attached to communications such as emails and letters;
- Addressing any data protection queries from journalists or media outlets like newspapers;
- Working with other team members to ensure marketing initiatives abide by data protection principles;
- Dealing with requests from individuals to see the data Wiser holds about them

Further details about Wiser's security procedures can be found on the Wiser Group Drive. All cyber related policies are also on CyberSmart.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under Wiser'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.

5.6 Training

Wiser will provide training to all individuals part of the induction process. This will cover their data protection responsibilities.

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.