DATA PRIVACY STATEMENT

(General Data Protection Regulations – GDPR)

Introduction

At AOK, we are committed to being transparent about how we collect and use the personal data of our workforce, and to meeting our 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 personal data of individuals or other personal data processed for business purposes only.

We have appointed David Turner, Managing Director as AOK's Data Controller (person with responsibility for data protection compliance within the business). Questions about this policy, or requests for further information, should be directed to GDPR@aokprinters.com

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

We process 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 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, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.
- We will update personal data promptly if advised to.
- We keep a record of our processing activities in accordance with the requirements of the General Data Protection Regulation (GDPR).

What information do we collect?

We collect and process a range of information depending on specific requirements.

Data will be stored electronically with several security measures in place such as encryption/passwords, giving limited access to files within our systems (including our email system).

Why do we process personal data?

We need to process data to meet our business obligations.

Who has access to data?
Your information may be shared internally, including with selected members of the AOK team or managers in the business area but only if access to the data is necessary for performance of their roles.

We may also on occasion share your data with third parties that process data on our behalf if its necessary to meet business needs.

International data transfers

We will not transfer your data to countries outside the European Economic Area.

How do we protect data?

We take the security of your data seriously. We have internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by AOK employees in the performance of their duties. We use a cloud-based system to store your data, which requires a duo factor authentication that only specific/limited staff in authority have access to.

Where we engage third parties to process personal data on our behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate measures to ensure the security of data.

Data breaches

If we discover that there has been a breach of 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.

For how long do we keep data?

AOK will hold your personal data for the duration of completing the task required, after which it will be destroyed.

Your rights

As a data subject, you have a number of rights. You can:

- Access and obtain a copy of your data on request (see below).
- Require us to change incorrect or incomplete data.
- Require us to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing.
- Object to the processing of your data.

If you would like to exercise any of these rights, please contact AOK at GDPR@aokprinters.com

If you believe that we have not complied with your data protection rights, you can complain to the Information Commissioner.

Subject access requests

If you make a subject access request, we tell you:

- Whether or not your 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 you.
- To whom your data is or may be disclosed.
- For how long your personal data is stored (or how that period is decided).
- Your rights to rectification or erasure of data, or to restrict or object to processing.
- Your right to complain to the Information Commissioner if you think AOK has failed to comply with your data protection rights.
- Whether or not we carry out automated decision-making and the logic involved in any such decision-making.

We can also provide you with a copy of the personal data undergoing processing. This will normally be in electronic form if you have made a request electronically, unless you agree otherwise.

To make a subject access request, you should send the request to GDPR@aokprinters.com. In some cases, we may need to ask for proof of identification before the request can be processed. We will inform you if we need to verify your 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. In some cases, such as where we process large amounts of your data, we may respond within three months of the date the request is received. We will write to you within one month of receiving the original request to tell you if this is the case.

If a subject access request is manifestly unfounded or excessive, we are not obliged to comply with it. Alternatively, we 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 we have already responded. If you submit a request that is unfounded or excessive, we will notify you that this is the case and whether or not we will respond to it.

Automated decision-making

Decisions are not based solely on automated decision-making.

Your responsibilities

You are responsible for helping us keep data up to date. You should let us know if data provided to us changes.

You may have access to the personal data of other individuals, our customers and clients in the course of your employment, contract, volunteer period, internship or apprenticeship. Where this is the case, we rely on individuals to help meet our data protection obligations to staff, customers and clients.

If you are have access to the data you provide, you are required:

- To access only data that you have authority to access and only for authorised purposes.
- Not to disclose data except to individuals who have appropriate authorisation.

- To keep data secure.
- Not to remove personal data, and to secure the data at all times.
- Not to store personal data on local drives or on personal devices.

Failing to observe these requirements may amount to an offence.

Training

We will provide training to all individuals about their data protection responsibilities at appropriate times where necessary.