

Data Protection Policy

Background

The Data Protection Act 2018 controls how personal information is used by organisations, businesses or the government.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Effective from: 31st July 2024

Signed off by: Helen Thain

Previous versions: Version 1 dated 1st November 2018

Introduction

Purpose

Adexchange is committed to being transparent about how it collects and uses personal data, and to meeting its data protection obligations. This policy sets out Adexchange's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to all personal data processed for business purposes, including the personal data of job applicants, employees, contractors, former employees, and clients both current and past.

Adexchange has appointed Helen Thain as the person with responsibility for data protection compliance within Adexchange. She can be contacted at helen@adexchange.co.uk. Questions about this policy, or requests for further information, should be directed to her.

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

Adexchange processes personal data in accordance with the following data protection principles:

- Adexchange processes personal data lawfully, fairly and in a transparent manner.
- Adexchange collects personal data only for specified, explicit and legitimate purposes.

- Adexchange processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Adexchange keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- Adexchange keeps personal data only for the period necessary for processing.
- Adexchange adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Adexchange tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

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

Personal data gathered during business activities is held in hard copy or electronic format, or both. The periods for which Adexchange holds personal data are contained in its privacy notices to individuals.

Adexchange keeps a record of its processing activities in respect of 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, Adexchange 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 Adexchange has failed to comply with his/her data protection rights; and
- whether or not Adexchange carries out automated decision-making and the logic involved in any such decision-making.

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

Adexchange will normally respond to a request within a period of one month from the date it is received. In some cases, such as where Adexchange processes large amounts of the individual's data, it may respond within three months of the date the request is received. Adexchange 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, Adexchange is not obliged to comply with it. Alternatively, Adexchange 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 Adexchange has already responded. If an individual submits a request that is unfounded or excessive, Adexchange will notify him/her that this is the case and whether or not it will respond to it.

Other rights

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

- the right to be informed about the collection and the use of personal data
- the right to access personal data and supplementary information
- the right to have inaccurate personal data rectified, or completed if it is incomplete
- the right to erasure (to be forgotten) in certain circumstances

- the right to restrict processing in certain circumstances
- the right to data portability, which allows them to obtain and reuse personal data for their own purposes
- the right to object to processing in certain circumstances
- rights in relation to automated decision making and profiling
- the right to withdraw consent at any time (where relevant)

To ask Adexchange to take any of these steps, the individual should send the request to helen@adexchange.co.uk.

Data security

Adexchange takes the security of personal data seriously. Adexchange 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.

All data stored on Adexchange systems is secured by user authentication with strong passwords. All data backed up on cloud servers is secured by 256 bit encryption. All Adexchange's systems are protected by up to date anti-virus software. All inbound and outbound email is scanned for SPAM and viruses. All Adexchange employees and contractors have signed Non-Disclosure Agreements. No data is stored outside the UK.

Where Adexchange 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 Adexchange measures to ensure the security of data.

Further details about Adexchange's security procedures can be found in its Information Security Policy.

Impact assessments

Some of the processing that Adexchange carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, Adexchange will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data breaches

If Adexchange discovers that there has been a breach of 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. Adexchange 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

Adexchange will not transfer personal data to countries outside the EEA.

Individual responsibilities

Individuals are responsible for helping Adexchange keep their personal data up to date. Individuals should let Adexchange know if data provided to Adexchange changes.

Individuals may have access to the personal data of other individuals in the course of their employment / contract. Where this is the case, Adexchange relies on individuals to help meet its 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 Adexchange) 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 Adexchange'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 Adexchange'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

Adexchange will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

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.