

## Pixel Takeaway Limited

1 Canada Sq, 37th Floor, Canary Wharf, London, E14 5AA, United Kingdom

# AdRoaster: GDPR data protection policy

Last updated: 7 April 2026

## 1. Introduction

This Data Protection Policy is the overarching policy for data security and protection for Pixel Takeaway Limited, trading under the name of “AdRoaster” (hereafter referred to as “us”, “we”, “our” or “The Company”), UK-registered company no. 08705786, registered office at 1 Canada Sq 37th Floor, Canary Wharf, London, E14 5AA, United Kingdom.

We are registered with the Information Commissioner’s Register of Data Controllers under number ZA346976 and handle your data according to GDPR.

We have been issued Cyber Essentials certificate number ff0db3db-adeb-4371-8a71-57caca13fa77 by The IASME Consortium Ltd, and comply with the requirements of the Cyber Essentials Scheme.

The Company obtains, keeps, and uses personal information about job applicants, current and former employees, temporary and agency workers, contractors, interns, volunteers, apprentices, and customers for a number of specific lawful purposes.

This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our workforce and customers.

We are committed to complying with our data protection obligations, and to being concise, clear, and transparent about how we obtain and use personal information.

If you have any questions or comments, please contact [team@adroaster.com](mailto:team@adroaster.com).

## 2. Purpose

The purpose of the Data Protection Policy is to support the 10 Data Security Standards, the General Data Protection Regulation (2016), the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation.

This policy covers our data protection principles and commitment to common law and legislative compliance, and procedures for data protection by design and by default.

## 3. Scope

This policy includes in its scope all data which we process either in hardcopy or digital copy, including special categories of data.

This policy applies to all customers, staff, including temporary staff and contractors.

We will review and update this policy regularly in accordance with our data protection obligations.

## 4. Definitions

**Data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information.

**Data subject** means the individual to whom the personal information relates.

**Personal information** means information relating to an individual who can be identified (directly or indirectly) from that information.

**Processing** means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it.

**Pseudonymised** means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information.

**Sensitive personal information** means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics information, biometric information, and information concerning health, sex life or sexual orientation.

## 5. Data protection principles

We will process personal information lawfully, fairly and in a transparent manner.

We will collect personal information for specified, explicit and legitimate purposes only.

We will only process the personal information that is adequate, relevant, and necessary for the relevant purposes.

We will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay.

We will keep personal information in a form which permits identification of data subjects for no longer than is necessary.

We will take appropriate technical and organisational measures to ensure that personal information is kept secure.

## 6. Basis for processing personal information

In relation to any processing activity, we will review the purposes and select the most appropriate lawful basis: consent; performance of a contract; compliance with a legal obligation; protection of vital interests; or legitimate interests of the Company.

We will document our decision as to which lawful basis applies, to help demonstrate our compliance.

## 7. Sensitive personal information

We will only process sensitive personal information if we have a lawful basis for doing so and one of the special conditions for processing applies (e.g. explicit consent, employment law obligations, vital interests, legal claims, or substantial public interest).

## 8. Data protection impact assessments (DPIAs)

Where processing is likely to result in a high risk to data subjects, we will carry out a DPIA to assess the level of risk and identify measures to mitigate it.

## 9. Documentation and records

We will maintain written records of our processing activities, including purposes, data categories, recipients, transfers, retention periods, and security measures.

## 10. Privacy notice

We will issue privacy notices setting out clearly and in plain language how we process personal data. These are reviewed and updated regularly.

## **11. Individual rights**

We will comply with data subjects' rights including: the right to be informed; right of access; right to rectification; right to erasure; right to restrict processing; right to data portability; right to object; and rights in relation to automated decision-making and profiling.

## **12. Information security**

We will use appropriate technical and organisational measures in accordance with our IT Security Policy to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

## **13. Data breaches**

In the event of a data breach, we will take immediate steps to assess the risk and take action to mitigate it. Where required, we will notify the ICO within 72 hours and inform affected data subjects without undue delay.

## **14. International data transfers**

We will not transfer personal data to a country outside the EEA unless that country ensures an adequate level of protection, or appropriate safeguards are in place (such as standard contractual clauses).

## **15. Training**

We will ensure that all staff who handle personal data receive appropriate training on data protection and this policy.

## **16. Compliance**

Compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action. Questions about this policy should be directed to [team@adroaster.com](mailto:team@adroaster.com).