Data Privacy Notice

Version 1.3

May 2019

Owner	ISM/DPO manager	
SIRO Approval	Martin Chamberlain	Date: 15/05/2019
Version / Date	1.3	Date: May 2019
Next Review Date	No later than May 2020	
Storage Location	Shared Drive: \ISMS\GDPR\Data Privacy Notice	

Reference to other documents
Information Security Policy
Computer Misuse Act 1990 Copyright, Designs and Patents Act 1988 Crime and Disorder Act 1998 Criminal Justice and Court Service Act 2000 Data Protection Act 2018 Data Protection Codes of Practice. Disability Discrimination Act 1995 Electronic Communications Act 2000 EU General Data Protection Regulation (GDPR) Human Rights Act 1998 Lawful Business Practice (Interception of Communications) Regulations 2000 Police and Criminal Evidence Act 1984 Privacy and Electronic Communications (EC Directive) Regulations 2003 Race Relations (Amendment) Act 2000 Regulation of Investigatory Powers Act 2000

1 Document Control

1.1 Change Control Record

Date	Author	Version	Change reference
May 18	Dean Scales	0.1	Initial draft
June 18	Dean Scales	1.0	Approved and published
Sept 2018	Ian Whitehead	1.1	Revised Policy
Nov 2018	Martin Chamberlain	1.2	SIRO Approved
Feb 2019	A Jama	N/A	Q1 Annual Review
May 2019	Richard Cornell	1.3	Updated contact details and other minor errors

Table 1 – Document change control record

1.2 Document Control Statement

The following outlines the access, handling, communication and disposal guidelines that are followed by The Information Assurance Programme for this document based on the assigned classification. For this document, which has a classification of T4 Unclassified, the following is recommended:

1.2.1 Access Guidelines

- There are no restrictions on this document.

1.2.2 Handling Guidelines

- This document will be stored in the ISMS, accessible via Shared Drive.
- There are no restrictions on electronic or paper copies.

1.2.3 Communications Guidelines

- Altodigital documents which are to be communicated external to Altodigital must be produced in PDF format.

1.2.4 Disposal Guidelines

- There are no restrictions on electronic or paper copies.

Table of Contents

2 Introduction

The term “Altodigital Networks Limited” or “us” or “we” refers to the owner of this website. The term “you” refers to the user or viewer of this policy.

Altodigital is an independent provider of office technology and supplies with over 35 years’ experience offering a range of products and services spanning across print, IT, communications, document management and office supplies. To complement these services, Altodigital offers a UK based call centre and 24/7 web portal. To support the service capability, Altodigital also operates a network of nationwide technical expertise.
Altodigital own many business assets, including physical items, IT services, communication systems, information and personnel, all of which have a high value to Altodigital and therefore need to be suitably protected.
To ensure the adequate protection of these business assets from a wide range of threats, Altodigital employs an Information Risk Management approach to the implementation of physical, procedural, technical and personnel security measures throughout the organisation. This ensures that all risks pertinent to Altodigital’s business assets are identified, prioritised, managed and treated in an effective and consistent manner, thereby maintaining their Confidentiality, Integrity and Availability.

3 Executive Summary

We appreciate the trust you place in us when sharing your personal data. The security of that data is very important to us. In this document, we will explain how we collect, use and protect your personal data.
We will also explain what rights you have with regards to your personal data and how you can exercise those rights.

4 Governance

Altodigital Networks Limited (Altodigital), has committed to protect all processing of personal data, and has appointed a Data Protection Officer (DPO).

Altodigital’s management team are committed to ensuring that all their employees responsible for the processing of personal data are aware of and comply with the contents of this policy.

In addition, Altodigital will make sure all Third Parties engaged to process personal data on their behalf (i.e. their Data Processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to personal data controlled by Altodigital.

5 Data Collection

5.1 Data Sources

Personal data should be collected only from the data subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the personal data from other persons or bodies
- The collection must be carried out under emergency circumstances to protect the vital interests of the data subject or to prevent serious loss or injury to another person

If personal data is collected from someone other than the data subject, the data subject must be informed of the collection unless one of the following apply:

- The data subject has received the required information by other means
- The information must remain confidential due to a professional secrecy obligation
- A national law expressly provides for the collection, processing or transfer of the personal data

Where it has been determined that notification to a data subject is required, notification should occur promptly, but in no case later than:

- One month from the first collection or recording of the personal data
- At the time of first communication, if used for communication, with the data subject
- At the time of disclosure, if disclosed, to another recipient

6 Notification

Data subjects have the right to be informed about the collection and use of their personal data, when required by applicable law, contract or where it considers that it is reasonably appropriate to do so, Altodigital will provide this information to data subjects

When the data subject is asked to give consent to the processing of personal data and when any personal data is collected from the data subject, all appropriate disclosures will be made in a manner that draws attention to them, unless one of the following apply:

- The data subject already has the information
- A legal exemption applies to the requirements for disclosure and/or consent

These disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the DPO. The associated receipt or form should be retained, along with a record of the facts, date, content and method of disclosure.

7 Data Use

7.1 Data Processing

Altodigital collects and processes personal data such as a contact name, phone number, and email address for the following purposes:

- Sales and Marketing account management and communications for existing contacts
- The ongoing administration and management of customer services
- Accounts Payable and Accounts Receivable processing

Altodigital will process personal data in accordance with all applicable laws and applicable contractual obligations. Specifically, Altodigital will not process personal data unless at least one of the following requirements are met:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party to, or to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for the purpose of the legitimate interests pursued by the controller or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child)

There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. When deciding as to the compatibility of the new reason for processing, guidance and approval must be obtained from the DPO before any such processing may commence.

If consent has not been gained for the specific processing in question, Altodigital will address the following additional conditions to determine fairness and transparency of any processing beyond the original purpose for which the personal data was collected:

- Any link between the purposes for which the personal data have been collected and the purposes of the intended further processing
- The context in which the personal data has been collected, in particular regarding the relationship between data subject and the data controller
- The nature of the personal data, in particular whether special categories of data are being processed, or whether personal data related to criminal convictions and offences are being processed
- The possible consequences of the intended further processing for data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymisation

7.2 Data About Children

Due to the nature of Altodigital's business there are occasions where we handle the Personal Data of children, however we don't offer services directly to children or collect personal data about children. Where we process children's data, we take extra care to make sure we protect their interests.

7.3 Data Accuracy

To ensure that the personal data it collects, and processes is complete and accurate in the first instance and is updated to reflect the current situation of the data subject, Altodigital shall adopt all necessary measures.

The measures adopted by Altodigital to ensure data quality include:

- Ensuring personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated is corrected, even if the data subject does not request rectification
- Ensuring personal data is held only for the period necessary to satisfy the permitted uses
- Ensuring the removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required

7.4 Data Retention

Altodigital will not retain personal data for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. All personal data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

8 Security Measures

Altodigital shall adopt physical, technical and organisational security measures to protect data subjects' Confidentiality, Integrity and Availability.

This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks affecting the confidentiality, integrity and availability of the personal data.

The minimum set of security measures to be adopted are set out in Altodigital's Information Security Policy and includes the following:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data is processed
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations
- Ensure the integrity and confidentiality of Personal Data in the course of electronic transmission is maintained meaning that it cannot be read, copied, modified or removed without authorisation
- Ensure that a system for maintaining accountability is in place. This means access logs are used to establish whether the personal data was entered into, modified or removed from a data processing system and by whom
- Ensure the availability of personal data is maintained, meaning that it is protected against undesired destruction or loss
- Ensure that personal data collected for different purposes can and is processed separately
- Ensure that personal data is not kept longer than necessary

9 Data Subject Rights

The DPO will establish a system which will enable the exercise of rights granted to the data subjects, which under the EU GDPR are:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right of data portability
- The right to object
- The right in relation to automated decision making and profiling

Legal requirements may override the rights of EU GDPR which shall be taken into consideration if a data subject's rights are to be exercised.

Based upon a written subject access request to the DPO by contacting dataprotectionofficer@altodigital.com and successful confirmation of identity, data subjects are entitled to obtain the following information about their own personal data:

- The purposes of the collection, processing, use and storage of their personal data
- The sources of the personal data, if it did not come directly from the data subject
- The categories of personal data stored for the data subject
- The recipients or categories of recipients to whom the personal data has been or may be transmitted, along with the location of those recipients
- The predicted period of storage for the personal data or the rationale for determining the storage period
- The right of the data subject to:
    - Object to processing of their personal data
    - Lodge a complaint with the data protection authority
    - Request rectification or erasure of their personal data
    - Request restriction of processing of their personal data

It should be noted that situations may arise where providing the information requested by a data subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as necessary or appropriate to protect that person's rights.

10 Consent

10.1 Data Subject Consent

All Altodigital entities must obtain personal data using only lawful and fair means where appropriate with the knowledge and consent of the individual concerned.

Altodigital is committed to requesting and receiving consent of an individual prior to the collection, use or disclosure of their personal data.

The DPO, with the cooperation of the business, shall establish a system for obtaining and documenting data subject consent for the collection, processing, and/or transfer of their personal data. The system must include provisions for:

- Ensuring clear disclosures are made around what the data is needed for and how it is going to be used
- Ensuring the request for consent is presented in a manner which is prominent and separate from any other terms and conditions, is made in an intelligible and easily accessible form and uses clear and plain language
- Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the consents given

10.2 Withdrawal of Consent

Data subjects have the right to withdraw consent of the processing of their personal data at any time.

To request withdrawal of consent, please contact the DPO by email: dataprotectionofficer@altodigital.com

11 Transfers

11.1 Third Party Transfers

Altodigital may transfer Personal Data to internal or Third-Party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects.

An approval transfer mechanism is complied with when transferring to countries lacking an adequate level of legal protection.

Altodigital employees may only transfer personal data where one of the transfer scenarios listed below applies:

- The data subject has given consent to the proposed transfer
- The transfer is necessary for the performance of a contract with the data subject
- The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the data subject
- The transfer is legally required on important public interest grounds
- The transfer is necessary in order to protect the vital interests of the data subject
- Altodigital shall only transfer personal data to, or allow access by, Third Parties when assurances are given that the information will be processed legally and fairly and protected according to the GDPR requirements. Pertaining to Third Party processing, Altodigital will first identify if, under applicable law, the Third Party is considered a data controller, or a data processor of the personal data being transferred
- If the Third Party is deemed to be a data controller, Altodigital will enter into, in cooperation with the DPO, an appropriate agreement with the controller to clarify each party's responsibilities in respect to the personal data being transferred
- Where the Third Party is deemed to be a data processor Altodigital will, in cooperation with the DPO, enter into an adequate processing agreement with the data processor. The agreement must require the data processor to protect the personal data from further disclosure and to only process personal data in compliance with

Altodigital's instructions. In addition, the agreement will require the data processor to implement appropriate technical and organisational measures to protect the personal data as well as procedures for providing notification of personal data breaches

- In the event that Altodigital outsources services to a Third Party, Altodigital will identify whether the Third Party will process personal data on its behalf and whether the outsourcing will entail any personal data crossing international borders. In either case, it will make sure to include, in cooperation with the DPO, adequate provisions in the outsourcing agreement for such processing
- The DPO shall conduct regular audits on the processing of personal data performed by Third Parties, especially with regard to technical and organisational measures they have in place

11.2 Internal Transfers

For Altodigital to carry out its business effectively across its various Altodigital entities, there may be occasions when it is necessary to transfer personal data from one Altodigital entity to another, or to allow access to the personal data from an overseas location. Should this occur, the Altodigital entity sending the personal data remains responsible for ensuring protection of that data.

When transferring personal data to another Altodigital entity, Altodigital must:

- Ensure that the recipient Altodigital Entity is included on the approved list of Altodigital entities. The approved list is held and maintained by the DPO
- Only transfer the minimum amount of personal data necessary for the purpose of the transfer (for example, to fulfil a transaction or carry out a particular service)
- Ensure adequate security measures are used to protect the personal data during the transfer (including password-protection and Encryption, where necessary)

12 Complaints

Should you wish to discuss a complaint, please feel free to contact the DPO by email: dataprotectionofficer@altodigital.com . All complaints will be treated in a confidential manner.
Should you feel unsatisfied with our handling of your data, or about any complaint that you have made to us about our handling of your data, you are entitled to escalate your complaint to a supervisory authority within the European Union. For the United Kingdom, this is the Information Commissioner's Office (ICO), who is also our lead supervisory authority. Its contact information can be found at https://ico.org.uk/global/contact-us/.

13 Reporting a Data Breach

The EU GDPR introduces a responsibility on all organisations to report certain types of personal data breaches to the supervisory authority for the UK the Information Commissioners office (ICO) https://ico.org.uk/

The timescale of reporting a data breach must be within 72 hours of becoming aware of the breach. If the breach is likely to result in a high risk of adversely affecting an individual's rights and freedoms, organisations must also inform the individuals affected without undue delay.

Altodigital must also keep a record of any personal data breaches, regardless of whether notification is required.