altodigital
your office technology partner

Data Protection Policy

Version 0.2

May 2018

Department	**Altodigital**	
Product or Process	**Data Protection Policy**	
Document Author	Dean Scales	
Document Approval	Dave Gibson SIRO	Approved: Dave Gibson Date: 01/06/2018
Document Accepted	Dean Scales ISM/DPO	Accepted: Dean Scales Date: 01/06/2018
Version	0.2	
Next Review Due	May 2019	
Storage	Shared Drive ISMS/GDPR (X Drive)	

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	0.2	Approved and published

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 internal staff access to this document.

1.2.2 Handling Guidelines

- This document will be stored in the ISMS, accessible via Shared Drive (Q Drive).
- Hardcopies of documents will be stored under lock and key.

1.2.3 Communications Guidelines

- Altodigital documents which are to be communicated external to Altodigital must be produced in protected PDF format and sent with encryption where appropriate.

1.2.4 Disposal Guidelines

- All hardcopies of this document will be securely shredded.

Table of Contents

2 Introduction

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

From 25th May 2018, the General Data Protection Regulation (GDPR) replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual EU Member States that were developed in compliance with the Data Protection Directive 95/46/EC i.e. the Data Protection Act 1998 in the UK. The purpose of the GDPR set out rules relating to the protection of natural persons, regarding the processing of personal data and rules relating to the free movement of personal data. GDPR protects the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and wherever possible, that is it processed with their consent.

Altodigital is committed to conducting any of its business in strict accordance with GDPR. This policy highlights the expected behaviours of Altodigital employees (including contractors, secondees, agency personnel, contracted third parties) pertaining to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to an Altodigital contact – i.e. the data subject. Under GDPR personal data is any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier. Personal data is liable to certain legal protections and other regulations, which force limitations on how organisations may process personal data. An organisation that handles personal Data and makes decisions about its utilization is known as a Data Controller. Altodigital, as a Data Controller, oversees compliance with the Data Protection requirements outlined in this policy. Failure to conform may open Altodigital to complaints, regulatory action, fines and also reputational harm.

4 Scope

This policy applies to all Altodigital entities where a data subject's personal data is processed. GDPR applies to electronic and paper records held in structured filing systems containing personal data, meaning data which relates to living individuals who can be identified from the data. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

5 Policy

5.1 Governance

5.1.1 Office of Data Protection

In Altodigital's efforts to show commitment to Data Protection, and in the hope of enhancing the effectiveness of our compliance efforts, Altodigital has appointed a Data Protection Officer (DPO) The DPO operates with independence and is staffed by suitability skilled individuals granted all necessary authority. The DPO reports directly to Altodigital's SIRO, Duties of the DPO include:

- Monitoring compliance with the GDPR and other data protection laws, Altodigital's data protection policies, awareness-raising, training, and audits.
- To inform and advise the controller and processor and employees who carry out processing of their obligations pursuant to GDPR and to other data protection provisions.
- Providing guidance pertaining to carrying out Data Protection Impact Assessments (DPIAs);
- Acting as a point of contact for and cooperating with Data Protection authorities (DPAs)
- Informing senior manager, officers, and directors of Altodigital of any potential corporate, civil and criminal penalties which may be levied against Altodigital and/or its employees for violation of applicable Data Protection laws.

5.1.2 Policy Dissemination & Enforcement

The Altodigital management team are committed to ensuring that all Altodigital 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.

5.1.3 Data protection by Design

Under the GDPR, Altodigital have an obligation to implement technical and organisational measures to show that data protection has been considered and integrated into processing activities. To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

Each Altodigital entity must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in conjunction with the DPO, for all new and/or revised systems or processes for which is has responsibility. The subsequent findings of the DPIA must then be submitted to the SIRO or delegated individual for review and approval. Where applicable, the Information Technology department, as part of its IT system and application design review process, will cooperate with the DPO to assess the impact of any new technology uses on the security of personal data.

5.1.4 Compliance Monitoring

To confirm that an acceptable level of compliance is being achieved by all Altodigital entities in relation to this policy, the DPO will carry out an annual Data Protection compliance audit for all such entities, including any Third Parties. Each audit should, as a minimum, assess:

- Compliance with Policy in relation to the protection of personal data, including:
  - The assignment of responsibilities
  - Raising awareness
  - Training employees
- The effectiveness of Data Protection related operational practices, including:
  - Data Subject rights.
  - Personal Data transfers.
  - Personal Data incident management.
  - Personal Data complaints handling.
- The level of understanding of Data protection policies and Privacy Notices.
- The currency of Data Protection policies and Privacy Notices.
- The accuracy of personal data being stored.
- The conformity of Data Processor activities.
- The adequacy of procedures for redressing poor compliance and personal data Breaches.

The DPO, in conjunction with key business stakeholders from Altodigital, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any critical deficiencies identified will be reported to and monitored by the Altodigital Executive Management team.

5.2 Data Protection Principles

Altodigital have adopted the following key principles as set out in GDPR to govern its collection, use, retention, transfer, disclosure and destruction of personal data:

- **Principle 1: Lawfulness, Fairness and Transparency** – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means, Altodigital must inform the data subject what processing will occur (transparency), the processing must match the description given to the data subject (fairness), and it must be for one of the purposes specified in the applicable data Protection regulation (lawfulness).
- **Principle 2: Purpose Limitation** – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. For Altodigital, this means that it must be specified exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.
- **Principle 3: Data Minimalisation** – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Altodigital must only store personal data which is absolutely required.
- **Principle 4: Accuracy** – Personal data shall be accurate and, where necessary, kept up to date. This means that every reasonable step must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- **Principle 5: Storage Limitation** – Personal Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Altodigital must, wherever possible, store personal data in a way that restricts or prevents identification of the data subject.

- **Principle 6**: **Integrity & Confidentiality** – Personal Data shall be Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. Altodigital must use adequate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.
- **Principle 7: Accountability** – The Data Controller shall be responsible for, and be able to demonstrate compliance. Altodigital must demonstrate that the six Data Protection Principles (outlined above) are adhered to for all personal data for which it is responsible.

5.3 Data Collection

5.3.1 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 in order 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 then:

- 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.

5.3.2 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.
- Providing a simple method for a data subject to withdraw their consent at any time.

5.3.3 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 advanced by the DPO. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

5.4 Data Use

5.4.1 Processing

Altodigital uses the personal data of its contacts for the following purposes:

- The general running and business administration of Altodigital.
- To enable Altodigital to provide services to its customers.
- The ongoing administration and management of customer services.

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 or in order 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 making a determination 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.

In the event 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 have 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.

5.4.2 Special Categories of Data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

The above does not apply, if one of the following applies:

- The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject.
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically of legally incapable of giving consent.
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.
- processing relates to personal data which are manifestly made public by the data subject.
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

5.4.3 Children's Data

Due to the nature of Altodigital's business there are occasions where it handles the Personal Data of children. Children are unable to consent to the processing of personal data. Consent must be sought from the person who holds parental responsibility over the child.

5.4.4 Data Quality

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.
- Ensuing the removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required.

5.5 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.

5.6 Data Protection

Altodigital shall adopt physical, technical, and organisational measures to ensure the security of personal data. 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 are processed
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that 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 there is a system for maintaining accountability is in place. This means access logs are used to establish whether, and by whom the personal data was entered into, modified on or removed from a data processing system.
- 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.

5.7 Data Subject Requests

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

- Information Access
- Objection to Processing
- Objection to automated decision-making and profiling
- Restriction of Processing
- Data Portability
- Data Rectification
- Data Erasure

Based upon a written request to the DPO 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 may be necessary or appropriate to protect that person's rights.

5.8 Law Enforcement Requests

In rare circumstances, it is permitted that personal data be shared without the knowledge or consent of a data subject. These are the cases where the disclosure of the personal data is necessary:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

5.9 Training

All Altodigital employees that have access to personal data will have their responsibilities under this policy outlined to them as part of their induction training. Additionally, Altodigital will provide regular data protection training and procedural guidance for their staff.

The training and procedural guidance set forth will consist of, at a minimum, the following elements:

- The GDPR data protection principles outlined in Section 5.2 above.
- Each employee's duty to use and permit the use of personal data only by authorised persons and for authorised purposes.
- The need for, and proper use of, the forms and procedures adopted to implement this policy.
- The correct use of passwords, security tokens and other access mechanisms.
- The importance of limiting access to personal data, by adopting a clear screen/clear desk policy.
- Securely storing paper files, printouts and electronic storage media.
- Proper disposal of personal data by using secure shredding facilities.

5.10 Data 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 approved transfer mechanism must be 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.

5.10.1 Internal Transfers

In order 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, you 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 particular 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).

5.10.2 Third Party Transfers

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 transferred.

Where the Third Party is deemed to be a data processor, Altodigital will enter into, in cooperation with the DPO, 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 events where Altodigital is outsourcing services to a Third Party, they 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 in respect of technical and organisational measures they have in place.

5.11 Complaints Handling

Data subjects with a complaint about the processing of their personal data, should put forward the matter in writing to the DPO/ISM. A full investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The DPO will inform the data subject of the progress and outcomes of the complaint within a reasonable period.

5.12 Breach Reporting

The GDPR introduces a responsibility on all organisations to report certain types of personal data breaches to the relevant supervisory authority. This must be done within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

Altodigital must also keep a record of any personal data breaches, regardless of whether you are required to notify.

5.13 Non-conformance

Non-conformance to this policy could mean Altodigital fail to comply with the GDPR requirements. There are strict fines failing to comply with GDPR, the tiers are as follows:

- **Lower** – Up to €10 million, or 2% of the worldwide annual revenue of the prior financial year, whichever is higher.
- **Upper** – Up to €20 million, or 4% of the worldwide annual revenue of the prior financial year, whichever is higher.

6 Glossary

Data Controller	A legal person, Public Authority, Agency or organisation which, determines the purposes and means of the processing of personal data.
Data Processors	A legal person, Public Authority, Agency or organisation, which processes personal data on behalf of a data controller.
Data Subject	The identified or identifiable natural person to which the data refers.
Identifiable Natural Person	Anyone who can be identified, directly or indirectly.
Personal Data	Any information which relates to an identified or identifiable natural person.
Third Party	An external organisation with which Altodigital conducts business and is also authorised to, under the direct authority Altodigital, process the personal data of Altodigital customers.