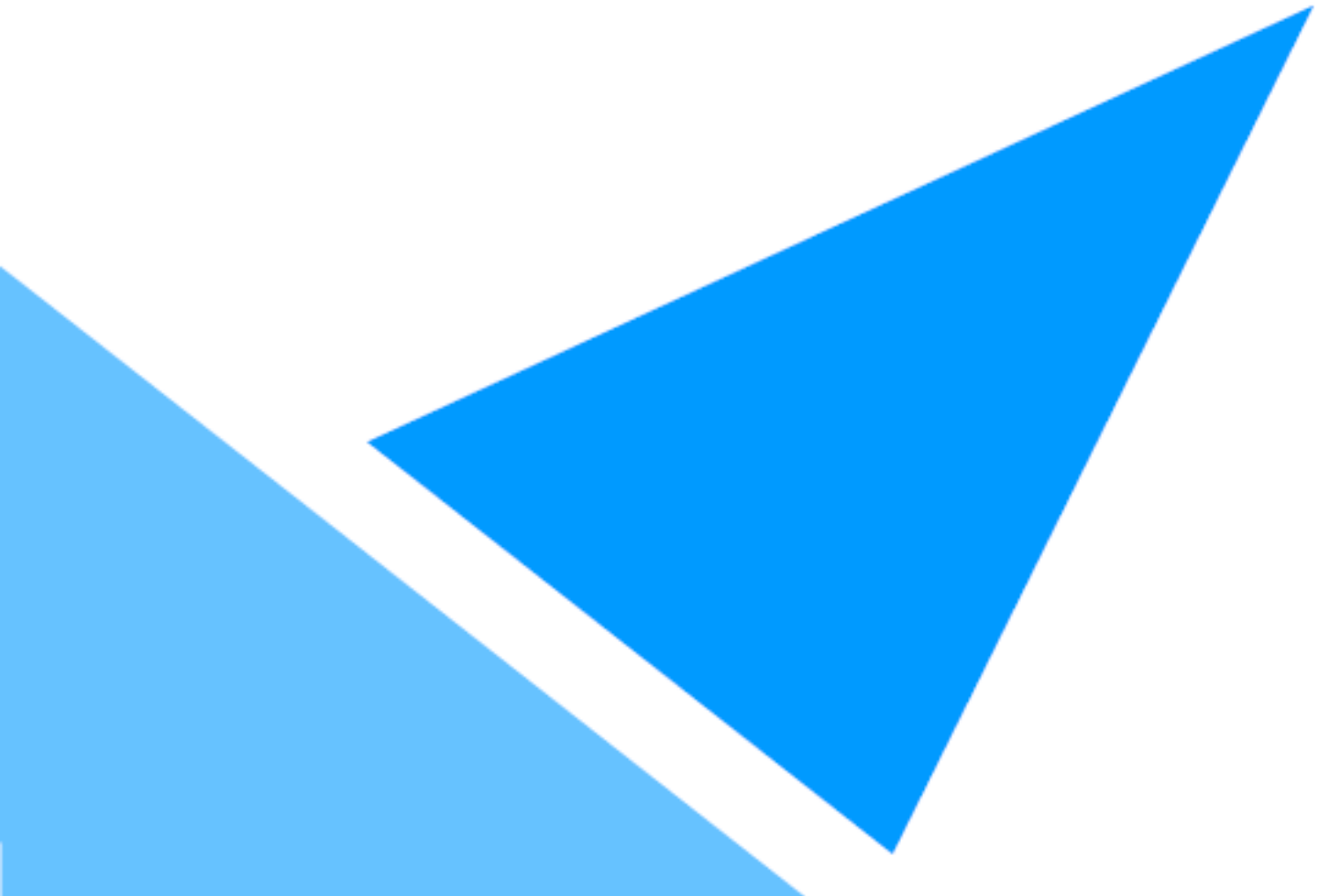
ATAMIS

Data Protection Policy

v1.8

Updated 06 January 2025



Contents

Revision History

Version	Date	Summary of Main Changes
1.2	18/05/2018	Re-formatted and restructured with additional sections
1.3	23/05/2018	Updated DPO contact details
1.4	25/05/2018	Added revision history and additional content for client specific GDPR variations.
1.5	23/09/2019	Contact details updated
1.6	30/09/2020	Contact details updated
1.7	25/01/2023	DPO Changed

Introduction

Atamis is committed to protecting the rights and freedoms of data subjects and safely processing their data in accordance with all of our legal obligations.

Atamis ("we") need to keep certain information about individuals to allow it certain legitimate business purposes, which include some or all of the following:

- Where the processing enables us to deliver, enhance, modify, personalise or otherwise improve our services / communications for the benefit of our customers.
- To meet the needs of legal and contractually binding arrangements.
- To enhance the security of our network and information systems.
- To better understand how people use and / or interact with our site and / or services.
- To provide postal communications which we believe will be of interest to you.
- To determine the effectiveness of promotional campaigns and advertising.
- To ensure unwanted marketing / communications are not continued.

We also need to process information so that legal obligations to clients and regulatory bodies are complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, we must comply with the Data Protection Principles, which are set out in the General Data Protection Regulations ("GDPRs").

In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes. Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose. Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Compliance and Accountability

Atamis processes all data fairly and lawfully, and in compliance with the GDPRs, is the responsibility of all members of Atamis. Any deliberate breach of this data protection policy may lead to disciplinary actions being taken, or even criminal prosecution. Likewise, the deliberate overlooking of a breach is to be considered a breach in itself. If you feel that at any point a breach has occurred, please raise it with the Data Protection Officer named in this document in a timely manner.

Where we act as controller, appropriate technical and organisational measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (where reasonably able to). We have a legal obligation to inform any data subjects we process as controller of any breaches to their personal data.

To comply with data protection laws and the accountability and transparency Principle of GDPRs, we must demonstrate compliance in the following areas:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conducting Data Protection Impact Assessments
- Implement measures to ensure privacy by design and default, including:

Additional compliance for the following areas:

- Data minimisation
- Pseudonymisation
- Transparency
- Allowing individuals to monitor processing.
- Creating and improving security and enhanced privacy procedures on an ongoing basis

Subject Consent & Retention of Data

Atamis acts in a data processor capacity for any data conferred to us by clients and processes data as such. We may obtain additional data to enrich this data through a variety of sources and activities outlined in our service level agreement and in accordance with the law. As a data processor we have a legal obligation to notify any controllers we act on behalf of in the event of any personal data breaches or permanent data loss. If you feel that this affects you in any way or would like to know more about the processes used, please contact the relevant body acting as data controller. As processor, we shall not retain any sensitive or identifying data provided to us for longer than justifiable outside of our contractual obligations. Once contractual obligations have been met, we retain the right to delete and destroy copies of data we have been passed without due notification to the data controller, thereby ending our role as data processor. We retain the right to maintain any records or data we have enriched at our own expense, when such records cannot be linked solely to one client.

Where we have obtained data ourselves, Atamis as a corporate body is the controller, and is therefore ultimately responsible for implementation. However, as is required, Atamis has designated Mr Mark Corbisiero to act as Data Protection Officer, who can be contacted at the address provided at the foot of this document. Atamis maintains our appropriate registration with the Information Commissioners Office in order to continue lawfully controlling and processing data.

Where we act as controller, every (reasonable) effort will be made to ensure that personal data we store is kept up to date and accurate and that express consent is given. Data which has been unmodified will be kept for two years and removed via a quarterly process. Modification of personal data through written forms or through verbal communication will be considered reaffirmation of any initial explicit consent and as a result will reset the two-year retention time.

Where data is stored on a data subject for contractual reasons, consent is implied through necessity and will be considered a legitimate commercial interest for both parties. Where this is the case, it will be clearly marked on any record that this is the case. It will also extend any retention periods indefinitely for the minimum of duration of any contractual periods where this time exceeds any other mentioned retention period.

Personal data will not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Unsubscribing from our mailing list will not automatically qualify your data for removal from any databases we maintain, rather a skeletal record will be retained which will include information necessary to conform with your wishes relating to marketing. This falls under the GDPR's right to restrict data, where, unless instructed otherwise, we must retain enough data to ensure the right to restriction is respected in the future.

Rights to Access/Modify Data

You have the right to access any personal data and accompanying supplementary data that is being kept about you either on computer or in certain files. You also have the right to information pertaining to the method in which such data is processed in the interest of verifying the lawfulness of the processing activities. Any person who wishes to exercise this right should contact Atamis support, in writing or via email. As per the conditions laid out by the GDPR we retain the right to refuse or charge for this on each occasion that access is requested, and subject to positive validation of identity of the data subject. We must provide any and all data in a commonly used, machine-readable format, and, where requested, send it directly to another controller if requested.

We aim to comply with requests for access to personal information as quickly as possible within three months of receipt but will aim to fulfill any request within one month.

You have the right to rectification, and we must amend the personal data of an individual if requested because it is inaccurate or incomplete. This must be done without delay, and within one month. This can be extended to two months where permission from the DPO is given.

You have the right at any time to request any and all data pertaining to you to be deleted if there is no compelling reason for its continued processing, however, this may result in you being re-added to our mailing lists from other sources. This right is separate from an individual's right to object, which states we must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task. We must respect the right of an individual to object to direct marketing, including profiling. We must also respect the right of an individual to object to processing their data for scientific and historical research and statistics.

We must comply with any request to restrict, block, or otherwise suppress the processing of personal data. We are permitted to store personal data if it has been restricted, but not process it further, retaining enough data to ensure any restriction requests are respected in the future.

Additional rights of the individual

Additionally, individuals have the right to be informed (through the provision of privacy notices) how we use personal data. Individuals also have the right, in relation to any automated decision making or profiling process, to have these processes explained, object to them, and to request human intervention.

Special categories

Previously known as sensitive personal data, this data requires additional protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example putting them at risk of unlawful discrimination, and pertains to things such as race, religion or sexual orientation. We do not process any special category data other than gender through the implied medium of "title".

If such an occasion should arise where we would need to store anything which could be categorised as a "special category", we shall, where needed, request additional explicit consent to do so as required by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

Responsibilities

Our Responsibilities

We have the following additional responsibilities in both a processor and controller capacity:

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised

Your Responsibilities

The following are responsibilities for all data subjects:

- Fully understand your data protection obligations
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions.
- Comply with this policy at all times.
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay.

Responsibilities of the Data Protection Officer

The following are responsibilities for the assigned Data Protection Officer:

- Keeping all relevant stakeholders updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and policies on a regular basis.
- Arranging data protection training and advice for all staff members and those included in this policy (where reasonable to do so).
- Answering questions on data protection from staff, board members and other stakeholders.
- Responding to individuals such as clients and employees who wish to know which data is being held on them by us.
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing.

Responsibilities of the IT Manager

The following are responsibilities for the IT Manager:

- Ensure all systems, services, software and equipment meet acceptable security standards.
- Checking and scanning security hardware and software regularly to ensure it is functioning properly.
- Researching third-party services, such as cloud services the company is considering using to store or process data.

Responsibilities of the Marketing Manager

The following are responsibilities for the Marketing Manager:

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy.

Data Protection Schedule

Description	Details
Business Purposes	The purposes for which personal data may be used by us can include personnel, administrative, financial, regulatory, payroll and business development purposes, shown by the following examples : Processing to deliver, enhance, modify, personalise or otherwise improve our services / communications for the benefit of our customers. To enhance the security of our network and information systems. To better understand how people use and / or interact with our site and / or services. To provide customised postal communications and to then determine the effectiveness of promotional/marketing campaigns and advertising. To ensure unwanted marketing / communications are not continued. To ensure business policies are adhered to (such as internet use). Monitoring staff conduct, disciplinary matters Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting and the investigation of complaints
Personal Data	'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. *Personal data we gather may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.*

	The names and work email addresses of system users and former system users are stored for the purpose of validating user access to the system and attribution of changes/edits to the system. *Personal data may be uploaded to the system if it forms part of supplier or expenditure information provided to Atamis as part of the SA Spend Analysis service or within the context of our other module based services. This data might include individual's names (for example where such names are part of supplier names or where individuals are named within expenditure details) and postcodes (for example the trading address of the supplier).*
Special categories of personal data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offenses, or related proceedings, and genetic and biometric information —any use of special categories of personal data should be strictly controlled in accordance with this policy. Atamis does not typically hold special categories of personal data on individuals.
Data controller	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office.
Skeletal record	Atamis will store email addresses of any persons unsubscribed from our mailing lists to ensure they are not re-added. These records may include limited personally identifying data.
Categories of Data Subject	Atamis employees, data provided by Clients (including additional data appended through research), supplier data, website cookie data, system users information (including log in times and locations), business leads and opportunities are all categories of data stored and processed by Atamis.
Type of Personal Data	Due to the multifaceted nature of our data storage requirements types of data stored will be varied depending on what area of the business needs it is used for. Typically, personal data includes names, email addresses and the organization an individual works for. Additional information may be stored, such as phone number and/or postal address.

Reporting breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. Atamis has a legal obligation to report any data breaches to the Information Commissioners Office within 72 hours.

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

DPO Contact Details

Mr Mark Cobisiero

Atamis Limited
South Gate House
Wood Street
Cardiff
CF10 1EW

T: 029 2079 0052

- email: mark.corbisiero@atamis.co.uk