



---

## Data Protection Policy

## **Statement from Executive Management Team**

Axiomatic has a long and proud tradition of conducting business in accordance with the highest ethical standards and in full compliance with all applicable laws. The Data Protection Policy was developed at the direction of Axiomatic Executive Management to provide clear guidance to all Axiomatic employees and to ensure a consistent approach to business practices throughout Axiomatic expanding operations.

Axiomatic Executive Management is fully committed to conduct business with the highest level of integrity and we expect your strict adherence to the Data Protection Policy and the law. There will be zero tolerance of non-compliance and any violations will result in swift corrective action, including possible termination of employment from Axiomatic Consultants.

Thank you for your commitment to comply unequivocally with the highest standards of integrity and business ethics.



## **Introduction**

Axiomatic provides payroll and various related services, including consulting, to its clients both locally and worldwide.

Inherent in the provision of these services to its clients, as well as the management of its employment relationships with its own “employees” (both permanent and on various types of contracts), Axiomatic continually has access to and needs to process personal data and information relating to individuals.

This policy sets out how such personal data shall be processed, handled and stored to meet the data protection standards of Axiomatic and to comply with the legal standards governing its clients as well as future legislation which may be enacted into law in South Africa in the foreseeable future.

This Data Protection Policy seeks to ensure that Axiomatic:

- Complies with international legal standards and best practice for the receipt, importing, processing, handling and storing of personal data of individuals (“data subjects”), both as received from its clients, and as held in respect of its own employees;
- Protects the rights of its own employees, as well as that of its clients and third parties in respect of individuals’ data;
- Transparently renders how it process, handles and stores individuals’ data;
- Protects itself from the risks of a data breach.

## **Legislative Environment**

This policy seeks to align best practice in Axiomatic with legal standards governing its clients, including Article 26(2) of Directive 95/46/EC, as well as the Protection of Personal Information Act (“POPI”) anticipated to be enacted into law in South Africa in the foreseeable future.

In doing so, it is acknowledged that Axiomatic does not collect or gather data from its clients, but receives and/or imports data from clients to enable Axiomatic to providing services. Axiomatic does however, collect or gather data from its own employees for various purposes related to human resources and employment benefit administration.

## **Scope**

### **Application**

This policy applies to all employees of Axiomatic in respect of all personal data accessed in the provision of services by Axiomatic to its clients, as well as the management of its employment relationships with its own employees.

It further applies to all data that it holds relating to identifiable individuals, including, but not limited to the following:

names of individuals; physical addresses; postal addresses; email details; all telephone and mobile phone numbers; all social media tags and identifiers; absolutely all data and information relating to an individual received from a client in the course of providing services to such client, and/or all data of a data subject protected for the benefit of such individual in terms of POPI, or sought to be protected by the latter statute.



## **Protection**

This policy seeks to protect Axiomatic from various very real data security risks including;

Breaches of confidentiality through data breaches, hacking risks, and the risks of liability in relation to its clients, third parties data acquired from such clients and all its own employees.

The rules and standards set out in this policy applies regardless of –

- whether personal data relates to a client or an employee of Axiomatic, and/or
- is stored electronically, digitally, on paper, or on other materials, or through other methods.

## **General rules relating to Personal Data**

Personal data shall at all times be:

- processed fairly and lawfully, in accordance with legal standards applicable to such data or data categories;
- obtained only for specific lawful purposes;
- adequate, relevant and not excessive;
- accurate, and kept up to date;
- held for no longer than necessary for the purpose it was obtained for;
- processed in accordance with the rights of data subjects;
- be protected in appropriate ways, methodologies and procedures and according to suitable methods, both organisationally and technologically;
- not be disclosed or transferred or exported illegally, or in breach of any agreement with a client.

## **Responsible Parties**

All employees shall continually be responsible for ensuring the safeguarding, protection and avoidance of any unauthorised disclosure or breach of data personal data in the execution of employment duties and services to Axiomatic, or otherwise in the course of rendering services or being associated with the company.

## **The Risk and Compliance Manager**

The Risk and Compliance Manager shall –

- in time be registered as the responsible officer under POPI, once enacted in South Africa;
- execute, and bear responsibility for reporting to executive management about compliance with all technological and operational data protection standards and protocols, and advise of any risk of breach at the earliest opportunity with a view to avoiding any risk or breach, or limiting any damage resulting from it. To ensure compliance with this provision, a Breach Notification Form must be completed by any employee of Axiomatic who becomes aware of any breach /or possible breach;
- ensure that all operational and technological data protection standards are complied with;
- arrange data protection training and provide advice and guidance to all employees;



- be entitled and have authorisation to initiate disciplinary proceedings against any employee who at any time breaches any technological and/or organisational and/or operational data protection standard, rule, custom, instruction, policy, practice and/or protocol (verbal, in writing or otherwise) (“rule”) applicable in any department or area of the operations of the company;
- review and approve any contracts or agreements with third parties to the extent that they may handle or process data subject information;
- attend to requests from individuals to access data Axiomatic holds about them “data subject requests”).

### **The IT Manager (External IT Service Provider)**

The IT Manager shall –

- ensure that all systems services and equipment used for processing and/or storing data adhere to internationally acceptable standards of security and data safeguarding, and is regularly updated to continue to comply with such standards;
- issue appropriate, clear, regular rules and directives, whether for the organisation as a whole or a particular part of it, department, person or level of person in relation to any aspect of the company’s work, including password protocols, data access protocols, levels of persons who enjoy access to certain data sign-on procedures, password safeguarding protocols, sign-on and sign-off procedures, log-on and log-off procedures; the description of accessories, applications and equipment that will or may be used, and/or that may not be used under any circumstances, and the like.
- evaluate any third-party services the company is considering or may acquire to process or store data, e.g. cloud computing services.

**Note:** It is acknowledged that these rules, directives and protocols are in themselves operationally confidential and to the company and organisation, and may be adjusted or changed at any time whether verbally or otherwise for a particular individual or group of individuals or the company as a whole, in order to ensure an adaptive, responsive, efficient functional IT management system which serves the requirements and risks of Axiomatic and all its clients and employees. For this reason, it is confirmed that not all such rules, directives and protocols will be captured in writing, as it may undermine or impair the afforested goals, if should this be the case.

### **General Data Protection Rules**

All personal data shall be deemed confidential information, and be handled as such.

The only person/s entitled to access data covered by this policy, will be those who need to access it for the execution of their direct work services or required outputs.

Under no circumstances will data or personal information be shared outside the scope of required work outputs, or informally. In the event of any doubt, an employee shall be entitled to access confidential information only after obtaining authorisation from their line manager or a senior manager, where any work output requiring access is unusual or out of the ordinary.

Employees will receive induction and on-the-job training in relation to all security standards applicable to such employee’s service delivery and work outputs involving personal information of data subjects.



Employees shall keep all data secure by taking sensible practical precautions and complying with all rules, practices and protocols:

- In particular, strong passwords shall be used at all times;
- Passwords shall not be shared under any circumstances;

**Note:** In the exceptional circumstance that a password may require to be shared, it shall only take place after explicit, provable authorisation has been procured from a senior manager or line manager before sharing it, and then only for the stated purpose. All necessary steps shall be taken after a password has been shared in such exceptional circumstances, to reset it to a strong, unique password to avoid future data compromise or breach.

## **Data Storage**

### **Paper**

Where data is stored on paper, it will always be kept in a secure place where an unauthorised person cannot access or see it. This also applies to data stored electronically which has been printed out for some reason.

When not required by such papers should be kept in a locked drawer, safe or cabinet.

Employees should ensure that paper and print outs are not left in places where unauthorised persons can see them, e.g. on a printer, and all unwanted paper must be shredded.

### **Electronic data**

Where data is stored electronically, it must be protected from unauthorised access, accidental deletion or any risk of exposure to malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees;
- Where data is stored on removable media such as a CD or a DVD these must at all times be locked away securely when not in immediate use;
- All data will only be stored on designated drives and servers and shall only be uploaded to approved cloud computing services;
- All servers containing personal data will be located in secure protected locations away from general office space;
- Data will be backed up frequently in accordance with backup protocols. Such backups will be tested regularly in line with the company's standard backup procedures and protocols under the direction of the IT Manager. The Risk and Compliance Manager will be responsible to schedule a minimum of two random tests each year;
- Data will never be saved directly to laptops or other mobile or removable devices such as tablets or smart phones or sticks or data sticks;
- All servers and computers containing data will be protected by approved security software, and one or more firewalls under the direction of the IT Manager.



## **Data Use**

It is acknowledged that personal data is at the greatest risk of loss, breach of confidentiality, corruption, hacking or theft when it is accessed or used. Therefore when working with personal data, employees should ensure that screens of their computers are always locked when left unattended;

Personal data will not be shared informally, and in particular it will never be sent by email or without protection with appropriate passwords, where required to be sent by email;

Data shall be encrypted before being transferred electronically. The IT manager together with the Risk Manager will develop and maintain protocols for data transfer to ensure it is sent in protected form to authorised external contacts only, and to avoid it being sent to any unauthorised external or internal parties;

Personal data shall never be transferred or sent to any entity not authorised directly to receive it;

Employees are prohibited from saving copies of personal data to their own computers;

Employees will at all times access and update only the central, official copy of any data or work output document, such as payroll.

Personal data is not of value to Axiomatic, unless the business makes use of it in the course of providing services to its clients, or administering its own employment relationships with employees.

## **Data Accuracy**

Employees shall take reasonable steps to comply with company rules and work practices to ensure data is kept accurate and up-to-date;

The more important the accuracy of any component of personal data is, the greater the effort and measures will be to ensure its accuracy;

Data will always be held in as few places as necessary to ensure efficient service delivery and risk avoidance. Employees are not permitted to create any unnecessary additional data sets;

Employees will make use of every opportunity to ensure that a data component is accurate and up-to-date, e.g. by confirming details when handling a client call.

Employees shall at all times remain knowledgeable and informed about all data updating practices and work protocols used by Axiomatic, such as updating via official, acknowledged websites and platforms used by clients.

## **Data Subject Access Requests**

Where an employee or individual who is entitled to it contacts the company requesting his/her personal information, it is called a "subject access request".

Employees and individuals who are the subject of personal data held by Axiomatic are entitled to:

- enquire what information is held about them and the purpose for holding it;
- enquire how to gain access to their own personal data;
- be informed of any special measures the company uses to keep such data up to date.



Subject Access Requests shall be made by e-mail and addressed to the Risk and Compliance Manager, who shall address it in consultation with management.

The identity of a person making a data subject request will always be verified before handing over any information requested.

### **Providing Information**

In certain circumstances, South African legislation will allow that personal data be disclosed to law enforcement or other agencies without the consent of the data subject. In such circumstance, Axiomatic may be obliged to disclose the requested data, but will first ensure that the request is legitimate and will seek assistance beforehand from its legal advisers or other experts. Only the Risk and Compliance Officer will be authorised to furnish the requested data to the enquiring party.

### **Disciplinary Code and Incorporation of this Policy into the Employee's Employment Contract**

This data protection policy governs every employee of Axiomatic, both during the course of his/her services to it, and to the extent applicable, after termination of services.

To the extent that this policy sets out workplace rules (as defined) governing the employee in the course of his/her work and services to the company, it shall form part of the company's Disciplinary Code and Procedure and is hereby also incorporated into it.

A breach of any rule in relation to the protection of personal data set out in this policy shall, in the event of breach thereof, form the basis of disciplinary action. In appropriate circumstances a breach hereof proven in a disciplinary enquiry may lead to dismissal.

The imposition of any disciplinary sanction or dismissal shall not preclude the company from instituting civil proceedings against an employee who acted in breach of this policy where such breach has resulted in liability, loss, reputational damage and/or other damages to the company in the course of pursuing its commercial operations.

**[Note:** It shall be incumbent upon every employee to familiarise him/herself with the content of this policy, and to remain up to date as to any changes to it issued in written form as part hereof by the company.]

