



# Osirian Consulting Limited

## Data Protection Policy

For Employees, Workers and Consultants

This Policy will be subject to change and updating from time to time and the Company reserves the right to make unilateral changes. Any alterations or changes will be communicated to you by the **Data Protection Manager** and if you require any clarification of the terms of this policy you should contact the **Data Protection Manager**.

### Policy Approval

The **Data Protection Policy** is issued with the approval and support of the Managing Director and the Data Protection Manager.

The **Data Protection Manager** (DPM) has been empowered to act on behalf of the Managing Director and has been delegated direct responsibility for ensuring adherence to the Policy by all staff, elected members, contractors, associates and any third parties using the Company's systems.

The viewer of this document should be aware that this physical copy may not be the latest version. The latest version, which supersedes all previous versions, is available from the **DPM**.

## 1. Introduction

We, the Company, take the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the **Data Protection Act 2018** (the 'DPA') and the **EU General Data Protection Regulation** ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

If you require any clarification of the terms of this policy, whether information amounts to personal data and or whether certain actions amount to processing within the meaning of the Data Protection Act, you should contact the **DPM**.

Although the Data Protection Act is specific to the UK, the principles apply to the European jurisdiction and are a benchmark for complying with contractual obligations in international jurisdictions.

We will comply with the **Six Data Protection Principles** which, in summary, state that personal data must:

- be processed fairly, lawfully and transparently
- be collected and processed only for specified, explicit and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed
- be accurate and kept up to date – any inaccurate data must be deleted or rectified without delay
- not be kept for longer than is necessary for the purposes for which it is processed
- be processed securely

We are accountable for these principles and must be able to show that we are compliant. **The Company** and all staff who process any personal information about other people must ensure that they comply with this Data Protection Policy. Knowingly or recklessly disclosing the personal data of

Document id:	Osirian Consulting Ltd – Data Protection Policy	Page 1 of 12
Version:	V3	Confidential Information
Issued:	08/04/2025	Document Owner: Rachael Lee

others without the express consent of the Company can constitute a criminal offence.

## 2. Scope of Policy

This Policy will be subject to change and updating from time to time. Any alterations will be communicated to you by us.

This policy applies to current and former employees, workers, volunteers, apprentices and consultants. If you fall into one of these categories, then you are a **'data subject'** for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data. This policy does not, however, form part of your contract of employment (or contract for services if relevant) and can be amended at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the Company intends to comply with the DPA and the GDPR.

This policy document covers the processing of personal data (i.e. information about natural living persons) whose use is controlled by the Company, as the **Data Controller**, and defined in the Company's Data Protection Notification Registration No. It applies to all staff, whether employed or otherwise engaged including volunteers, who process data on behalf of the Company. Personal data applies to both computer and manual records. Any breach of the Act or failure to follow this Data Protection Policy may, therefore, result in disciplinary action being taken.

## 3. Purpose of Policy

We are committed to protecting the rights and privacy of individuals in accordance with the Data Protection Act, currently in force, to which the Company is subject as a controller and processor of personal data ("**data controller**"). We need to process information about its staff and other individuals ("**data subjects**") for example to monitor performance, for the recruitment process, pay, health and safety and various legal obligations. Such information must be collected and used fairly, stored safely and not disclosed unlawfully.

## 4. Definitions

### 4.1 How we define personal data

**'Personal data'** means information which relates to a living person who can be identified from that data (a "data subject") on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person, including personal references taken at time of hire, and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

### 4.2 How we define special categories of personal data

**'Special categories of personal data'** are types of personal data consisting of information as to:

- your racial or ethnic origin

Document id:	Osirian Consulting Ltd – Data Protection Policy	Page 2 of 12
Version:	V3	Confidential Information
Issued:	08/04/2025	Document Owner: Rachael Lee

- your political opinions
- your religious or philosophical beliefs
- your trade union membership
- your genetic or biometric data
- your health
- your sex life and sexual orientation
- any criminal convictions and offences

We may hold and use any of these special categories of your personal data in accordance with the law.

#### 4.3 How we define processing

**'Processing'** means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage
- adaption or alteration
- retrieval, consultation or use
- disclosure by transmission, dissemination or otherwise making available
- alignment or combination
- restriction, destruction or erasure

This includes processing personal data which forms part of a filing system and any automated processing.

## 5. Processing Data

### 5.1 Personal Data

We will process your personal data (including special categories of personal data) in accordance with our obligations under the DPA.

We will use your personal data for:

- performing the contract of employment (or services) between us
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights below.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data, you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

We also record incoming and outgoing telephone calls for training and quality purposes, recordings may include your personal data.

Document id:	Osirian Consulting Ltd – Data Protection Policy	Page 3 of 12
Version:	V3	Confidential Information
Issued:	08/04/2025	Document Owner: Rachael Lee

## 5.2 Examples of when we might process your personal data

We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

For example (the bullet points with an \* are defined in clause 5.6 below):

- to decide whether to employ (or engage) you
- to decide how much to pay you, and the other terms of your contract with us
- to check you have the legal right to work for us
- to carry out the contract between us including where relevant, its termination
- training you and reviewing your performance\*
- to decide whether to promote you
- to decide whether and how to manage your performance, absence or conduct\*
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability\*
- to monitor diversity and equal opportunities\*;
- to monitor and protect the security (including network security) of the Company, of you, our other staff, customers and others
- to monitor and protect the health and safety of you, our other staff, customers and third parties\*
- to pay you and provide pension and other benefits in accordance with the contract between us\*
- paying tax and national insurance
- to provide a reference upon request from another employer
- to pay trade union subscriptions\*
- monitoring compliance by you, us and others with our policies and our contractual obligations\*
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us\*
- to answer questions from insurers in respect of any insurance policies which relate to you\*
- running our business and planning for the future
- the prevention and detection of fraud or other criminal offences
- to defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure\*
- for any other reason which we may notify you of from time to time

We also record incoming and outgoing telephone calls to assist in training our staff and to monitor quality of information provided, such recordings may include your personal data.

## 5.3 Special Category Data

We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data, then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting the **DPM**.

Document id:	Osirian Consulting Ltd – Data Protection Policy	Page 4 of 12
Version:	V3	Confidential Information
Issued:	08/04/2025	Document Owner: Rachael Lee

5.4 We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent
- where you have made the data public
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity

5.5 [Intentionally deleted]

5.6 We might process special categories of your personal data for the purposes in paragraph 5.4 above which have an asterisk beside them. In particular, we will use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety
- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members

We do not take automated decisions about you using your personal data or use profiling in relation to you.

### 5.7 Sharing your personal data

Sometimes we might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

Third Party companies that we share your data with include, but are not limited to:

Company	DPA Registration No.	Reason for sharing personal data
JC Payroll Services Ltd	Z9344736	Payroll processing, including tax and NI payments to HMRC
Johnson Fleming Services Ltd	ZA031356	Employee pension processing
Pennymatters Ltd	Z3183135	Medical insurance and Life Assurance (DiS)
M12 Solutions Ltd	Z1783240	Call recordings
VCI Systems Ltd		Access PC etc
HMRC		P11d, auditing, PAYE

We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be

explained.

### 5.8 How should you process personal data for the Company?

Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company’s Information Security and Data Retention policies, where applicable.

The Company’s **DPM** is responsible for reviewing this policy and updating the Managing Director on our data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

- You should not share personal data informally
- You should keep personal data secure and not share it with unauthorised people
- You should regularly review and update personal data which you have to deal with for work – this includes telling us if your own contact details change
- You should not make unnecessary copies of personal data and should keep and dispose of any copies securely
- You should use strong passwords
- You should lock your computer screens when not at your desk
- Personal data should be encrypted before being transferred electronically to authorised external contacts. [Speak to IT for more information on how to do this.]
- Consider anonymising data or using separate keys/codes so that the data subject cannot be identified
- Do not save personal data to your own personal computers or other devices
- Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the **DPM**
- You should lock drawers and filing cabinets – do not leave paper with personal data lying about.
- You should not take personal data away from Company’s premises without authorisation from your line manager or **DPM**
- Personal data should be shredded and disposed of securely when you have finished with it
- You should ask for help from our **DPM** if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon
- Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.
- It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

## 6. Maintaining Records

The Company will take all reasonable steps and regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- IT systems will be designed, where possible, to encourage and facilitate the entry of accurate data
- Data on any individual will be held in as few places as necessary and all staff will be discouraged from establishing unnecessary additional data sets

Document id:	Osirian Consulting Ltd – Data Protection Policy	Page 6 of 12
Version:	V3	Confidential Information
Issued:	08/04/2025	Document Owner: Rachael Lee

- Effective procedures will be in place so that all relevant systems are updated when information about any individual changes.
- Out of date information or information that is no longer required will be deleted by the Company on a regular basis
- Staff who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping

To ensure accuracy the Company will ask you periodically to check that your personal information held by the Company is correct. You should always contact the **DPM** should your personal information change for any reason, for example a change of surname, home address or telephone number.

## 7. Sickness & Health Records

For day-to-day management the Company needs to keep records relating to the personal sickness and health records of each member of staff. Such personal data will record any periods of sickness or health matters, detailing the length and nature of the issue and the outcome. These records will be used to assess the health and welfare of members of staff and to highlight any issues that may require further investigation.

Such data will only be disclosed to management and will not be disclosed to fellow members of staff, (except those members of staff within the personnel department who process such data). If for any reason you do not wish your health records to be kept please contact the **DPM**.

## 8. Employee Reviews & Appraisals

We will only collect data required for the day-to-day operation of the Company.

## 9. Benefits Schemes

Where we provide additional benefits such as health insurance and pension schemes, we will not make use of data collected by third parties administering the schemes where such data is not required for the day-to-day operation of the Company. We will provide members of staff with details of what information will be collected by these third parties and how it will be used. Furthermore, we will seek permission for the collection and use of this data prior to collection.

## 10. Equal Opportunities Monitoring

We may collect information relating to ethnic origin, sex or disability as part of an equal opportunities policy. We will ensure that any questionnaires relating to such information are accurate and that where possible the results will identify employment trends within the Company, and not identify individual members of staff.

## 11. Security of Data

We are committed to the secure storage and where undertaken the secure transmission of members of staffs' personal data. Only management and members of staff within the personnel department have access to such data. All such data is protected by physical security, such as locks and technical security, such as usernames and passwords to access computer records and data. Such data is only disclosed on a "need to know" basis.

To further ensure the security of such records the Company reserves the right to monitor and keep detailed log file and computer data analysis of all accesses to staffs' personal data. The Company

Document id:	Osirian Consulting Ltd – Data Protection Policy	Page 7 of 12
Version:	V3	Confidential Information
Issued:	08/04/2025	Document Owner: Rachael Lee

also reserves the right to vet all members of staff who have access to such data during their normal employment within the Company.

All staff are reminded that unauthorised attempts to gain access to or accessing such data is a disciplinary offence and in certain situations may constitute gross misconduct leading to summary dismissal. Such breaches may also constitute a criminal offence under the Data Protection Act.

## 12. External Data Processing

Where we use third parties to process data and provide services or administer schemes around such data the Company will take reasonable steps to ensure that such third parties have in place their own data protection policies.

## 13. Data Transfers outside the European Economic Area

If the Company transfers data outside the European Economic Area such data will only be transferred to countries deemed by the European Commission to provide adequate data protection or to countries, which are recognised "safe harbours" for such data. However, the Company may transfer data to other countries where the permission of the members of staff has been given.

## 14. References

The Company will not disclose details of confidential references where to do so would disclose the identity of the author or where it may cause harm or detriment to the author.

## 15. Data Breaches

### 15.1 How to deal with data breaches

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we must also notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact the **DPM** immediately and keep any evidence you have in relation to the breach.

## 16. Data Subject Access Rights

### 16.1 Subject access requests

Data subjects can make a 'subject access request' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request, you should forward it immediately to the **DPM** who will coordinate a response.

If you would like to make a SAR in relation to your own personal data, you should make this in writing to the **DPM**. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

### 16.2 Your data subject rights

- You have the right to information about what personal data we process, how and on what basis as set out in this policy

Document id:	Osirian Consulting Ltd – Data Protection Policy	Page 8 of 12
Version:	V3	Confidential Information
Issued:	08/04/2025	Document Owner: Rachael Lee

- You have the right to access your own personal data by way of a subject access request (see above)
- You can correct any inaccuracies in your personal data
- You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected
- While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made
- You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop
- You have the right to object if we process your personal data for the purposes of direct marketing
- You have the right to receive a copy of your personal data and to transfer your personal data to another data controller – we will not charge for this and will in most cases aim to do this within one month
- With some exceptions, you have the right not to be subjected to automated decision-making
- You have the right to be notified of a data security breach concerning your personal data.
- In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the **DPM**.
- You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner’s Office directly. Full contact details including a helpline number can be found on the Information Commissioner’s Office website ([www.ico.org.uk](http://www.ico.org.uk)). This website has further information on your rights and our obligations.

If you want to exercise any of your rights, please contact the **DPM**.

## 17. External Disclosure Requests

Where members of staff receive external requests for the disclosure of data the following guidelines should be observed:

1. Verify the identity of the person requesting the information
2. Be on the lookout for fraud or deception
3. Seek a written request where possible
4. Check any telephone numbers where a verbal request is received
5. Inform the Data Protection Manager if any request appears suspicious
6. The Data Protection Manager should also be contacted where the party requesting the data states that disclosure is required by law
7. Remember that a duty is owed to the members of staff whose data is to be disclosed, where possible seek their permission, unless doing so would alert them to a criminal investigation
8. If the disclosure of the data is non-routine where possible provide the members of staff in question with a copy of the data disclosed. A record of all non-routine data disclosures should also be kept.

If in doubt, consult the **DPM**.

Document id:	Osirian Consulting Ltd – Data Protection Policy	Page 9 of 12
Version:	V3	Confidential Information
Issued:	08/04/2025	Document Owner: Rachael Lee

## 18. Other Disclosures

Where we want to disclose staff data for promotional, marketing or other business purposes, (for example incorporated into an advertisement or brochure) the consent of the member of staff will be sought in advance. The member of staff should also be told where the data will be published and how widely.

## 19. Trade Unions

We will only provide data to trade unions where the trade union is recognised by the employer. The data will be limited to name, job description and job location. We will also give each member of staff a prior right to object to the disclosure. Where any such data is provided for collective bargaining the data will not identify individual members of staff.

## 20. Staff Monitoring

We will inform all members of staff where staff monitoring is introduced or increased. We will take reasonable steps to ensure that members of staff 's privacy and autonomy are preserved. We will take reasonable steps to ensure that specific details of personal conversations or correspondence are not accessed. However, we retain the right to monitor the actual use of Company resources by members of staff.

## 21. Medical Testing

If we undertake any form of medical testing of members of staff such testing will only be undertaken for clear health and safety reasons, for assessing a members of staff 's medical fitness for continued employment or to assess their entitlement to health benefits, such as sick pay. Prospective members of staff may be tested for similar reasons. The results of any testing required for a health or pension scheme shall not be given to the Company.

## 22. Retention of Records

We will establish retention periods for at least the following categories of data:

Type	Retention period (up to)
Application form:	For period of employment
References:	1 year
Payroll and tax information:	6 years
Sickness records:	3 years
Annual leave records:	2 years
Annual appraisal/assessments:	5 years
Promotions/Transfers/Training	1 year from end of employment
Disciplinary and grievance matters:	1 year from end of employment
Summary of service:	6 years from end of employment
Injury or accident at work:	6 years from end of employment
Call recordings	1 year

We will ensure the safe and secure disposal of records that are no longer required.

## 23. Data Protection Manager

The **DPM** has the following responsibilities:

- Briefing the Managing Director on data protection responsibilities
- Reviewing data protection and related policies
- Advising other staff on data protection issues

- Ensuring that data protection induction and training takes place
- Notification
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data
- Approving contracts with data processors

**End.**

---

Document id:	Osirian Consulting Ltd – Data Protection Policy	Page <b>11</b> of <b>12</b>
Version:	V3	Confidential Information
Issued:	08/04/2025	<b>Document Owner:</b> Rachael Lee

## Annex 1: Document Control and Change History

Document Control			
<b>Company</b>	Osirian Consulting Ltd		
<b>Policy Name:</b>	Data Protection Policy		
<b>Policy Version:</b>	V2	<b>Policy Issued:</b>	07 April 2022
<b>Policy Review Date:</b>	01 April 2023	<b>Document Status:</b>	Confidential Information
<b>Designated Owner:</b>	Rachael Lee		
<b>Data Controller:</b>	Osirian Consulting Ltd		
<b>Data Protection Officer:</b>	N/A		
<b>Data Protection Manager:</b>	Rachael Lee		
<b>DPA Registration No.</b>	Z4813004		

Change History				
Version	Revisor	Description of Change	Date of Change	Next Review
V1	RL/CL/RSH	Final version	22/05/2018	01/06/2019
V1	RL	Policy review – no change	03/06/2019	01/06/2020
V1	RL	Policy review – no change	01/06/2020	01/06/2021
V2	VP	Call recording details and retention added	08/04/2021	01/04/2022
V2	RL	Policy review – no change	07/04/2022	01/04/2023

Document Distribution List		
Name or Group	Name	Contact / Email
To all Staff		

Supporting Documents

Document Approvals			
This document requires approval from:			
<b>Sponsor Approval</b>	<b>Name</b>	<b>Date</b>	<b>Signature</b>
Data Protection Manager	Rachael Lee	07/04/2022	