# GDPR Handbook

## Koncise Solutions Limited

KONCISE SOLUTIONS

THE CLOUD. SIMPLIFIED.

| Section | Handbook Sections and Section Title | Section Version |
|---|---|---|
| | **Governance** | |
| 2.01 | Responsibility and Data Privacy | |
| 2.02 | Data Privacy Lead | |
| 2.03 | Communication Plan | |
| | **Data Privacy Law** | |
| 3.01 | Personal Data Definition | |
| 3.02 | Privacy Principles | |
| | **Data Subject** | |
| 4.01 | Data Subject Rights | |
| | **Polices & Processes** | |
| 5.01 | Data Protection Policy | |
| 5.02 | Privacy Policy | |
| 5.03 | Data Retention Policy | |
| 5.04 | Access Control Policy | |
| 5.05 | Subject Access Policy & Process | |
| 5.06 | Request for Erasure Policy & Process | |
| 5.07 | Request for Data Portability Policy & Process | |
| 5.08 | Breach Notification Process | |
| 5.09 | Data Rectification Policy & Process | |
| 5.10 | Data Accuracy Policy & Process | |
| 5.11 | Data Deletion & Destruction Policy | |
| | **Contractual Requirements** | |
| 6.01 | Employment Contracts | |
| 6.02 | Client Contract Summary | |

## 2.01 - Responsibility for Data Privacy

The below outlines who is responsible for Data Privacy within the business.

| Name | Job Title | Role in Data Privacy | Start Date of Appointment | End Date/Review Date of Appointment | Brief Description of Duties |
|---|---|---|---|---|---|
| Ben Konopinski | Director | GDPR Lead | 01/01/2018 | | Oversee GDPR Compliance |
| Varsha Mistry | Executive Assistant | Data Privacy Lead | 01/01/2018 | | Support Data Privacy Lead |

### 2.02 – Data Privacy Lead

The below outlines the nature of the role adopted to manage Data Privacy.

Each employee has a responsibility to ensure Personal Data is protected and used in a compliant manner. The following roles provide a framework for the execution of GDPR compliance. The responsibilities at each level allow for the effective transfer of information across the business to respond to any breach or subject right request.

Data Privacy Lead has been appointed and is considered beneficial to the organisation:

- To ensure there is a main point of contact for all Data Protection related issues,
- To have a subject matter expert to advise and guide the organisation
- Introduce a Privacy by Design approach
- Monitor and evaluate compliance.

The Data Privacy lead will:

- Be the subject matter reference on compliance with GDPR
- Provide advice to on day-to-day activities involving the use of Personal Data
- Create and manage policies, processes and procedures and template documents establishing standards of Personal Data protection
- Oversee the learning content of GDPR training.
- Manage the Data Flow Diagrams
- Manage the GDPR Risk Register
- Stay up to date with the regulatory environment including guidance from the ICO, Article 29 Working Party, Brexit negotiations and other external factors that could influence GDPR compliance.

## 2.03 – Communication Plan

The below describes the communication of Data Privacy both internally and externally. To assist in the embedding of Data Privacy communications both internally and externally should be broadcasted to highlight to customers and employees how personal data is collected and used.

To achieve this the introduction of a Privacy Notice and Privacy Policy is required. All Privacy communications should be drafted in clear and concise language and easily accessible for both customers and employees to read.

**Privacy Notice:**

A Privacy Notice (also referred to as a Privacy Statement) is a statement made to data subjects to highlight how the organisation collects, uses and retains their personal data. Privacy Notices usually appear in the form of pop up box or highlighted area of an organisation's website.

**Privacy Policy:**

In addition, a Privacy Policy is an internal statement that governs the organisation's handling practices of personal data. This helps to instruct employees on the collection and use of their personal data and any specific rights of a data subject. Further detail of this can be found in Section 5.02 of this handbook.

Further examples of communicating privacy principles internally can be found in the below guidance from the ICO. This includes printable posters and communications that can be used to support the Privacy Policy within the organisation.

**https://ico.org.uk/media/for-organisations/think-privacy/2693/ico-think-privacy-toolkit.pdf**

## 3.01 – Personal Data Definition

**The below provides the definition of Personal Data.**

Every single one of us has a unique set of information that only applies to us. From the way that we look, to our name, age, address and behaviour, we possess a unique combination of data which is linked to our identity. This is called personal data.

Organisations will store personal data about customers and employees to comply with legislation, operate successfully and to achieve competitive advantage.
Personal Data can be defined as follows:

"Any information which relates to a person and can be used to identify the individual. For example; name, address, email, photographs, phone numbers, CCTV footage, IP addresses etc".

The important aspect to remember is that personal data has the potential to cause harm, distress or damage to individuals and the company if lost or stolen.

There are two types of personal data that are classified as high risk;

- **Sensitive personal data** – Any type of personal data that is likely to be private and could be used in an inappropriate way. For example, details of physical/mental health, religious beliefs, or political opinions.

- **Children's data** – The ICO define a "child" as anyone aged 13 or over. Parental or custodian consent must be obtained in order to use any child's data.

## 3.02 – Privacy Principles

The below details of the principles of Data Privacy.

Data Privacy is an organisation's commitment to:

- Valuing the privacy rights of those whose personal data it uses,
- Recognising the impact of its actions upon individuals' privacy; and
- Never using an individual's personal data for a use that benefits the business at the detriment of the individual

A Data-Privacy focussed approach is not driven by the need to demonstrate compliance with the GDPR; it is driven by a collective aim of delivering an exceptional level of service to those whose data is held, underpinned by a respect for their privacy.

The result is that organisations may not always be able to use personal data in a way which would commercially benefit them; but by putting privacy at the forefront of their strategy, they will almost certainly exceed the compliance requirements of the GDPR.

## Why is this important?

Every day, your organisation processes the personal data of its employees and customers. Many of the ways in which it uses the personal data that it collects will naturally benefit its customers or employees and will not infringe their privacy rights. However, in some instances the organisation's commercial needs will infringe or directly oppose the privacy rights of the individual. As a result, senior management must decide to put the privacy of the customer at the forefront and adopt a Data Privacy culture.

## To adopt this approach the ICO recommend a Privacy by Design approach.

'Privacy by Design' means designing new activities involving Personal Data with privacy at the heart of the aim of the activity. By adopting Privacy by Design, it is a way of ensuring that Personal Data is continuously processed in a fair, lawful and transparent manner to the customers and employees.

## GDPR Principles

Personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

6. 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, using appropriate technical or organisational measures ('integrity and confidentiality').

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

## 4.01 – Data Subject Rights

The below provides details of the rights of a Data Subject.
Article Six of the GRPR allows and individual the right to view personal data that organisations hold about them and proposes that personal data should be processed in accordance with the rights of data subjects under the Act.

All data subjects are entitled to obtain:

- Confirmation as to whether the organisation is processing any personal data about that individual;
- A right of access to a copy of the information comprised in their personal data;
- A right to object to processing that is likely to cause or is causing damage or distress;
- A right to prevent processing for direct marketing;
- A right to object to decisions being taken by automated means (profiling activity);
- A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed;
- A right to claim compensation for damages caused by a breach of the Act;
- Any related information (including a description, source of the data, the reasons it is being processed and whether it will be shared with any other organisation or people).

It is important to note that data subjects have a right to request to see their own personal data but do not have the right to view copies of the entire documents that contain their personal data. Often, the easiest way to provide the relevant information is to supply copies of original documents, but you are not obliged to do this.

However, an individual is entitled only to their **own** personal data, and not to information relating to other people (unless they are acting on behalf of that person).

| **DATA SUBJECT RIGHTS** | | | **LEGAL BASIS FOR PROCESSING** | | | |
|---|---|---|---|---|---|---|
| | **Consent** | **Necessary for the Performance of a Contract** | **Legal Obligation** | **Vital Interests** | **Public Task** | **Legitimate Interests** |
| **Informed of how their data is processed** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Subject Access** | ✓ | ✓ | | ✓ | ✓ | ✓ |
| **Rectification** | ✓ | ✓ | | | | ✓ |
| **Erasure** | ✓ | | | | | ✓ |
| **Restriction** | ✓ | | | | | ✓ |
| **Portability** | ✓ | | | | | ✓ |
| **Objection** | ✓ | | | | | ✓ |
| **Automated/decisions Profiling** | | | | | | ✓ |

## 5.01 – Data Protection Policy

The below sets out the organisation's Data Protection Policy.

### Background

The EU General Data Protection Regulation (GDPR) replace the Data Protection Act of 1998 and its main purpose is to protect the rights and freedoms of natural persons and to ensure that their personal data is not processed without their knowledge and without a lawful basis.

The accountability principle in Article 5(2) of the GDPR requires organisations to demonstrate compliance with the principles of the GDPR. Article 24 sets out how organisations can do this by requiring the implementation of appropriate technical and organisational measures to ensure that organisations can demonstrate that the processing of personal data is performed in accordance with the GDPR.

The organisation recognises data protection as a fundamental right of our customers and is committed to ensuring that this fundamental right is duly respected and protected. This policy sets out how the organisation deals with personal data, including key contacts, the principles & rights, and how to handle a request.

### Important definitions under Article 4:

**'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;

**'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;

**'Restriction** of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

**'Profiling'** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

**'Pseudonymisation'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

**'Filing System'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

**'Controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

**'Processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

**'Third Party'** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

## Key contacts

### Data Privacy Lead

The Data Privacy Lead is the main contact responsible for the GDPR work and also the key contact for all data protection related matters within the organisation.

Main duties are:

- Create a GDPR plan and assign responsibility for data privacy throughout the organisation
- Inform, advice and issue recommendations on meeting the GDPR requirements.
- Analyse and check the compliance of processing activities involving personal data and have due regard to associated risks. This includes providing advice on performing Data Protection Impact Assessments; these need to be done "where a process is using new technologies, and taking into account the nature, scope, context and purposes of the processing, there is a high risk to the rights and freedoms of natural persons."

### General Data Protection Principles

Article 5 requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

- 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, using appropriate technical or organisational measures.

**Individual's Rights:**

The GDPR includes the following rights for individuals:

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

**Handling Individuals Request**

Is important to be aware that individuals' request derived from the right to access, the right to rectification, the right to erasure, the right to data portability are in most circumstances provided free of charge and within one month of receipt of the request. You may charge a fee or refuse to respond if requests are manifestly unfounded or excessive.

**Employees' obligations regarding personal information**

If an employee acquires any personal information in the course of his/her duties, he/she must ensure that:

- The information is accurate and up to date, insofar as it is practicable to do so;
- The use of the information is necessary for a relevant purpose and that it is not kept longer than necessary; and
- The information is secure.
- Uses password-protected and encrypted software for the transmission and receipt of emails,
- Follows the instructions provided in the BYOD policy.
- Locks files in a secure cabinet.
- Make use personal data only if he/she has been appointed to do so.
- Report breaches immediately to the Data Privacy Lead or Data Protection Officer.

## 5.02 – Privacy Policy

The following contains the organisation's Privacy Policy.

We understand that there might be different collecting points for obtaining personal data and different lawful basis for processing it, therefore, the following privacy policy shall be disclosed, used, and adapted throughout the organisation, this includes marketing communications and website.

In order to make this information concise and easily accessible to our customers, our privacy policy can be provided in the form of a statement and FAQs as follows:

**Privacy Policy:**

The organisation is committed to ensuring that your privacy is protected. We will always ensure your data is kept securely and not disclosed to an unauthorised person. Should we ask you to provide certain information by which you can be identified when using our services, then you can be assured that it will only be used in accordance with this privacy statement and in compliance with the EU General Data Protection Regulation GDPR, the Data Protection Act 1988, and the Data Protection (Amendment) Act 2003.

Koncise Solutions Ltd may change this policy from time to time by updating this page. You should check this page from time to time to ensure that you are happy with any changes. This policy is effective from 25th May 2018.

**What kind of information we will collect from you?**

In order to provide our services, we have collected and processed the following information where applicable to you:

- Your name, company name, and job title.
- Your contact information including address, phone number, and email.

**How we will use your personal data?**

- If you are a customer at present we may use your personal data to improve the products and services we currently provide you or;
- If you are a former customer, we may use your personal data to improve the products and services we have delivered to you and conform to good business practices or;
- If we consider that our products or services might be of your interest then we may use your personal information to contact you with newsletters, marketing or promotional materials and other relevant information.
- From time to time, we may also use your information to contact you, by email, for research purposes.

**Would we be sharing your personal data to others?**

- We will not sell, distribute or lease your personal information to third parties unless we have your permission or are required by law to do so. We may use your personal information to send you promotional information which we think you may find interesting if you tell us that you wish this to happen.

**How long we will retain your personal data?**

- We will keep your personal data for as long as you remain a customer of the company plus **18 months**. After this period, we will securely delete and destroy your personal data.

- Some data, however, must be retained in order to protect the company's interests, preserve evidence, and conform to good business practices. Some data will be retained to allow us to contact you where we have received your consent to do so, or where a legitimate interest to both parties has been determined.

- Note that the need to retain certain information can be mandated by local, industry regulations and will comply with EU General Data Protection Regulation GDPR and the Data Protection Act 1988 and the Data Protection (Amendment) Act 2003. Where this policy differs from applicable regulations, the policy specified in the regulations will apply.

**What are your rights as a data subject?**

It is in our best interest to safeguard your rights as our customer, therefore, we would like you to have a clear understanding of what happens to your personal data once we have collected it. The following list explains your rights as an individual under the EU General Data Protection Regulation:

- You have the right to be informed of what we do with your data and to know is what the purpose of collecting and processing is.

- You have the right to access your personal data and supplementary information so that you aware of, and can verify, the lawfulness of the processing. You can obtain the following information: a) confirmation that your data is being processed and b) access to your personal data. We will provide this information within one month of the request and free of charge.

- You have the right to request us to rectify your personal data if is inaccurate or incomplete.

- You have the right to request the deletion or removal of your personal data where there is no compelling reason for its continued processing, although, this can only be done under specific circumstances. Find out more: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

- You have the right to restrict the data processing, however, this can only be done under specific circumstances. Find out more: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/

- You have the right to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. This is commonly known as “data portability”. We will provide this in a structured, commonly used and machine-readable form, free of charge, and we will deliver it you in one month following the request.

## Our details

- Koncise Solutions Ltd is a company based in the United Kingdom. Our company number is 7789203, registered in England and Wales.

- You can reach us at info@koncisesolutions.com

- You can write to us at: Koncise Solutions Ltd, The Auction House, Glenhaven Avenue, Borehamwood, Hertfordshire, WD6 1AY

## How we use Cookies

A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you agree, the file is added and the cookie helps analyse web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences.

We use traffic log cookies to identify which pages are being used. This helps us analyse data about web page traffic and improve our website in order to tailor it to customer needs. We only use this information for statistical analysis purposes and then the data is removed from the system.

Overall, cookies help us provide you with a better website, by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us. You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website.

Portions of this website use Google Analytics, a web analytics service provided by Google, Inc. ("Google"). Google Analytics uses "cookies", which are text files placed on your computer, to help the website analyse how users use the site. The information generated by the cookie about your use of the website (including your IP address) will be transmitted to and stored by Google on servers in the United States.

Google will use this information for the purpose of evaluating your use of the website, compiling reports on website activity for website operators and providing other services relating to website activity and internet usage. Google may also transfer this information to third parties where required to do so by law, or where such third parties process the information on Google's behalf. Google will not associate your IP address with any other data held by Google.

You may refuse the use of cookies by selecting the appropriate settings on your browser, however please note that if you do this you may not be able to use the full functionality of this website. By using this website, you consent to the processing of data about you by Google in the manner and for the purposes set out above.

## 5.03 – Retention Policy

The following sets out the organisation's Retention Policy.

Article 5 (e) states that personal data should be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which they are further processed." The data must therefore be erased when those purposes have been served.

This policy sets out the guideline for retaining and deleting personal data.

**Retention Policy:**

- Customer's personal data: Personal data will be held for as long as the individual is a customer of the company plus 18 months.

- Personal employee data (Including employee health and sickness documents, records of leave): Employee data will be held for the duration of employment and then for 3 years after the last day of contractual employment. Employee contracts will be held for 3 years after last day of contractual employment.

- Recruitment details: Interview notes of unsuccessful applicants will be held for 6 months after interview.

- Financial & Accounting records will be held for 6 years.

- Contract documents will be held for 10 years.

**Destruction Policy:**
When the retention timeframe expires, the company shall actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by the Data Privacy Lead or GDPR Lead.

## 5.04 – Access Control Policy

The below details the Access Control Policy.

The purpose of this policy is to maintain an adequate level of security to protect the organisation data and information systems from unauthorised access. This policy defines the rules necessary to achieve this protection and to ensure a secure and reliable operation of the organisation information systems.

The scope of this policy includes all access to the organisation information, IT systems and physical access to areas and locations where information and data is located. This policy applies throughout the information lifecycle from acquisition/creation, through to processing, storage and disposal.

### Policy

### Electronic Systems

1. The organisation controls access to information based on the security requirements of the business and in line with data privacy legislation to ensure the protection of data held by the company.
2. Risk assessments are carried out for each business applications to assess the security requirements and risks associated with each application.
3. Access and user rights are controlled by the use of standard user profiles for common roles within the business (See appendix).
4. All user access requests should be formally authorised.
5. Access rights are granted at the minimum level necessary for that role.
6. Any changes to a user's standard profile must be formally authorised.
7. New user access and changes to access must be processed by the Information Security Manager.
8. Standard user profiles should be reviewed periodically.
9. A user removal request should be sent to the Information Security manager by HR when an employee leaves the company.
10. All users are subject to the "Acceptable Usage Policy" and must sign and agree to the terms before their access is set up.

### Physical Documents

1. The organisation controls access to paper files based on the security requirements of the business and in line with data privacy legislation to ensure the protection of data held by the company.
2. Risk assessments are carried out to assess the security requirements and risks associated with each file type. These files include –
    a. Payroll & Human Resources
    b. Financial Accounting Records

3. All paper files must have adequate security. This should include locked filing cabinets or a locked archive room.
4. Access to these files are based on job requirements and only those roles that require access to these files will be granted access.

5. All key holders must sign a declaration to acknowledge receipt of the key and confirm their understanding of the Data Privacy legislation.
6. All keys holders must ensure any files removed from the secure location are returned at the end of each working day or whilst they are away from their desks.
7. A clean desk policy should be in place for all employees that have access to confidential files.
8. The allocation of keys for secure areas should be reviewed periodically.
9. A leaver form should be sent to the Information Security manager by HR when an employee leaves the company. The Information Security manager is responsible for ensuring all keys are returned.

### 5.05 – Subject Access Policy & Process

The below describes the policy and process for Subject Access requests (SAR).
The purpose of this policy is to ensure that the organisation provides data subjects access to information held on them by the organisation as per the rights of individuals set down by the GDPR.

This right, commonly referred to as subject access, is created by Article 15 of the GDPR. It is most often used by individuals who want to see a copy of the information an organisation holds about them. An individual who makes a written request is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the information comprising the data; and given details of the source of the data (where this is available)

**Policy**

1. Subject access requests should be made in writing to the organisation.
2. The data subject must provide evidence of their identity. This could be in the form of a passport or driving licence and this information should be checked to ensure the identity is correct before processing the request.
3. All Subject Access requests should be forwarded to the Data Privacy Lead.
4. the organisation must respond to a SAR without undue delay and within 1 month of receipt of the request. If there are any exceptional circumstances that require a longer period of time to collate the SAR then the data subject must be informed of this within the 1 month time and explain the reasons for the delay.
5. A fee cannot be levied for a subject access request.
6. If it is felt that a request is unfounded or excessive then the organisation has the right to refuse a request or charge a reasonable fee to cover the costs of administration.
7. the organisation should collate the necessary information by searching all databases and all relevant manual filing systems. This should include all back up and archived files and e-mail folders.
8. If the information is requested electronically the information should be provided electronically. It is possible to supply information in other formats, but this must be agreed with the Data Subject.
9. Data may not be altered or destroyed in order to avoid disclosing it.
10. The Data Privacy Lead is responsible for reviewing all information to ensure it does not disclose any information relating to a 3rd party. If there is any information relating

to a 3rd party, then this should be removed or if this is not possible then permission from the 3rd party should be sought to allow their data to be disclosed.

11. If the requested data falls under one of the following exemptions, it does not have to be provided:

    a. Crime prevention and detection.
    b. Negotiations with the requester.
    c. Management forecasts.
    d. Confidential references given by the organisation (not ones given to the organisation).
    e. Information used for research, historical or statistical purposes.
    f. Information covered by legal professional privilege.

12. The Data Privacy Lead should keep a record of all SAR's in the SAR Register see 5.05.01

## 5.06 – Request for Erasure Policy & Process

The below describes the policy and process to respond to requests for Erasure, also known as a request to be forgotten.

The purpose of this policy is to ensure that the organisation provides Data Subjects the right to have personal data held by the company erased and the procedure for erasing information from our systems both electronically and information held as part of a filing system.

This right, commonly referred to as the right to be forgotten, is created by Article 17 of the GDPR. It covers the rights of the Data Subject to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay.

### Policy

1. The Data Subject has the right to request their personal data is deleted where one of the following grounds applies:-

a. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b. he Data Subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
c. the Data Subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the Data Subject objects to the processing pursuant to Article 21(2);
d. the personal data have been unlawfully processed;
e. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
f. the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. If the organisation has made the personal data public and is obliged to erase the personal data, then the organisation, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the Data Subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. The right to erasure does not apply to the extent that processing is necessary: -

a. for exercising the right of freedom of expression and information;

b. for compliance with a legal obligation which requires processing by Union or Member State law to which the organisation is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the organisation;

c. for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

d. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

e. for the establishment, exercise or defence of legal claims. 4. All erasure requests should be forwarded to the designated data privacy lead.

5. The Data Subject must provide evidence of their identity. This could be in the form of a passport or driving licence and this information should be checked to ensure the identity is correct before processing the request.

6. A fee cannot be levied for a subject access request.

7. The organisation must respond to an erasure request without undue delay.

8. Once it has been established that the erasure request is valid the organisation must take reasonable measures to ensure all data is removed. This should include searching all databases and all relevant manual filing systems. This should include all back up and archived files and e-mail folders. Once all data has been located then relevant action should be taken to delete all personal data.

9. The Data Privacy Lead shall keep a record of all erasure requests. This should include the name of the Data Subject, the date of receipt and the date of erasure. See 5.06.01

10. The Data Privacy Lead should inform the Data Subject once the erasure of their personal data has been completed.

**Process**

1. All requests should be forwarded to the Data Privacy Lead and GDPR Lead at info@koncisesolutions.com.

2. The Data Privacy Lead should contact the Data Subject to confirm receipt of their request, outline the process to the Data Subject, and validate the request is genuine and reasonable before processing (including confirming the Data Subjects identity).

3. On confirmation of the Data Subject's identity and that the request is genuine and reasonable, the Data Privacy Lead should manage the identification of the Data Subject's personal data held by the company and relevant third parties.

4. The Data Privacy Lead will produce a report within 30 days of the request outlining the personal data that is stored and confirm with the Data Subject the action that should be taken.

5. The Data Privacy Lead will maintain a record of any such requests.

**5.07 – Request for Data Portability Policy & Process**

The below describes the policy and process for responding to a request for Data to be provided to a Data Subject in a portable structure.

The purpose of this policy is to ensure that the organisation provides Data Subjects the right to have personal data held by the company.

The right to data portability is created by Article 20 of the GDPR. It covers the rights of the Data Subject to receive the personal data concerning him or her, which he or she has provided to the organisation, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the organisation to which the personal data have been provided.

## Policy

1. The Data Subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the organisation, in a structured, commonly used and machine-readable format and have the right to transmit the data to another controller without hindrance from the organisation to which the personal data have been provided, where:

a. the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
b. the processing is carried out by automated means.
c. In exercising his or her right to data portability pursuant to paragraph 1, the Data Subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
d. The exercise of the right referred to point 1 shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the organisation.
e. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

2. All data portability requests should be forwarded to the Data Privacy Lead.
3. The Data Subject must provide evidence of their identity. This could be in the form of a passport or driving licence and this information should be checked to ensure the identity is correct before processing the request.
4. A fee cannot be levied for a data portability request.
5. the organisation must respond to a data portability request without undue delay.
6. Once it has been established that the data portability request is valid the organisation must provide the requested data in a structured, commonly used and machine-readable format to the other controller.
7. The Data Privacy Lead shall keep a record of all data portability requests. See 5.07.01.
8. The Data Privacy Lead should inform the Data Subject once the request has been completed.

## Process

1. All requests should be forwarded to the Data Privacy Lead and GDPR Lead at info@koncisesolutions.com.
2. The Data Privacy Lead should contact the Data Subject to confirm receipt of their request, outline the process to the Data Subject, and validate the request is genuine and reasonable before processing (including confirming the Data Subjects identity).
3. On confirmation of the Data Subject's identity and that the request is genuine and reasonable, the Data Privacy Lead should manage the identification of the Data Subject's personal data held by the company and relevant third parties.
4. The Data Privacy Lead will produce a report within 30 days of the request outlining the personal data that is stored and confirm with the Data Subject the action that should be taken.
5. The Data Privacy Lead will maintain a record of any such requests.

## 5.08 – Breach Notification Process

The below describes the policy and process to respond to an identified Data Breach.

The purpose of this policy is to ensure that the organisation has a robust system in place for reporting data breaches.

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority.

There is a distinction between a 'Data Controller' and a 'Data Processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Therefore, the organisation should establish whether it is Data Controller. See Data Map summary 4.03.01

This policy defines the breach notification policy for both 'Data Controllers' and a 'Data Processors'.

All users (including Employees, contractors and third-party users) and owners of the organisation are required to be aware of, and to follow this procedure in the event of a personal data breach.

### Policy

Data Processors

1. The organisation must report any personal data breach to the Data Controller without undue delay.
2. All breached reported to the Data Controller must be recorded on the Internal Breach Register - 5.08.01
3. Notifications to the Data Controller should be made by phone call to the Data Privacy Lead, followed up by an email to info@koncisesolutions.com outlining the breach.
4. The organisation must obtain a receipt from the Data Controller acknowledging receipt of the notification.

Data Controller

1. When a personal data breach has occurred, the organisation need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk, then the local supervisory authority must be informed.
2. If a breach is reportable then the organisation must do this within 72 hours of becoming aware of the breach, where feasible.
3. When reporting a breach, you must provide:

a. a description of the nature of the personal data breach including, where possible:
b. the categories and approximate number of individuals concerned; and
c. the categories and approximate number of personal data records concerned;
d. the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
e. a description of the likely consequences of the personal data breach; and

f. a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

4. If the organisation is not able to provide full details within 72 hours, the breach should still be reported, and details given of when it is expected that the additional information will be available.
5. If a breach is likely to result in a high risk to the rights and freedoms of individuals, the organisation must inform those concerned directly and without undue delay. You need to describe, in clear and plain language, the nature of the personal data breach and, at least:

a. the name and contact details of the organisation data protection officer or data privacy lead;
b. a description of the likely consequences of the personal data breach; and
c. a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

6. If a breach is deemed not reportable then it should still be recorded on the Internal Breach Register - 5.08.01. This should include full details of the breach and your assessment of the decision not to report the breach.
7. All breaches, regardless of whether or not they need to be reported should be recorded on the Internal Breach register. The register should document the facts relating to the breach, its effects and the remedial action taken.
8. The organisation should investigate all data breaches to ascertain whether or not the breach was a result of human error or a systemic issue and implement measures to prevent recurrence.

### 5.09 – Data Rectification Policy & Process

The below describes the policy and process responding to data rectification requests received.

The purpose of this policy is to ensure that the organisation fulfils the right of Data Subjects to request that data held is rectified without undue delay.

Data accuracy is created by Article 5 section d) of the GDPR. The organisation has an obligation to ensure personal data is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

### Policy

1. The Data Subject shall have the right to request that their personal data is rectified without undue delay.
2. All data rectification requests from external sources should be forwarded to the Data Privacy Lead.
3. All data rectification requests from employees should be forwarded to the HR Manager.
4. The Data Subject must provide evidence of their identity. This could be in the form of a passport or driving licence and this information should be checked to ensure the identity is correct before processing the request.
5. A fee cannot be levied for a rectification request.

6. The organisation must respond to a data rectification request without undue delay.
7. Once it has been established that the request is valid the organisation must ensure all records held are updated without undue delay.
8. The organisation should identify all information by searching all databases and all relevant manual filing systems. This should include all back up and archived files and e-mail folders. See Personal Data summary 4.03.01.
9. If The organisation has shared the personal data with any 3rd parties these parties should be sent a rectification request and confirmation should be obtained to confirm that this has been processed.
10. The Data Privacy Lead shall keep a record of all data rectification requests - 5.09.01.
11. The Data Privacy Lead shall inform the Data Subject once the request has been completed.

**Process**

1. All requests should be forwarded to the Data Privacy Lead and GDPR Lead at info@koncisesolutions.com.
2. The Data Privacy Lead should contact the Data Subject to confirm receipt of their request, outline the process to the Data Subject, and validate the request is genuine and reasonable before processing (including confirming the Data Subjects identity).
3. On confirmation of the Data Subject's identity and that the request is genuine and reasonable, the Data Privacy Lead should manage the identification of the Data Subject's personal data held by the company and relevant third parties.
4. The Data Privacy Lead will produce a report within 30 days of the request outlining the personal data that is stored and confirm with the Data Subject the action that should be taken.
5. The Data Privacy Lead will maintain a record of any such requests.

## 5.10 – Data Accuracy Policy & Process

The below describes the policy and process required to maintain the accuracy of personal data.

The purpose of this policy is to ensure that the organisation takes reasonable steps to ensure personal data held, both electronically and in manual files, is kept accurate and up to date.

Data accuracy is created by Article 5 section d) of the GDPR. The organisation has an obligation to ensure personal data is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. This policy covers the process of ensuring personal data records are kept up to date.

**Policy**

1. The organisation should have records of all personal data held and where it is stored for both electronic and manual files. See Personal Data summary 4.03.01
2. Records should be deleted in line with the Data Retention Policy. See 5.03.

3. Where possible the organisation should include processes to ensure data is accurate. This may include an online portal where data subjects can update their own information.
4. Employee records should be updated on a periodic basis by sending out a form to all employees detailing current data held and requesting any changes to be noted and then returned to the HR manager.
5. Records should be updated in line with the Data Rectification Process and Policy (See section 5.07).
6. If the organisation becomes aware of any inaccuracies and has shared the personal data with any 3rd parties these parties should be sent a rectification request and confirmation should be obtained to confirm that this has been processed.
7. The Data Privacy Lead may keep a record of all inaccuracies that are identified and details of when they were rectified.

**Process**

1. All requests should be forwarded to the Data Privacy Lead and GDPR Lead at infor@koncisesolutions.com
2. The Data Privacy Lead should contact the Data Subject to confirm receipt of their request, outline the process to the Data Subject, and validate the request is genuine and reasonable before processing (including confirming the Data Subjects identity).
3. On confirmation of the Data Subject's identity and that the request is genuine and reasonable, the Data Privacy Lead should manage the identification of the Data Subject's personal data held by the company and relevant third parties.
4. The Data Privacy Lead will produce a report within 30 days of the request outlining the personal data that is stored and confirm with the Data Subject the action that should be taken.
5. The Data Privacy Lead will maintain a record of any such requests.

### 5.11 – Data Deletion & Destruction Policy

The below describes the policy and process required to destroy or delete data.

The purpose of this policy is to ensure that the organisation has a robust system in place to ensure that data is kept for no longer than necessary and is disposed of in a secure manner. Article 5 of the GDPR states that personal records should 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 are processed.

This policy covers the process for the destruction of this data in order to comply with this article and also covers the secure disposal of media storage hardware.

**Policy**

1. The Data Privacy Lead is responsible for arranging the destroying of data once it has reached the end of the retention period specified in The Data Retention Policy 5.01, or when an erasure request has been verified as required in the Request for Erasure policy 5.06.
2. Destruction must be completed within **20 working days** of the planned retention period or without undue delay following an Erasure request.
3. Destruction is handled as follows:

a. Paper Files – We operate a clean desk policy, therefore any unwanted ***or*** retention-expired paper files that contain personal data should be either placed into the confidential waste bins to be shredded ***or*** shredded immediately.
b. Emails – Any emails containing personal data ***and*** where the retention period has expired should be deleted from your Outlook 'Inbox', and then deleted from your 'Deleted Items' folder.
c. Files saved on server or desktop (including word, excel, PDF etc.) – you should either:
   i. Pseudonymise the data to ensure it can't be traced back to an individual; ***or***
   ii. Delete the document by deleting it from its 'Folder', and then deleting it from the 'Recycle Bin' folder.
d. CRM Systems, Cloud Storage Programmes – you should either:
   i. Pseudonymise the data to ensure it can't be traced back to an individual; ***or***
   ii. Delete the document by deleting it from its 'Folder', and then deleting it from the 'Recycle Bin' folder (if applicable).

4. The role of **Data Privacy Lead** is responsible for managing the secure disposal of all storage media. This includes-

a. Hard disks must be cleared of all software and all organisation information prior to disposal.
b. Portable or removable storage media are cleared prior to disposal.
c. Documents containing personal data are shredded by organisation, using a shredder with an appropriate security classification or sent to an approved secure shredding contractor. Any shredding done at organisation premises is removed by an approved contractor.

5. The **Data Privacy Lead** must retain a log showing the media destroyed and/or disposed of, and the date of disposal - 5.11.01. The Personal Data summary should be updated once the asset has been disposed as applicable.
6. All physical electronic storage media must be disposed of in line with the UK Waste Electric and Electronic Equipment (WEEE) Regulations 2013.

## 6.01 – Employment Contracts

The following provides details of the privacy requirements for employment contracts.

Article 32 requires an “appropriate” level of security based on the state of the art and costs of implementation, processing activities, and risk of varying likelihood and severity to individuals' rights and freedoms. Also, Article 29 indicates that Data Processors and staff of Data Controllers and Data Processors must only process personal data in accordance with the Data Controller instructions or legal requirements.

### Employment contracts privacy requirements

The organisations executes a regular audit to ensure security of processing. For this purpose three important elements are reviewed:

- ✓ Employment contracts include non-disclosure agreements and privacy policies to ensure that employees that have access to personal data will undertake all possible measures to protect it and comply with General Data Protection Regulation’s principles.
- ✓ Identity access management: the organisation has a register of employees and contractors detailing access rights to IT systems and data.
- ✓ Access of personal data is limited to agreed roles and responsibilities.

## 6.02 – Client Contracts Summary

The following provides details regarding the clients’ contracts.

Article 6(1)(b) gives a lawful basis for processing where “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. Also, this Article establishes that the legal basis must be recorded, therefore, in the case of contractual performance as a legal basis the copies of contracts or requests to enter a contract should be stored in order to demonstrate accountability.

**The organisation has concluded that the processing is necessary provided that:**

- ✓ There is a current contract with the individual and processing their personal data is needed to comply with the obligations under the contract.
- ✓ The client has asked us to do something as a first step (e.g. provide a quote) and therefore processing their personal data is needed.