**CAV Systems Group Limited**

**Data Protection Policy & Procedures**



***Revision History***

|  |  |  |  |
| --- | --- | --- | --- |
| ***Version*** | ***Revision Date*** | ***Revised by*** | ***Section Revised*** |
| 1.0 | 17.05.2018 | P Watson | Whole Document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

***Document Control***

|  |  |  |  |
| --- | --- | --- | --- |
| ***Document Owner:***  **Richard Lowery** | ***Document No:***  ***1.0*** | ***Status:***  Approved | ***Date Approved:***  ***17 May 2018*** |
|  | | | |
| ***Security Classification:***  High | ***Next Review Date:***  ***TBC*** | ***Version:***  V1.0 | ***Department:***  CAVSS |

Contents

[1 Policy Statement 5](#_Toc513043894)

[2 Purpose 5](#_Toc513043895)

[3 Scope 5](#_Toc513043896)

[3.1 Definitions 5](#_Toc513043897)

[4 Data Protection Background 7](#_Toc513043898)

[4.1 National Data Protection Law 7](#_Toc513043899)

[4.2 General Data Protection Regulation (GDPR) 7](#_Toc513043900)

[4.2.1 Personal Data 7](#_Toc513043901)

[4.2.2 The GDPR Principles 8](#_Toc513043902)

[4.3 The Information Commissioner’s Office (ICO) 8](#_Toc513043903)

[4.4 Data Protection Officer 9](#_Toc513043904)

[5 Objectives 9](#_Toc513043905)

[6 Governance Procedures 11](#_Toc513043906)

[6.1 Accountability & Compliance 11](#_Toc513043907)

[6.1.1 Data minimisation 11](#_Toc513043908)

[6.1.2 Encryption 11](#_Toc513043909)

[6.1.3 Restriction 11](#_Toc513043910)

[6.1.4 Information Audit 12](#_Toc513043911)

[6.2 Legal Basis for Processing 12](#_Toc513043912)

[6.2.1 Processing Special Category Data 13](#_Toc513043913)

[6.2.2 Records of Processing Activities 13](#_Toc513043914)

[6.3 Third-Party Processors 14](#_Toc513043915)

[6.4 Data Retention & Disposal 15](#_Toc513043916)

[7 Data Protection Impact Assessments 15](#_Toc513043917)

[8 Data Subject Rights Procedures 16](#_Toc513043918)

[8.1 Consent & The Right to be Informed 16](#_Toc513043919)

[8.1.1 Consent Controls 16](#_Toc513043920)

[8.1.2 Alternatives to Consent 17](#_Toc513043921)

[8.1.3 Information Provisions 17](#_Toc513043922)

[8.2 Privacy Notice 18](#_Toc513043923)

[8.3 Personal Data Not Obtained from the Data Subject 19](#_Toc513043924)

[8.3.1 Employee Personal Data 19](#_Toc513043925)

[8.4 The Right of Access 19](#_Toc513043926)

[8.4.1 Subject Access Request 19](#_Toc513043927)

[8.5 Data Portability 20](#_Toc513043928)

[8.6 Rectification & Erasure 20](#_Toc513043929)

[8.6.1 Correcting Inaccurate or Incomplete Data 20](#_Toc513043930)

[8.6.2 The Right to Erasure 21](#_Toc513043931)

[8.7 The Right to Restrict Processing 21](#_Toc513043932)

[8.8 Objections 21](#_Toc513043933)

[9 Oversight Procedures 22](#_Toc513043934)

[9.1 Security & Breach Management 22](#_Toc513043935)

[10 Transfers & Data Sharing 22](#_Toc513043936)

[11 Monitoring 23](#_Toc513043937)

[12 Training 23](#_Toc513043938)

[13 Penalties 23](#_Toc513043939)

[14 Responsibilities 23](#_Toc513043940)

# Policy Statement

**CAV Systems Group Limited** *(hereinafter referred to as the* ***“Group”****)* needs to collect personal information to effectively carry out our everyday business functions and activities and to provide the products and services defined by our business type. Such data is collected from employees, suppliers and customers and may include *(but is not limited to),* name, address, email address, data of birth, IP address, identification numbers, private and confidential information, sensitive information and bank/credit card details.

In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to processing all personal information in accordance with the ***General Data Protection Regulation (GDPR)***, ***UK data protection laws*** and any other relevant the data protection laws and codes of conduct *(herein collectively referred to as* ***“the data protection laws”****).*

The Group has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the data protection laws and principles, including staff training, procedure documents, audit measures and assessments. Ensuring and maintaining the security and confidentiality of personal and/or special category data is one of our top priorities.

# Purpose

The purpose of this policy is to ensure that the Group meets its legal, statutory and regulatory requirements under the data protection laws and to ensure that all personal and special category information is processed in a compliant manner, and in the individual’s best interests.

Data protection laws include provisions that promote accountability and governance and as such the Group has put comprehensive and effective governance measures in place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data. This policy also serves as a reference document for employees and third parties on the responsibilities of handling and accessing personal data and data subject requests.

# Scope

This policy applies to all staff within the Group *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Group in the UK or overseas).* Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

## Definitions

* ***“Biometric data”*** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or fingerprint data.
* ***“Binding Corporate Rules”*** means personal data protection policies which are adhered to by the Group for transfers of personal data to a controller or processor in one or more third countries or to an international organisation.
* ***“Consent”*** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
* ***“Cross Border Processing”*** means processing of personal data which: -
  + takes place in more than one country; or
  + substantially affects or is likely to affect data subjects in more than one country.
* ***“Data 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 country or state laws, the controller or the specific criteria for its nomination may be provided for by such laws.
* ***“Data processor”*** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
* ***“Data protection laws”*** means for the purposes of this document, the collective description of the GDPR, Data Protection Act 1998 and any other relevant data protection laws that the Group complies with.
* ***“Data subject”*** means an individual who is the subject of personal data.
* ***“GDPR”*** means the *General Data Protection Regulation (EU) (2016/679)*.
* ***“Genetic data”*** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
* ***“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.
* ***“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.
* ***“Recipient”*** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
* ***“Supervisory Authority”*** means an independent public authority which is established by a Member State.
* ***“Third Party”*** means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority.

# Data Protection Background

The Data Protection Act 1984 was originally in place in the UK to regulate the use of processed information that related to individuals. However, in 1995 the introduction of EU Directive 95/46/EC which set aims and requirements for member states on the protection of personal data when processing or sharing, meant an updated Act was required.

The UK subsequently developed and enacted The Data Protection Act 1998 (DPA) to ensure that British law complied with the EU Directive and to provide those with obligations under the Act with updated rules, requirements and guidelines for processing and sharing personal data.

2018 marks the 20th anniversary of the DPA enactment and whilst there have been periodical additions or alterations to the Act, technology has advanced at a far faster rate, necessitating new regulations for the current digital age. The past 20 years has also seen a vast increase in the number of businesses and services operating across borders, further highlighting the international inconsistency in Member States data protection laws.

For this reason, in January 2012, the European Commission proposed a new regulation applying to all EU Member States and bringing a standardised and consistent approach to the processing and sharing of personal information across the EU.

## National Data Protection Law

As the Group is in the UK, we are obligated under the GDPR and the UK’s Data Protection Bill that implements the GDPR into UK law. Our data protection policies and procedures adhere to both the GDPR and Data Protection Bill requirements, as applicable to our business type.

## General Data Protection Regulation (GDPR)

The ***General Data Protection Regulation (GDPR)*** ***(EU)2016/679)*** was approved by the European Commission in April 2016 and will apply to all EU Member States from 25th May 2018. As a *'Regulation*' rather than a *'Directive'*, its rules apply directly to Member States, replacing their existing local data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation.

As the Group processes personal information regarding individuals (*data subjects*), we are obligated under the General Data Protection Regulation (GDPR) to protect such information and to obtain, use, process, store and destroy it, only in compliance with its rules and principles.

### Personal Data

Information protected under the GDPR is known as *“personal data”* and is defined as:

*“Any information relating to an identified or identifiable natural person; 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.”*

The Group ensures that a high level of care is afforded to personal data falling within the GDPR’s **‘special categories’** *(previously* ***sensitive personal data***), due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

In relation to the ‘Special categories of Personal Data’ the GDPR advises that:

*“Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies.”*

### The GDPR Principles

Article 5 of the GDPR requires that 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’).***

***Article 5(2)*** requires that *‘the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles’* ***(‘accountability’)*** and requires that firms ***show how*** they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

## The Information Commissioner’s Office (ICO)

The Information Commissioner’s Office (ICO) is an independent regulatory office which reports directly to Parliament and whose role it is to uphold information rights in the public interest. The legislation they have oversight for includes: -

* The Data Protection Act 1998 *(pre-25th May 2018)*
* General Data Protection Regulation *(post-25th May 2018)*
* The Privacy and Electronic Communication (EU Directive) Regulations 2003
* Freedom of Information Act 2000
* The Environmental Information Regulations 2004

The ICO's mission statement is *“to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals”* and they can issue enforcement notices and fines for breaches in any of the Regulations, Acts and/or Laws regulated by them.

Under the data protection laws the ICO, as the UK's data protection authority (*Supervisory Authority*), will have a similar role as previously, when it comes to oversight, enforcement and responding to complaints with regards to the data protection laws and those firms located solely in the UK.

The Group’s UK trading companies CAV Ice Protection Limited and CAV Advanced Technologies Limited are registered with ICO and appear on the Data Protection Register as processorsof personal information.

Our Data Protection Registration Numbers are:

CAV Ice Protection Limited - Z2031703

CAV Advanced Technologies Limited - Z2031691

## Data Protection Officer

Articles 37-39, and Recital 97 of the GDPR detail the obligations, requirements and responsibilities on firms to appoint a Data Protection Officer and specifies the duties that the officer themselves must perform.

A Data Protection Officer (DPO) must be appointed by a firm where:

* The processing is carried out by a public authority or body *(except for courts acting in their judicial capacity)*
* the core activities of the controller/processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale
* the core activities of the controller/processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10

As the Group does not fall within these requirements a DPO has not been appointed. However this policy decision will be kept under review and a decision to appoint a DPO on a voluntary basis may be considered in the future.

# Objectives

We are committed to ensuring that all personal data processed by the Group is done so in accordance with the data protection laws and principles, along with any associated regulations and/or codes of conduct laid down by the Supervisory Authority and local law. We ensure the safe, secure, ethical and transparent processing of all personal data and have stringent measures to enable data subjects to exercise their rights.

The Group has developed the below objectives to meet our data protection obligations and to ensure continued compliance with the legal and regulatory requirements.

The Group aims to ensure that:

* We protect the rights of individuals with regard to the processing of personal information
* We develop, implement and maintain a data protection policy, procedures, audit plan and training program for compliance with the data protection laws
* Every business practice, function and process carried out by the Group is monitored for compliance with the data protection laws and principles
* Personal data is only processed where we have verified and met the lawfulness of processing requirements
* We only process special category data in accordance with the GDPR requirements and in compliance with the Data Protection Bill Schedule 1 conditions
* We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested
* Employees are competent and knowledgeable about their GDPR obligations and are provided with training in data protection laws, principles, regulations and how they apply to their specific role and the Group
* Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection laws
* We monitor compliance with the data protection laws to identify gaps and non-compliance before they become a risk, taking action where necessary
* We monitor the Supervisory Authority, European Data Protection Board (EDPB) and any GDPR news and updates, to stay abreast of changes, notifications and additional requirements
* We have robust and documented Complaints Handling and Data Breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regard to data protection
* We have appointed a Responsible Person who takes responsibility for the overall supervision, implementation and ongoing compliance with the data protection laws and performs specific duties as set out under Article 37 of the GDPR
* We monitor compliance with our data protection policies, procedures and the relevant regulations
* We provide clear reporting lines and supervision with regard to data protection
* We store and destroy all personal information, in accordance with our retention policy and schedule which has been developed from legal, regulatory and statutory requirements and suggested timeframes
* Any information provided to an individual in relation to personal data held or used about them will be in a concise, transparent, intelligible and easily accessible form, using clear and plain language
* Employees are aware of their own rights under the data protection laws and are provided with a Privacy Notice
* Where applicable, we maintain records of processing activities
* We have developed and documented appropriate technical and organisational measures and controls for personal data security and have a robust Information Security program in place

# Governance Procedures

## Accountability & Compliance

We have implemented adequate and appropriate technical and organisational measures to ensure the safeguarding of personal data and compliance with data protection laws and we can evidence such measures through our documentation and practices.

Our main governance objectives are to:

* Educate senior management and employees about the requirements of data protection laws and the potential impact of non-compliance
* Provide a dedicated and effective data protection training program for relevant employees
* Identify key stakeholders to support data protection compliance
* Allocate responsibility for data protection compliance and ensure that the designated person(s) has sufficient access, support and budget to perform the role
* Identify, create and disseminate the reporting lines within the data protection governance structure

The technical and organisational measures that the Group has in place to ensure and demonstrate compliance with data protection laws, regulations and codes of conduct, are detailed in this document and associated information security policies.

### Data minimisation

The data that we hold and process should be *'limited to what is necessary'*.

We only ever obtain, retain, process and share the data that is essential for carrying out our services and/or meeting our legal obligations and only retain data for as long as is necessary.

Our systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data minimisation enables us to reduce data protection risks and breaches, and supports our compliance with data protection laws.

### Encryption

We utilise encryption as a further risk prevention measure for securing the personal data that we hold.

### Restriction

We use Group-wide restriction methods for all personal data activities. Restricting access is built into the foundation of the Group’s processes, systems and structures and ensures that only those with authorisation and/or a relevant purpose have access to personal information.

### Information Audit

To enable the Group to fully prepare for and comply with data protection laws, we have carried out a Group-wide data protection information audit to better enable us to record, categorise and protect the personal data that we hold and process.

The audit has identified, categorised and recorded all personal information obtained, processed and shared by our Group in our capacity as a controller/processor and has been compiled on a central register which includes:

* What personal data we hold
* Where it came from
* Who we share it with
* Legal basis for processing it
* What format(s) is it in
* Who is responsible for it?

## Legal Basis for Processing

At the core of all personal information processing activities undertaken by the Group is the assurance and verification that we are complying with Article 6 of the GDPR and our lawfulness of processing obligations. Prior to carrying out any personal data processing activity, we identify and establish the legal basis for doing so and verify these against the regulation requirements to ensure we are using the most appropriate legal basis.

The legal basis is documented on our information audit register and in our Privacy Notice and, where applicable, is provided to the data subject and Supervisory Authority as part of our information disclosure obligations.

Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where:

* The data subject has given consent to the processing of their personal data for one or more specific purposes
* Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
* Processing is necessary for compliance with a legal obligation to which we are subject
* Processing is necessary in order to protect the vital interests of the data subject or of another natural person
* Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Group
* Processing is necessary for the purposes of the legitimate interests pursued by the Group or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data)

### Processing Special Category Data

Special categories of Personal Data are defined in the data protection laws as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

Where the Group processes any personal information classed as special category or information relating to criminal convictions, we do so in accordance with Article 9 of the GDPR regulations and in compliance with the Data Protection Bill's Schedule 1 Parts 1, 2, 3 & 4 conditions and requirements.

We will only ever process special category data where:

* The data subject has given explicit consent to the processing of the personal data
* Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
* Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
* Processing is carried out in the course of its legitimate activities with appropriate safeguards
* Processing relates to personal data which are manifestly made public by the data subject
* Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
* Processing is necessary for reasons of substantial public interest
* Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care
* Processing is necessary for reasons of public interest in the area of public health
* Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)

The Data Protection Bill provides specific conditions and circumstances when special category personal data can be processed and it details the requirements that organisations are obliged to meet when processing such data.

Where the Group processes personal information that falls into one of the above categories, we have adequate and appropriate provisions and measures in place.

### Records of Processing Activities

As an organisation with less than 250 employees, the Group is not required to maintain records of our processing activities. However, should the Group increase in size we will begin to record such information as detailed in GDPR Article 30 if and when:

* We employee 250 or more employees
* Processing personal data could result in a risk to the rights and freedoms of individual
* The processing is not occasional
* We process special categories of data or criminal convictions and offences
* Such records are maintained in writing, are provided in a clear and easy to read format and are readily available to the Supervisory Authority upon request.

## Third-Party Processors

The Group utilises external processors for certain processing activities. We monitor the personal data that is processed outside of the Group, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible. Such external processing includes (but is not limited to):

* Payroll and pension
* IT Hosting Services and Email Servers
* Health and safety and 0ccupational health services
* Insurance company

We assess all processors prior to forming a business relationship. We obtain Group documents, certifications, references and ensure that the processor is adequate, appropriate and effective for the task we are employing them for.

We monitor processes and activities during the contract period to ensure compliance with the data protection regulations and we review any codes of conduct that they have signed up to in order to confirm compliance.

The continued protection of data subjects’ rights and the security of their personal information is always our top priority when choosing a processor and we understand the importance of adequate and reliable outsourcing for processing activities as well as our continued obligations under data protection laws for data processed and handled by a third party.

We work under service level agreements (SLAs) and contracts with processors covering:

* The processor’s data protection obligations
* Our expectations, rights and obligations
* The processing duration, aims and objectives
* The data subjects’ rights and safeguarding measures
* The nature and purpose of the processing
* The type of personal data and categories of data subjects

Each of the areas specified in the contract is monitored. Processors are notified that they shall not engage another processor without our prior specific authorisation and any intended changes concerning the addition or replacement of existing processors must be done in writing, in advance of any such changes being implemented.

The SLA and associated contract reflect the fact that the processor:

* Processes the personal data only on our documented instructions
* Seeks our authorisation to transfer personal data to a third country or an international organisation (*unless required to do so by a law to which the processor is subject*)
* Shall inform us of any such legal requirement to transfer data before processing
* Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
* Takes all measures to secure the personal data at all times
* Respects, supports and complies with our obligation to respond to requests for exercising the data subject's rights
* Assists the Group in ensuring compliance with our obligations for data security, mitigating risks, breach notification and privacy impact assessments
* When requested, deletes or returns all personal data to the Group after the end of the provision of services relating to processing, and deletes existing copies where possible
* Makes available to the Group all information necessary to demonstrate compliance with the obligations set out in the agreement and contract
* Allows and supports audits, monitoring, inspections and reporting as set out in the contract
* Informs the Group immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract

## Data Retention & Disposal

The Group has defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and our business requirements, as well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects *(e.g. shredding, disposal as confidential waste, secure electronic deletion)* and prioritises the protection of the personal data in all instances*.*

# Data Protection Impact Assessments

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by the Group.

Where the Group is considering carrying out processing that utilises new technologies, and/or where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, we will carry out a Data Protection Impact Assessment *(also known as a Privacy Impact Assessment*).

We consider processing that is likely to result in a high risk to include:

* Those involving the use of new technologies
* New processing activities not previously used
* Processing activities making it difficult for the data subject(s) to exercise their rights

Carrying out these assessments enables us to identify the most effective way to comply with our data protection obligations and ensure the highest level of data privacy when processing. It allows us to assess the impact and risk before carrying out the processing, thus identifying and correcting issues at the source, reducing costs, breaches and risks.

The aim of solutions and mitigating actions for all risks is to ensure that the risk is either:

* Eliminated
* Reduced
* Accepted

# Data Subject Rights Procedures

## Consent & The Right to be Informed

The collection of personal and sometimes special category data is fundamental to the activities of the Group and we therefore have specific measures and controls in place to ensure that we comply with the conditions for consent under the data protection laws.

Data protection law defines consent as; *‘Any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her’.*

Where processing is based on consent, all consent mechanisms have reviewed and revised to ensure that:

* Consent requests are transparent, using plain language and exclude unintelligible terms, jargon or extensive legal terms
* Consent is freely given, specific and informed, as well as being an unambiguous indication of the individual’s wishes
* Consent is always given by a statement or a clear affirmative action (*positive opt-in*) which signifies agreement to the processing of personal data
* Pre-ticked, opt-in boxes are **never** used
* Where consent is given as part of other matters (*i.e. terms & conditions, agreements, contracts*), we ensure that the consent is separate from the other matters and is **not** be a precondition of any service (*unless necessary for that service)*
* We will provide details of any other third party who will use or rely on the consent
* Consent is always verifiable, and we have controls in place to ensure that we can demonstrate consent in every case
* We keep detailed records of consent and can evidence at a minimum:
  + that the individual has consented to the use and processing of their personal data
  + that the individual has been advised of any third party using the data
  + what the individual was told at the time of consent
  + how and when consent was obtained
* We have ensured that withdrawing consent is as easy, clear and straightforward as giving it
* Consent withdrawal requests are processed immediately and without detriment
* For special category data, the consent obtained is explicit with the processing purpose(s) always being specified

### Consent Controls

The Group maintains records of data subject consent for processing personal data and is able to demonstrate that the data subject has consented to processing of his or her personal data where applicable. We also ensure that the withdrawal of consent is as clear, simple and transparent and is documented in all instances.

Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent is presented in a manner which is clearly distinguishable from those matters, in an intelligible and easily accessible form, using clear and plain language.

Consent to obtain and process personal data is obtained through:

* Face-to-Face meeting
* By Telephone
* In Writing
* E-mail
* Electronic form *(e.g. via website form*)

Any electronic methods of gaining consent are regularly reviewed and tested to ensure that a compliant Privacy Notice is accessible and displayed and that consent is clear, granular and utilises a demonstrable opt-in mechanism. Where consent is obtained verbally, we utilise scripts, checklists to ensure that all requirements have been met and that consent is obtained compliantly and can be evidenced.

Electronic consent is always by a non-ticked, opt-in action (*or double opt-in where applicable*), enabling the individual to provide consent after the below information has been provided. This is then followed up with an email, SMS or written confirmation of the consent to process, store and share the personal information.

Privacy Notices are used in all forms of consent and personal data collection, to ensure that we are compliant in disclosing the information required in the data protection laws in an easy to read and accessible format.

### Alternatives to Consent

There are six lawful bases for processing and consent is not always the most appropriate option. We have reviewed all processing activities and only use consent as an option where the individual has a choice.

When reviewing the processing activity for compliance with the consent requirements, we ensure that none of the following situations occurs:

* Where we ask for consent but still process data even if it was not given *(or withdrawn).* If we would still process the data under an alternative lawful basis regardless of consent, we recognise it is not the correct lawful basis to use
* Where we ask for consent to process personal data as a precondition of a service we are offering, it is not given as an option and consent is not appropriate
* Where there is an imbalance in the relationship, e.g. with employees

### Information Provisions

Where personal data is obtained directly from the individual *(i.e. through consent, by employees, written materials and/or electronic formats*), we provide the following information in the form of a Privacy Notice:

* The identity and the contact details of the controller and, where applicable, of the controller's representative
* The purpose(s) of the processing for which the personal information is intended
* The legal basis for the processing
* The recipients or categories of recipients of the personal data *(if applicable)*
* The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
* The existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
* Where relevant, the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
* The right to lodge a complaint with the Supervisory Authority
* Whether providing personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data

This information is provided to the data subject at the time the information is collected and records pertaining to the consent obtained are maintained and stored for 6 years from the date of consent, unless there is a legal requirement to keep the information longer.

## Privacy Notice

A Privacy Notice is a document, form, webpage or pop-up that is provided to individuals at the time their personal data is collected (or at the earliest possibility where that data is obtained indirectly).

Our Privacy Notice provides individuals with all the necessary and legal information about how, why and when we process their data, along with their rights and obligations.

We have a link to our Privacy Notice on our website and we will provide copies of physical and digital formats upon request. For enquiries from customers this is the means by which we provide the legal information on how we handle, process and disclose their personal information.

The notice is easily accessible, legible, jargon-free and is available in several formats, dependent on the method of data collection:

* Via our website
* Linked to or written in full in the footer of emails
* Worded in full in agreements, contracts, forms and other materials where data is collected in writing or face-to-face
* In employee contracts and recruitment materials
* Printed media, adverts and financial promotions
* Digital Products/Services

Where we rely on consent to obtain and process personal information, we ensure that it is:

* Displayed clearly and prominently
* Asks individuals to positively opt-in
* Gives them sufficient information to make an informed choice
* Explains the different ways we will use their information
* Provides a clear and simple way for them to indicate they agree to different types of processing
* Includes a separate unticked opt-in box for direct marketing

## Personal Data Not Obtained from the Data Subject

Where the Group obtains and/or processes personal data that has **not** been obtained directly from the data subject, we must ensure that we inform the data subject within 30 days of our obtaining the personal data *(except for advising if the personal data is a statutory or contractual requirement).*

### Employee Personal Data

Under data protection law, we do not use consent as a legal basis for obtaining or processing employee personal information. Our HR policies have been updated to ensure that employees are provided with the appropriate information disclosure and are aware of how we process their data and why.

All employees are provided with our Staff Handbook which informs them of their rights under data protection laws and how to exercise these rights and are provided with a Privacy Notice specific to the personal information we collect and process about them.

## The Right of Access

We have ensured that appropriate measures have been taken to provide information on rights of access to personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject’s identity *(i.e. verbally, electronic*).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

### Subject Access Request

Where a data subject asks us to confirm whether we hold and process personal data concerning him or her and requests access to such data; we provide them with:

* The purposes of the processing
* The categories of personal data concerned
* The recipients or categories of recipient to whom the personal data have been or will be disclosed
* If the data has or will be disclosed to (an)other country(ies) or international organisations and the appropriate safeguards pursuant to the transfer
* Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
* The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
* The right to lodge a complaint with a Supervisory Authority
* Where personal data has not been collected from the data subject, any available information as to the source and provider

Subject Access Requests (SARs) are recorded as soon as received. SARs are targeted for completion within 30 days and are provided free of charge. Where the individual makes the request by electronic means, we provide the information in a commonly used electronic format, unless an alternative format is requested.

## Data Portability

The Group will provide personal information pertaining to a data subject to them on request and in a format that is easy to disclose and read.

Where requested by a data subject, we will transmit the personal data directly from the Group to a designated controller, where technically feasible.

Requests for information to be provided to the data subject or a designated controller are done so free of charge and within 30 days of the request being received. If for any reason, we do not act in responding to a request, we provide a full, written explanation within 30 days to the data subject or the reasons for refusal and of their right to complain to the supervisory authority and to a judicial remedy.

All transmission requests under the portability right are assessed to ensure that no other data subject is concerned. Where the personal data relates to more individuals than the subject requesting the data/transmission to another controller, this is always without prejudice to the rights and freedoms of the other data subjects.

## Rectification & Erasure

### Correcting Inaccurate or Incomplete Data

Data held and processed by the Group is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data subject or controller informs us that the data we hold is inaccurate, we will take all reasonable steps to ensure that such inaccuracies are corrected with immediate effect.

The Responsible Person is notified of the data subject’s request to correct personal data and is responsible for validating the information and rectifying errors where they have been notified. The information is altered as directed by the data subject, with checks made to ensure that all data relating to the subject is corrected where incomplete or inaccurate.

Where notified of inaccurate data by the data subject, we will aim rectify the error within 30 days and inform any third party of the rectification if we have disclosed the personal data in question to them. The data subject will be informed in writing of the correction and, where applicable, provided with the details of any third party to whom the data has been disclosed.

If for any reason, we are unable to act in response to a request for rectification and/or completion, we will provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

### The Right to Erasure

Also, known as *‘The Right to be Forgotten’*, the Group ensures that personal data which identifies a data subject is not kept longer than is necessary for the purposes for which the personal data is processed.

All personal data obtained and processed by the Group is categorised and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

## The Right to Restrict Processing

There are certain circumstances where the Group restricts the processing of personal information to validate, verify or comply with a legal requirement of a data subject’s request. Restricted data is removed from the normal flow of information.

The Group will apply restrictions to data processing in the following circumstances:

* Where an individual contests the accuracy of the personal data and we are in the process verifying the accuracy of the personal data and/or making corrections
* Where an individual has objected to the processing (*e.g. where it is necessary for the performance of a public interest task or purpose of legitimate interest*), and we are considering whether we have legitimate grounds to override those of the individual
* When processing is deemed to have been unlawful, but the data subject requests restriction as oppose to erasure
* Where we no longer need the personal data, but the data subject requires the data to establish, exercise or defend a legal claim

The Responsible Person reviews and authorises all restriction requests and actions and retains copies of notifications from and to data subjects and relevant third parties. Where data is restricted, and we have disclosed such data to a third party, we will inform the third-party of the restriction in place and the reason. We will also notify them if any restriction is subsequently lifted.

Data subjects who have requested restriction of data are informed within 30 days of the restriction application and are also advised of any third party to whom the data has been disclosed. We also notify the subject in writing of any decision to lift a restriction on processing. If, for any reason, we are unable to act in response to a request for restriction, we will provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

## Objections

Our Privacy Notices inform data subjects of their right to object to processing in and at the point of first communication, in a clear and legible form and separate from other information.

Individuals have the right to object to:

* Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority
* Direct marketing
* Processing for purposes of scientific/historical research and statistics

Where the Group processes personal data for the performance of a legal task, in relation to legitimate interests or for research purposes, a data subject’s objection will only be considered where it is on *'grounds relating to their particular situation'*. We reserve the right to continue processing such personal data where:

* We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
* The processing is for the establishment, exercise or defence of legal claims

Where we are processing personal information for direct marketing purposes under a previously obtained consent, we will stop processing such personal data immediately where an objection is received from the data subject (effectively a withdrawal of consent).

Where a data subject objects to data processing on valid grounds, the Group will cease the processing for that purpose and advise the data subject of cessation in writing within 30 days of the objection being received.

# Oversight Procedures

## Security & Breach Management

We ensure the maximum security of data that is processed, including when it is shared, disclosed and transferred. Our information security policies provide the detailed measures and controls that we take to protect personal information and to ensure its security from consent to disposal.

We have implemented adequate and appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Whilst every effort and measure are taken to reduce the risk of data breaches, the Group has dedicated controls and procedures in place for such situations, along with the notifications to be made to the Supervisory Authority and data subjects (where applicable).

# Transfers & Data Sharing

The Group takes proportionate and effective measures to protect personal data held and processed by us at all times. However we recognise the high risk nature of disclosing and transferring personal data and as such, we place a priority on the protection and security of data being transferred.

Where data is being transferred for a legal and necessary purpose we ensure such data is encrypted and where possible is also subject to the principle of data minimisation. We use approved, secure methods of transfer.

# Monitoring

This policy and procedure document details the controls, measures and methods used by the Group to protect personal data, uphold the rights of data subjects, mitigate risks, minimise breaches and comply with the data protection laws and associated laws and codes of conduct. In addition to these, we also monitor compliance with a view to ensuring that the measures and controls in place to protect data subjects and their information are adequate, effective and compliant at all times.

# Training

We ensure that relevant staff understand, have access to and can easily interpret data protection laws and principles and that they have access to training as necessary.

# Penalties

The Group understands the Supervisory Authority’s power to impose and enforce fines and penalties where we fail to comply with the regulations and operate in a knowingly non-compliant manner.

We recognise that:

* Breaches of the obligations are subject to administrative fines up to €10,000,000 or 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
* Breaches of the basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international organisation, specific processing situations or non-compliance with an order by the Supervisory Authority, are subject to administrative fines up to €20,000,000 or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

# Responsibilities

The Group has appointed a Responsible Person whose role is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and senior management and to actively stay informed and up-to-date with all legislation and changes relating to data protection.

The Responsible Person will work in conjunction with the VP of Business Improvement and the IT Manager to ensure that all processes, systems and staff are operating in compliance with the requirements of data protection laws and principles.