DATA PROTECTION POLICY

In compliance with the General Data Protection Regulations (GDPR)

CONTENTS

DATA PROTECTION POLICY STATEMENT

The Company commits to protect personal data and to comply with the Six Data Protection Principals and to fulfilling the Eight Individual Rights in regards the retention and storage of personal data.

The company will, in compliance with Article 5 of the General Data Protection regulations ensure that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date: Every reasonable step must be taken to ensure that personal data that is inaccurate is either rectified or erased without delay;

e) 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; and

f) 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.

To enable this commitment, we have appointed a Director with responsibility for data protection, and a Data Controller who if the Accounts & Administration Manager for ensuring day-to-day compliance and dealing with information requests and the Information Commissioners Office. The company is exempt from appointing a Data Protection Officer.

We have produced a Data Privacy Register which documents the personal data that we hold and the basis for retention.

We will ensure that all data is kept secure, and that we have defined Information Security Policies which include for cyber security and data transfer protocols.

The company will maintain registration with the Information Commissioners Officer for the use of CCTV cameras for crime surveillance.

We will communicate the responsibilities of individuals through induction and Contracts of Employment, briefings and to sub-contractors through Supplier Terms and Conditions.

We will review this policy as part of change planning (eg to external requirements, changes in organisation, developments in information technology and cyber security, knowledge transfer / lessons, following any personal data breach and periodically every three years.

As Director responsible for data protection I approve this policy,

Signed

Martin Rush, Managing Director 03 March 2021

SCOPE AND PURPOSE OF GDPR AND THIS DOCUMENT

General Data Protection Regulation (GDPR) 2015 and Data Protection regulations 2018.

From the organisational perspective, businesses must comply with the Six Data Protection Principals and fulfil the Nine Individual Rights. This includes rules regarding information and what is collected, why, how it is used and how it is managed. This also includes ensuring data is stored and processed in a secure manner, and with respect for the individual's rights.

From an individual's perspective, GDPR is about providing with a degree of control over the way businesses and other organisations use their personal data, giving them certain rights, which are legally enforceable.

The below policy and procedures are based on the Information Commissioners Guide to the General Data Protection Regulation https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

SUMMARY OF THE REQUIREMENTS OF THE GENERAL DATA PROTECTION REGULATIONS [GDPR]

The Six Data Protection Principals

1. Lawfulness, Fairness and Transparency (including consent)
2. Purpose Limitation
3. Data Minimisation
4. Accuracy
5. Storage Limitation
6. Integrity and Confidentiality systems[1]

Note 1: This includes effective and secure IT systems and for paper documents physical security. See separate Information Security Policy. The ICO reference the government Cyber Essentials scheme is a Cyber Security Assurance Scheme which is becoming a mandatory requirement for many Buyers who have ISO27001 Information Security certification and for public sector contracts. https://www.cyberessentials.ncsc.gov.uk/

The Lawful Bases for Data Processing

The lawful basis for processing are set out in Article 6 of the GDPR.

#	Lawful Basis	Description	Example
1.	Consent	The individual has given clear consent for the company to process their personal data for a specific purpose. This "Explicit Consent" is required only if Items 2-6 below don't apply eg for Direct Marketing purposes, where a Privacy Statement is required with explicit opt-in.	Direct Marketing
2.	Contract	The processing is necessary for a contract the company have with the individual, or because they have asked the company to take specific steps before entering into a contract.	Employment Contract Commercial Contract
3.	Legal Obligation	The processing is necessary for the company to comply with the law (not including contractual obligations).	Health & Safety Protection of Vulnerable Persons
4.	Vital Interests	The processing is necessary to protect someone's life.	Health / Medical Restrictions

5.	Public Task	The processing is necessary for the company to perform a task in the public interest or for the company official functions, and the task or function has a clear basis in law.	This basis is not applicable to most businesses
6.	Legitimate interests	The processing is necessary for the company legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.	Uses of an individual's data in ways they would reasonably expect, & which have a minimal privacy impact
7.	Special Categories	Anonymised data is held for equality & diversity monitoring purposes only.	Diversity Data

The Nine Rights of Users

1. The Right to be Informed
2. The Right of Access
3. The Right of Rectification
4. The Right to Erasure
5. The Right to Restrict Processing
6. The Right to Data Portability
7. The Right to Object
8. Rights in Relation to Automated Decision Making

Registration with The Information Commissioners Office (ICO)

Certain companies must register with the ICO as a Data Controller, for instance:

- Advertising, marketing and public relations for others
- Where CCTV is used for Crime Prevention;
- Where personal data on individuals from another organisations is held eg accountancy, consultancy, training and other activities.

If the company only holds the personal data of the company's own employees and customers for commercial transactions the company is exempt from registration.

Personal Data Breaches

All personal data breaches must be investigated, and higher risk breaches reported to the ICO, and high risk breaches also reported to the individual.

DEFINITIONS AND APPLICABILITY

Personal Data: The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. Due to the small size of the company there is a risk that anonymised, retracted or pseudonymised, eg key-coded, data could be attributed to an individual employee.

Data for Product Marketing Purposes: Due to the nature of the business, the business undertakes limited direct marketing activities. All customers are organisations, eg limited companies, public sector organisations. Where direct marketing is undertaken, it shall comply with the Consent Arrangements below.

Controller: Under GDPR the company is a controller of data. The company determines the purposes and means of processing personal data.

Individual: This may be an employee, ex-employee, self-employed worker, sub-contractor, customer (though most customers are limited companies).

Processing means doing any of the following with the information:

- obtaining it;
- recording it;
- storing it;
- updating it; and
- sharing it.

'Personal information' means any detail about a living individual that can be used on its own, or with other data, to identify them.

SCOPE OF COMPANY ACTIVITY REGARDING PERSONAL DATA PROTECTION

The company only hold data on its employees, contracted workers and customers so to fulfil it's contractual obligations, legal obligations, the vital interests of the individual and the legitimate interests of the company and the individuals.

The company does not undertake direct marketing eg by email.

The company does not undertake marketing or public relations for others.

The company does not hold personal data on individuals other than for:

- existing employees and contracted workers;
- potential employees and workers – applications may be held for 6 months;
- past employees and contracted workers – for specified health & safety reasons (See below)
- customers – for only the period applicable for the contract preparation, delivery and post-delivery eg warranty / guarantee period.

TABLE OF PERSONAL DATA HELD AND LAWFUL BASIS FOR ITS RETENTION (aka Data Privacy Register)

Data Set Name	Data Examples	Lawful Basis	Storage Method	Retention Period	Method of Disposal
Personnel Data for Safety Compliance	H&S data such as signed safety documentation, site audits, etc.	Legal: H&S Compliance Vital Interest: Protection of harm to the employee or through omission to others. Legitimate Interests: Insurance Accident Claims	Held on paper and electronic contract / project files, accessible to office staff only	3.5 years under injury insurance claim rules	Deletion from Server Hardcopy secure shredding Authority – Administration & Accounts Manager
	H&S data such as signed medical health self-declarations and medical fitness examinations, accident reports etc.	Legal: H&S Compliance Vital Interest: Protection of harm to the employee or through omission to others. Legitimate Interests: Insurance Accident Claims	Held on paper and electronic personnel files, accessible only to Administration & Accounts Manager.	3.5 years under injury insurance claim rules	Deletion from Server Hardcopy secure shredding Authority – Administration & Accounts Manager
	Drugs & Alcohol Test	Legal, Vital interest: Proof of fitness to work	Held on paper and electronic personnel files, accessible only to Administration & Accounts Manager.	10 years under railway industry rules.	Deletion from Server Hardcopy secure shredding Authority – Administration & Accounts Manager
	Driving license checks	Legal, Vital Interest, Legitimate Interest: Road Traffic Acts Consensual: Signed Mandate	Held on paper and electronic personnel files, accessible only to Administration & Accounts Manager.	3.5 years under injury insurance claim rules	Deletion from Server Hardcopy secure shredding Authority – Administration & Accounts Manager

Data Set Name	Data Examples	Lawful Basis	Storage Method	Retention Period	Method of Disposal
Personnel Data for Occupational Health Compliance	COSHH: Risk Assessments, Safety Data Sheets, Exposure Monitoring Results	Legal, Vital Interest, Legitimate Interest: Exposure to hazardous substances harmful to health – respiratory & other diseases	Held on paper Site Files, and server management system, accessible to office staff only	40 years under the CoSHH Regulations.	Deletion from Server Hardcopy secure shredding Authority – Administration & Accounts Manager
	COSHH: PPE Issue Forms, Face Fit Tests	Legal, Vital Interest, Legitimate Interest: Exposure to hazardous substances harmful to health – respiratory & other diseases	Held on paper and electronic personnel files, accessible only to Administration & Accounts Manager.	40 years under the CoSHH Regulations.	Deletion from Server Hardcopy secure shredding Authority – Administration & Accounts Manager
	Noise and vibration exposure data	Legal, Legitimate Interest: Exposure to hazardous physical agents harmful to health	Held on paper and electronic personnel files, accessible only to Administration & Accounts Manager.	40 years for Occupational Health purposes	Deletion from Server Hardcopy secure shredding Authority – Administration & Accounts Manager
Personnel Data for Human Resources	Employment contracts, personal details, training records, equality & diversity data, absence data, working time opt out agreement	Legal, Contractual, Legitimate Interests: Employment Law, Equality Acts	Held on paper and electronic personnel files, accessible only to Administration & Accounts Manager.	Duration of employee's employment plus six years in case of unfair employment claim	Deletion from Server Hardcopy secure shredding Authority – Administration & Accounts Manager
	Performance appraisal records, capability & disciplinary	Legitimate Interests: Employee Performance Review	Held on paper and electronic personnel files, accessible only to Administration & Accounts Manager and Line Manager.		
	Criminal offence data-	Legitimate Interests: Only processed for security clearance or DBS, not selection, see comment below.	The data is not usually held by the company as it is held in the clearance provider database with either a pass or fail outcome.	The data is not usually held by the company as it is held in the clearance provider database with	Not applicable

Data Set Name	Data Examples	Lawful Basis	Storage Method	Retention Period	Method of Disposal
				either a pass or fail outcome.	
Personnel data for payroll	Payroll payments	Legal: For payroll payment and income tax / national insurance purposes	Payroll system accessible only to Administration & Accounts Manager Financial Manager / Payroll Coordinator	6 Years after financial year end as per HMRC rules	Deletion from Server Hardcopy secure shredding Authority – Finance Manager
Personnel data for pension	Pension Payments and Policies	Contractual, Legitimate Interests	Pension data only available to: Administration & Accounts Manager Financial Manager Pension Provider	For life on Pension Policy	Deleted at expiry of Pension Policy or Withdrawal from Pension Scheme

Whilst not covered under GDPR, the company acknowledges that it holds Corporate Sensitive Data, whose loss or inaccuracy could damage the company. Corporate Sensitive Data, includes:

Data Set Name	Data Examples	Lawful Basis	Storage Method	Retention Period	Method of Disposal
Company Financial Data	Company accounts, Payments, Receipts etc	Legal: Companies Act & HMRC Rules	Finance system accessible only to Administration & Accounts Manager Financial Manager /	6 Years after financial year end as per HMRC rules	Deletion from Server Hardcopy secure shredding Authority – Finance Manager
Contract Commercial Data	Quotes, pricing and tender responses Supplier / Sub-Contractor Contracts	Contract: Customer and supplier contract reasons	Held on server management system, accessible to office staff only	6 Years after financial year end as per HMRC rules	Deletion from Server Hardcopy secure shredding Authority – Finance Manager
Company Compliance Performance	Accident Statistics, Prosecutions, Notices, Audit Findings etc	Contract, Legitimate Interest: Evidence of compliance to customers in PQQ and sector procurement	Held on server management system, accessible to office staff only	5 years in line with customer requirements	Deletion from Server Hardcopy secure shredding Authority – Administration &

Data		schemes			Accounts Manager
Customer Order data	Customer purchase orders	Contract, Legitimate Interest: Quality system & invoicing purposes	Held on server management system, accessible to office staff only	6 Years after financial year end as per HMRC rules	Deletion from Server Hardcopy secure shredding Authority – Administration & Accounts Manager

SPECIAL CATEGORY DATA

Special Category Data	Lawful Bases
Gender / Gender Identity; race; ethnicity; disability; parental / carer status; distance to home location	Legitimate Interests: Customers and the company are interested in the makeup of its workforce for equality and diversity monitoring purposes. Individual's completed Equality & Diversity Questionnaires will be retained as confidential documents. Anonymised data is published in PQQs.
Disability	Legitimate Interest: In been able to provide adaptions to work environments or conditions to permit as far as is reasonably practical the individual to work. Disability may be physical or mental. Vital Interest, Legal Obligation: certain safety critical works eg work on railways, highways, require individuals to achieve set medical fitness levels to protect their own H&S. Disability related data may be required to be shared with company appointed Occupational Health Practitioners, H&S Advisors, Line Managers, Supervisor's to enable a Safe System of Work to be produced. The Safe System of Work shall be signed by the individual to provide consent to communicate to the wider workforce or customer.
Health Genetics; Pregnancy.	Vital Interest – under Health & Safety Control of Substances Hazardous to Health (CoSHH) certain harmful substances can cause genetic, birth or growth (eg to new born breast fed baby) defects. Other health conditions eg asthma, dermatitis, allergies can be worsened by exposure to certain hazardous substances or work environment conditions eg arthritis in damp cold conditions. Consent is requested on the company Self-Assessment Medical Self Data may be required to be shared with company appointed Occupational Health Practitioners, H&S Advisors, Line Managers, Supervisor's to enable a Safe System of Work to be produced. The Safe System of Work shall be signed by the individual to provide consent to communicate to the wider workforce or customer.
Politics; religion; sex life; sexual orientation; transsexuality.	There is no lawful basis for individuals to declare this data, and this data will not be requested.
Trade union membership;	Legal Obligation – the company is legally obliged to recognise trade union membership, which the company does. It is the choice of individual whether to communicate this to the company or workforce.

EVALUATION OF PROCESSING FOR PURPOSES OTHER THAN LEGAL OBLIGATION, CONTRACT OR VITAL INTERESTS

If the company is processing for purposes other than legal obligation, contract or vital interests then the appropriate lawful basis may not be so clear cut, and in many cases the company will have a choice between using legitimate interests or consent. There are three data process activities this relates to in regards personal data, and these are evaluated below. The data process activities that require additional consideration are:

1. Employee Performance Monitoring
2. Validation of Driving Licenses on the DVSA Database

1. Employee Performance Monitoring	
1.1 Who does the processing benefit?	The employer in terms of employee performance monitoring, the employee in terms of performance feedback and improvement.
1.2 Would individuals expect this processing to take place?	Yes, employee performance monitoring is undertaken by all business.
1.3 What is your relationship with the individual?	Employer – Employee or Contracted Self-Employed Operative
1.4 Are you in a position of power over them?	Yes, as Employer
1.5 What is the impact of the processing on the individual?	Limited but positive– performance monitoring is done with positive aims of commending good behaviours and correcting bad behaviours.
1.6 Are they vulnerable?	Potentially in relation to possible mental health issues including stress or undiagnosed mental health / behavioural issues. This should be identified as a potential contributing factor and be picked up through Capability Review, rather than reactively through Disciplinary Review.
1.7 Are some of the individuals concerned likely to object?	No, employee performance monitoring is undertaken by all business.
1.8 Are you able to stop the processing at any time on request?	Unlikely, as usually done as part of employee performance review process.
1.9 Conclusion	Processing of personnel data for employee performance monitoring is a legitimate interest.

2. Validation of Driving Licenses on the DVSA Database: The DVSA require the drivers consent to access the data.	
(1) Who does the processing benefit?	The employer in terms of demonstrating corporate compliance to the Motor Vehicles (Driving Licences) Regulations 1999, so to permit employer to drive and comply with insurance requirements and avoid possible H&S / Corporate Manslaughter charges. The employee in terms of been permitted to undertake driving duties and be paid.
(2) Would individuals expect this processing to take place?	Likely, driving license validation is undertaken by many businesses.
(3) What is your relationship with the individual?	Employer – Employee or Contracted Self-Employed Operative
(4) Are you in a position of power over them?	Yes, as Employer
(5) What is the impact of the	Validation will permit the use of company vehicles but identification

processing on the individual?	of a high number of penalty points will incur more vigorous driver evaluation and performance monitoring. Drivers with six or more points on their license have to be reported to the company Motor Vehicle Insurance Provider, who will class them as High Risk Drivers, which will increase premiums and reduce the employee's reputation. Failure to have declared penalty points or bans is fraud and is likely to lead to dismissal, or at least disrepute of the employee.
(6) Are they vulnerable?	Potentially, as they may be fearful of losing their job if they have no license or too many points. Potentially in relation to possible mental health issues including stress or undiagnosed mental health / behavioural issues. This should be identified as a potential contributing factor and be picked up through Capability Review, rather than reactively through Disciplinary Review.
(7) Are some of the individuals concerned likely to object?	Vast majority no, but possibly yes if (1) if fraudulent claim of holding a license, (2) if fraudulent claim of no penalty points, (3) fearful of losing job / reputation due to high penalty points, (4) fearful of driver re-training, evaluation, performance monitoring.
(8) Are you able to stop the processing at any time on request?	Yes, but refusal to consent to driving license checks means that compliance cannot be assured and thus the driver not permitted to drive.
(9) Conclusion	Processing of employees driving license is a legitimate interest to protect both Employer and Employee.

Data Protection by Design and Data Protection Impact Assessments

The company is exempt from Data Protection by Design and Data Protection Impact Assessments (DPIA) for the following reasons:

High Risk Situation	**Description of Claimed Exclusion**
Deployment of New Technology	All technology is off-the shelf and subject to software developers security protocols;
Profiling Operation likely to significantly affect individuals	The company does not undertake profiling operations.
Large scale processing of the special categories of data	The company does not undertake large scale processing of data.

THE DATA PROTECTION PRINCIPALS AND HOW THEY ARE IMPLEMENTED IN THE COMPANY

Principle	Method of Implementation
Lawfulness, fairness and transparency (including consent)	All employees informed of the reasons that data is held through induction. All employees and self-employed workers sign a Privacy Notice. For marketing – the Consent Conditions are followed as per below.
Purpose Limitation	The organisation does not hold any data which is not explicitly required for contractual, employment purposes or marketing purposes. This data is not used for any additional purposes outside this purpose. Criminal offence data, ie data regards criminal convictions, criminal offences or related security measures will only be processed to achieve the contractual conditions and legitimate interests of customers operating on high security sites, eg military bases, prisons, central government, finance sector, requiring security clearance; or working with vulnerable people, eg schools, care facilities (Disclosure & Barring Service). Criminal offence data shall not be processed as part of employee recruitment processes as it is not a legitimate use.
Data Minimisation	No additional data is held or requested beyond what is required for the fulfilment of sales contracts or the purpose of employment or worker health protection and safety.
Accuracy	Employment data is the responsibility of the employee / worker to ensure its accuracy. There are clear lines of communication to facilitate this. See The Right to Rectification below.
Storage Limitation	Where an employee leaves employment data such as home addresses, next of kin, contact information etc is destroyed. For other personal data see above Table Of Personal Data Held And Lawful Basis for its Retention

Principle	Method of Implementation
Integrity and Confidentiality	Data is only available to the relevant people within the organisation. Personal data shall only be shared by the Data Protection Officer: ▪ To the Information Commissioners Office (ICO) on request of the ICO; ▪ To regulators, insurance providers, appointed legal advisors as part of their incident investigations; ▪ To other parties on the receipt of a specific request of the individual (Right of Portability) The data shall not be exported out of the EU, and is highly unlikely to be exported out of the UK. All Cloud Servers have been verified to be in the UK. The company has documented business continuity and disaster recovery plans which further defines information security protocols. The company doesn't process special category data or criminal conviction and offence data though as part of site activities it may need to apply for special permissions eg Disclosure & Barring Scheme (DBS), or security clearance, but the data processing is conducted by the organisation making the approval. The company confirms it is a small and medium enterprise and that data processing is incidental to the main purpose of the business and is thus exempt from the requirement to further document processing arrangements. Paper information is stored in secured filing cabinets. Personal data is locked and only available to the Administration & Accounts Manager and their deputy. Electronic data is held within secure IT systems. Computer systems are secured using industry level cyber security systems and access protection. See the company IT Security Policy for specific details.
Accountability[1]	The person ultimately responsibility for data protection is XXX, Managing Director. They are accountable for ensuring data privacy throughout the organisation. The Appointed Data Controller is Diana Albon, Administration & Accounts Manager. They will ensure compliance on a day-to-day basis and deal with Subject Access Requests from individuals and any interaction with the Information Commissioners Office. Employment contracts and Sub-Contractor contracts make individuals accountable for managing data under their control, and include a confidentiality statement.

Note 1: Whilst not obliged to formally a Data Protection Officer (DPO) as the organisation is not a high risk organisation, the Data Controller (DC) is appointed to coordinate data protection within the organisation.

INDIVIDUAL RIGHTS AND HOW THEY ARE IMPLEMENTED IN THE ORGANISATION

Right	What this Means	How this is Implemented
The Right to be Informed	Individuals must know why their information is to be provided, how it will be used.	When personal data is collected from individuals the company must inform them why this data is being collected. There are some types of information that must always be provided, while the provision of other types of information depends on the particular circumstances of your organisation, and how and why you use people's personal data. The full list of requirements is provided here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-privacy-information-should-we-provide-to-individuals/

Right	What this Means	How this is Implemented
The Right of Access	Individuals have the right to obtain a copy of all information held on them by an organisation.	Individuals make information access requests to the Data Controller who will respond within one month of receipt of the request. The company can extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, the Data Controller must inform the individual within one month of the receipt of the request and explain why the extension is necessary. A copy of the information must be provided free of charge, however, the company can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. The company may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that the company can charge for all subsequent access requests. The fee must be based on the administrative cost of providing the information. Where requests are manifestly unfounded or excessive, in particular because they are repetitive the company can charge a reasonable fee taking into account the administrative costs of providing the information; or refuse to respond. Where the company refuse to respond to a request, the Data Controller must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month. Before the information is provided, the company must verify the identity of the person making the request, using 'reasonable means'. If the request is made electronically, the company should provide the information in a commonly used electronic format.

Right	What this Means	How this is Implemented
The Right of Rectification	If an individual believes their information is wrong the organisation must allow the individual to be able to correct it.	Upon request from the individual the Data Controller will correct the information and evidence this to the individual. On receipt of request for rectification the data controller must respond within one month. This can be extended by two months where the request for rectification is complex. Where the company is not taking action in response to a request for rectification, the company must explain why to the individual, informing them of their right to complain to the Information Commissioners Office and to a judicial remedy. This rejection must be done without undue delay and at the latest, within one month. If the company has disclosed the personal data in question to others, the company must contact each recipient and inform them of the rectification - unless this proves impossible or involves disproportionate effort. If asked to, the company must also inform the individuals about these recipients. All customer orders are considered to be correct at the point of ordering and do not rely on previous information.

Right	What this Means	How this is Implemented
The Right to Erasure	If an individual wants their information be removed from the organisations systems, they have a right to request removal of the information providing there is no legal requirement for the organisation to retain it. Note: This primarily relates to social media companies, but may be extended to customer and employee data held by the company.	The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances: • Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed. • When the individual withdraws consent. • When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing. • The personal data was unlawfully processed (ie otherwise in breach of the GDPR). • The personal data has to be erased in order to comply with a legal obligation. Under the GDPR, this right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger. The company can refuse to comply with a request for erasure where the personal data is processed for the following reasons (note: the below list is truncated from the full list and only the relevant reasons is shown). • to comply with a legal obligation for the performance of a public interest task. • the exercise or defence of legal claims. H&S information has to be retained for legally defined periods eg task related safety documentation upto 7.5 years, drugs and alcohol test results upto 10 years, occupational health records eg PPE issue records, health surveillance results 40 years. As these are required under law the right of erasure does not apply. For non H&S data held on ex-employees the Data Controller will erase the information either by deletion from the server and any backups, or secure destruction of paper documents via shredding. For existing employees erasure of employee data will be undertaken on a case by case basis. If the company has disclosed the personal data in question to others, the Data Controller must contact each recipient and inform them of the erasure of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, the Data Controller must also inform the individuals about these recipients.

Right	What this Means	How this is Implemented
The Right to Restrict Processing	If an individual believes their data may be inaccurate, they can stop an organisation from using it until it has been corrected.	Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, the company is permitted to store the personal data, but not further process it. The company can retain just enough information about the individual to ensure that the restriction is respected in future. Employees and Sub-Contractors can check their information before processing. Customers have the ability to check and amend their information prior to placing the order.
The Right to Data Portability	If an individual wants to move their information to another organisation, they can request a copy of it in a common portable format which the organisation must provide free of charge.	*Note: The Right of Portability only applies where data is processed by automated means. It is more typically applicable to organisations like banks and insurance companies where an individual may wish to use their personal data in price comparison websites.* Individuals can make requests to the Data Controller to provide their personal data in a portable form that can be transferred from one IT environment to another in a safe and secure way, without hindrance to usability. The company must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. The information must be provided free of charge. If the individual requests it, the Data Controller may be required to transmit the data directly to another organisation if this is technically feasible. However, the company is not required to adopt or maintain processing systems that are technically compatible with other organisations. The company must respond without undue delay, and within one month. This can be extended by two months where the request is complex or the company receive a number of requests. The Data Controller must inform the individual within one month of the receipt of the request and explain why the extension is necessary. Where the company is not taking action in response to a request, the Data Controller must explain why to the individual, informing them of their right to complain to the Information Commissioners Office and to a judicial remedy without undue delay and at the latest within one month.

Right	What this Means	How this is Implemented
The Right to Object	If an individual believes an organisation is using their data inappropriately, for purposes beyond what was originally stated or without their explicit consent, they can demand the organisation stops using their data immediately.	Individuals have the right to object to direct marketing (including profiling). The organisation does not provide any form of direct marketing so the Right to Object does not apply. *Note: Individuals also have a right to object to data processed in the public interest and processing for purposes of scientific / historical research and the production of statistics but this isn't relevant to the company's activities.* In making an objection, the Individuals must do this on grounds relating to his or her particular situation. The company must stop processing the personal data unless: • the company can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or • the processing is for the establishment, exercise or defence of legal claims. The company must inform individuals of their right to object "at the point of first communication" and in the company's privacy notice. This must be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information. See Appendix A further guidance and the contents of Privacy Notices. The company must stop processing personal data for direct marketing purposes as soon as the company receives an objection. There are no exemptions or grounds to refuse. The Data Controller must deal with an objection to processing for direct marketing at any time and free of charge. For employees the organisation only uses data for the purposes of H&S, HR & Payroll. Data is only shared with regulators and on request insurance provider as part of investigation or due to a high risk driver (6 or more points on license).

Right	What this Means	How this is Implemented
Rights in Relation to Automated Decision Making	If a credit decision, or some form of computer-originated decision is made which can adversely affect an individual, they can demand that the organisation reappraises its decision using people rather than computers	This does not apply under the processing carried out by this organisation.

INFORMATION SECURITY

Data must be kept secure and the company maintains a separate Information and Cyber Security Policy.

Note: The government Cyber Essentials scheme is a Cyber Security Assurance Scheme which is becoming a mandatory requirement for many Buyers who have ISO27001 Information Security certification and for public sector contracts. https://www.cyberessentials.ncsc.gov.uk/

TRANSFER OF DATA OUTSIDE THE EU

The GDPR imposes restrictions on the transfer of personal data outside the European Union.

It is confirmed that the organisation only operates in the UK, and has no parent company.

It is confirmed that all data is held in the UK and that all cloud servers are based in the UK / EU.

REGISTRATION WITH THE INFORMATION COMMISSIONERS OFFICE

The organisation uses CCTV for the purposes of crime surveillance so is required to maintain annual registration with the Information Commissioners Office. Chiel Construction Limited ICO Registration Number is ZA250243. The Administration & Accounts Manager is responsible for maintaining registraition.

To justify the use of CCTV Cameras for Crime Surveillance an Annual Assessment of CCTV Camera Use will be produced and kept under review.

The organisation is not required to register for the purposes of holding the personal data of their employees and customers.

PROCEDURES FOR PERSONAL DATA BREACH DETECTION, REPORTING AND INVESTIGATION

Definition of Personal Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Initial Investigation

When a security incident takes place, the Data Controller must quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

Determination whether to Report Breach to the ICO

When a personal data breach has occurred, the company need to establish the likelihood and severity of the resulting risk to people's rights and freedoms[2], and it is the likelihood that determines if the ICO is informed:

- If it's likely that there will be a risk then the Data Controller must notify the ICO;
- If it's unlikely then the company doesn't have to report it. If the company decides it doesn't need to report the breach the Data Controller will need to be able to justify this decision so the decision must be documented and approved by the Managing Director.

[Note 2: In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

"*A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.*"]

Reporting a Breach to the ICO

The Data Controller must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it[3]. If the company takes longer than this, the Data Controller must give reasons for the delay.

To report the breach to the ICO:

1. Telephone 0303 123 1113. ICO offices are open Monday to Friday between 9am and 5pm, however, are closed after 1pm on Wednesdays for staff training.

2. Report it online but only if the Data Controller is confident that they have dealt with the breach it appropriately or if they are still investigating and will be able to provide more information at a later date. https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

[Note 3: Section II of the Article 29 Working Party Guidelines on personal data breach notification gives more details of when a controller can be considered to have "become aware" of a breach.]

When reporting a breach, the Data Controller must provide:

- a description of the nature of the personal data breach including, where possible the categories and approximate number of individuals concerned; and the categories and approximate number of personal data records concerned;
- the name and contact details of the Data Controller where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- 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.

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So Article 34(4) allows the company to follow up the initial breach report with further information, as long as this is done without undue further delay. The ICO expects Data Controllers to prioritise the investigation, give it adequate resources, and expedite it urgently.

Informing Individuals about a Breach

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says the Data Controller must inform those concerned directly and without undue delay.

A 'high risk' means that the individual may need to mitigate an immediate risk of damage to them so they can take steps to protect themselves from the effects of a breach.

Examples of breach which:

- should be reported is theft (or potential theft) of bank details, security passwords or medical records.
- doesn't need reporting is the accidental deletion of personal data which is then successfully recovered from a back-up.

The breach must still be reported to the ICO regardless of if the company informs the individual.

Information to provide to individuals when telling them about a breach:

The Data Controller shall describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of the Data Controller where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- 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.
-

Final Investigation

Regardless of if the breach was reported to the ICO or the individual as with any incident, the company shall document the facts relating to the breach, its effects and the remedial action taken. This is part of the company's overall obligation to comply with the accountability principle, and verification of the adequacy of the organisation's data protection arrangements.

As with any security incident, the company shall investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented –eg whether through better processes, information security, further training or other corrective action.

Penalties for failure to notify of a data breach to the ICO

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of the company's global turnover.