Data Protection policy

1. Introduction

Everyone who is employed by ISG Limited and/or its subsidiary companies ("**ISG**") in any capacity is bound by this policy, including all directors, officers, employees, agency workers, contractors and freelancers (together referred to as the "**ISG Employees**"). For the avoidance of doubt, this includes **ALL** ISG Employees working in the UK, Europe, Asia and the Middle East.

ISG needs to gather and use certain personal data about individuals, to include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how personal data must be collected, handled and stored to meet ISG's data protection standards and to comply with the law.

The definition of personal data under privacy laws (such as the GDPR, Data Protection Act 2018 and the CCPA) is any information relating to a living person that is already identified or can be identified.

There are some pieces of information that can identify a person on their own (for example, a phone number, facial image, IP address, passport number, national insurance number or CCTV image).

Some pieces of information cannot identify a person on their own but when you put them together with other pieces of information you can then identify a person (for example, information regarding someone's age or home address).

2. Contents of policy

This policy includes various appendices as follows:

2.1 Data retention policy (Appendix 1)

2.2 Data retention schedule (Appendix 2)

2.3 Data protection – on-site instructions (Appendix 3)

2.4 Data protection – frequently asked questions (FAQ) (Appendix 4)

A dedicated data protection section has also been established on Workspace, which includes a copy of this policy and other associated policies and procedures, It also has additional material, such as data checklists, bite-sized data protection training courses, template privacy notices and ISG's project site surveillance policy.

3. Important contact details

Further information regarding this policy and/or ISG's commitment to compliance with data protection can be found via various sources as follows:

Data Protection Officer:

Data Protection Officer
ISG Limited
86 Sandy Hill Lane
Ipswich
Suffolk
IP3 0NA
data.protection@isgltd.com

UK IT Service Desk

From time to time there may be a requirement for ISG Employees to report specific data protection related queries or concerns – and in some instances time may be of the essence. If in doubt, or where specifically required by this policy, contact the UK IT Service Desk:

Telephone: +44 (0) 3333 211901

Via Workspace: https://isgplc.sharepoint.com/

Or directly: https://isgplc.sharepoint.com/Pages/isg-applications/it-service-desk.aspx

The UK IT Service Desk is open between the hours of:

Monday – Thursday: 07.00 – 18.00 UK time

Friday: 07.00 – 16.00 UK time

4. Why this policy exists

This data protection policy (together with its various Appendices) ensures that ISG:

- complies with data protection law and follows good practice;
- protects the rights of employees, customers, suppliers and other partners;
- is open about how it stores and processes individuals' data; and
- protects itself from the risks of a data breach

5. Data protection law

In 2018 The European Union's General Data Protection Regulation ("**GDPR**") and the UK's Data Protection Act 2018 came into force. These new regulations describe how organisations (including ISG) must collect, handle and store personal information to ensure compliance, within the UK and EU.

This policy has been written to ensure that ISG is able to comply with its specific GDPR compliance obligations. However, it is acknowledged that for other jurisdictions in which ISG carry on business, specific local data protection compliance obligations may also exist, on a country by country basis. In such instances, additional local policies and procedures may be required to supplement this over-arching group policy.

The Data Protection Officer (DPO) will monitor compliance against GDPR across all territories, but where local data protection legislation requires a higher or different standard than that provided by the GDPR, the relevant regional Managing Directors shall be responsible for all such audit and compliance activities.

The GDPR applies regardless of whether data is stored electronically, on paper, or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and cannot be disclosed unlawfully.

The GDPR is underpinned by the following important principles, whereby personal data must be:

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

ii) obtained only for specific, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

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

iv) accurate and kept up to date;

v) held for no longer than necessary; and

vi) processed in a manner that ensures appropriate security of the personal data;

ISG (as the Controller of all relevant personal data) shall be responsible for, and be able to demonstrate, compliance with the above principles.

6. Data breaches

All ISG Employees must report actual or potential data protection compliance failures to the Data Protection Officer and the UK IT Service Desk as soon as is practicable (contact details as shown in section 3 above). Examples of data breaches could include:

- Loss of IT equipment.
- Loss of physical documentation containing personal information.
- Emailing or sharing personal information with people who are not entitled to see it.
- Failing to secure data adequately in transit e.g. emailing unencrypted personal bank details.
- If you suspect your work account has been hacked.

Additional information regarding data breaches can be found in the data protection section of Workspace or by contacting the DPO.

7. Data Privacy Impact Assessments ("DPIA's")

A key component of ISG's data protection procedures is to ensure that '*Privacy by Design'* is at the heart of all its data collection, handling and storage processes. In simple terms, privacy needs to be considered throughout ISG. The design of all our processes, procedures and technologies should promote privacy and data protection compliance from start to finish, rather than just an 'add-on' or 'after-thought'.

Consequently, a DPIA must be considered for any business change activity and it is the responsibility of all Managing Directors/ Enabling Department Heads to ensure this (also see section 8.4 below).

For more information and advice please contact the Data Protection Team.

8. Responsibilities

All ISG Employees have some responsibility for ensuring that personal data is collected, stored and handled appropriately and that ISG complies with data protection legislation within their country of operation. Such responsibilities include:

- Ensuring that personal data is handled and processed in line with this policy and the data protection principles highlighted in section 5 above.
- Ensuring that all contracts are compliant with data protection legislation across the geographies ISG operates in.

- Ensuring that the transmission of personal data is appropriately secure.

- The completion of appropriate data protection training as may be requested by ISG from time to time.

- The immediate reporting of any suspected or actual data breaches (see section 5 above).

- The immediate reporting of any information security weaknesses or events.

If you receive a request regarding personal information (such as a Data Subject Access Request) from someone within ISG or a member of the public, you should advise the data subject to fill in a request via the web form held on the ISG website, as this is the most efficient way to log their request. If the data subject refuses, or is unable to fill in the form, please refer to Workspace where you can find the 'data subject request form' in the Data Protection section. Complete this on behalf of the data subject and submit the details. If you are unable to access the form on Workspace, record the data subjects name and contact details and log the information and description of request with the UK IT Service Desk. Failure to adhere to this policy will be dealt with under ISG's disciplinary procedures and may result in summary dismissal.

Further details can be found in the FAQ (Appendix 4) to this policy or on Workspace in relation to specific responsibilities.

The following positions of authority within ISG have key areas of responsibility for implementing this policy:

8.1 The Board of directors

The board of directors is ultimately responsible for ensuring that ISG meets its legal obligations, to include the provision of relevant training and adherence to the principles stated in section 5 above. The Chief Financial Officer will represent the DPO in making material business decisions relating to data protection and compliance with relevant data protection laws, in all territories in which ISG operates.

8.2 Data Protection Officer

The data protection officer, is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.

- Managing the assignment of responsibilities to deliver compliance with data protection laws and policies of ISG, including through managers, teams and champions from within each business.

- Informing and advising on data protection laws and ISG policies

- Maintaining data protection policies and procedures.

- Monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities.

- Ensuring that major legislative changes that affect countries that ISG operate in are communicated to the relevant business units and entities.

- Being the first point of contact for communications with supervisory authorities, in accordance with the timelines dictated by the data protection laws.

- Supervising and advising on data protection impact assessments (DPIAs).

- Managing an ongoing programme of awareness-raising and training to deliver compliance and to foster a data privacy culture.

- Provide advice to the Business Assurance/Business Unit Compliance teams conducting both site audits and Right to Work checks.

- Handling data protection questions from ISG Employees and anyone else covered by this policy.

- Dealing with requests from individuals to see the data that ISG holds about them (also called 'subject access requests').

- Working with ISG's legal and commercial departments in checking and approving any contracts or agreements with third parties that may handle personal data on behalf of ISG

8.3 Group IT Director

The Group IT Director is responsible for:

- Ensuring that resources are available to implement the necessary technical security controls required by the GDPR.

- Ensuring policies and security controls are in place to protect ISG's IT systems confidentiality, integrity and availability in accordance with the Information Security Policy.

- Evaluating the security of any third-party services that ISG is considering using to store or process data, for example, cloud computing services.

8.4 Managing Directors / Project Directors / Project Managers

ISG collects large quantities of personal data at our Project Sites, such as identity and qualifications evidence, Health and Safety information and contact details for people entering the site. To ensure we are gathering this information in a secure way, collecting only the information we need, and deleting it when it serves no further purpose, the Project Site Instructions at Appendix 3 to this policy provide instruction and support for the Project Leadership team. For the avoidance of doubt, failure to follow the guidance in the Project Site Instructions may lead to projects incurring additional costs if they have to mitigate data protection risks mid project. In the worst-case UK and European Data protection legislation allows ISG to be fined up to 4% of its global turnover.

8.5 Managing Directors / Enabling Department Heads

Managing Directors and the Heads of each Enabling Department are responsible for ensuring the day-to-day Data Protection principles (as listed in within section 4) are adhered to, including:

- Supporting the board of directors and the Data Protection Officer in the implementation of this policy.

- Providing resources to assist the Data Protection Officer with Subject Access Requests, Breach Notifications, DPIA's and any other relevant activities required to maintain ISG's compliance with data protection legislation.

- Ensuring that ISG Employees have the resources to complete any individual training that has been identified.

- Ensuring that '*Privacy by Design*' is built into any business change activity (see section 6 above).

- Ensuring that any data breaches are reported in a timely manner.

- Ensuring that all contracts are compliant with data protection legislation across the geographies ISG operates in.

9. ISG's commitment

ISG is committed to complying with data protection legislation and good practice. Sections 9.1 to 9.7 confirm each of these specific commitments:

9.1 Lawfulness, fairness and transparency

ISG will implement technical and organisational measures to ensure that it is processing personal information fairly and lawfully. These measures are meant to ensure that ISG:

- has lawful grounds for collecting and using the personal data it holds;
- will not use the data in ways that have unjustified adverse effects on the individuals concerned;
- will be transparent about how it intends to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- will handle people's personal data only in ways they would reasonably expect; and make sure it does not do anything unlawful with the data; and
- has specific procedures in place that apply when processing sensitive personal data/ special category information

9.2 Purpose limitation

ISG will implement technical and organisational measures to ensure that it is processing personal information for specified and lawful purposes and will not be further processed in any manner incompatible with that purpose or those purposes.

These measures are meant to ensure that ISG:

- is clear from the outset about why it is collecting personal data and what it intends to do with it;
- complies with what the local laws say about notifying and registering with the supervisory authority; and
- confirms if it wishes to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or that the disclosure is fair and lawful and that the data subject is informed.

9.3 Data Minimisation

ISG will implement technical and organisational measures to ensure that the personal data it collects, and processes is adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

These measures are meant to ensure that ISG:

- holds personal data about an individual that is sufficient for the purposes it is using the data for; and
- does not hold more information than it needs for that purpose.

9.4 Accuracy

ISG will implement technical and organisational measures to ensure that the personal data it collects, and processes is accurate and, where necessary, kept up to date.

These measures are meant to ensure that ISG:

- takes reasonable steps to ensure the accuracy of any personal data it obtains;
- ensures that the source of any personal data is clear; and
- carefully considers any challenges to the accuracy of information; and considers whether it is necessary to update the information.

9.5 Storage Limitation

ISG will implement technical and organisational measures to ensure that the personal data it collects and processes for any purpose shall not be kept for longer than is necessary for that purpose. ISG's Data Retention Schedule (Appendix 2) gives detailed guidance on the length of time we should retain personal information for. If you believe that you cannot comply with the schedule, contact the DPO for advice.

These measures are meant to ensure that ISG:

- reviews the length of time it keeps personal data;
- considers the purpose or purposes it holds the information for, and the lawful basis for processing, in deciding whether (and for how long) to retain it;
- securely deletes information that is no longer needed for this purpose or these purposes;
- updates, archives or securely deletes information if it goes out of date; and
- advises data subjects as to how long their personal data is retained for.

9.6 Data subjects' rights

ISG will implement technical and organisational measures to ensure that it will process personal data in accordance with the rights of data subjects under the GDPR.

These measures are meant to ensure that ISG can adequately respond to a data subject exercising the following rights:

- Right of access to a copy of the information comprised in their personal data.
- Right to object to processing that is likely to cause or is causing damage or distress.
- Right to prevent processing for direct marketing.
- Right to object to decisions being taken by automated means.
- Right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed.
- Right to claim compensation for damages caused by a breach of the GDPR.

Any ISG Employee or member of the public may choose to exercise the rights listed above by sending a request to ISG in a number of ways, which could include emails, telephone calls, written letter, verbally, text.

This information must be provided without delay and at the latest within one month of receipt. ISG will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, ISG must inform the individual within one month of the receipt of the request and explain why the extension is necessary

9.7 Managing compliance and record keeping

The DPO will maintain records of non-compliances, requests to exercise data subject rights, Data Protection Impact Assessments, privacy statements, along with other records required by the data protection legislation in the countries that we operate in.

10. Approval

The content of this policy has been approved by the Statutory Board.

For and on behalf of ISG
Signed:

Paul Cossell
Chief Executive ISG

Date: 12 November 2020

Data Retention

Appendix 1 to ISG's Data Protection policy

1. Introduction

One of ISG's key obligations under the various privacy acts that we are required to comply with is to ensure that we only keep personal data for the minimum period necessary. This policy sets out maximum retention periods for different categories of information and is guided by national laws and industry best practice. The definition of personal data under privacy laws (such as the GDPR and the UK's Data Protection Act 2018) is any information relating to a living person that is already identified or can be identified.

2. Important contact details

Further information regarding this policy and ISG's commitment to compliance with data protection is available from the:

Data Protection Team
ISG Limited
86 Sandy Hill Lane
Ipswich
Suffolk
IP3 0NA
data.protection@isgltd.com

3. Why this policy exists

This Data Retention Policy ensures that ISG:

- Complies with data protection law and follows good practice about how we retain personal data;
- Protects the rights of employees, customers, suppliers and other partners;
- Is open about how it processes and retains individuals' data; and
- Protects itself from the risks of a data breach by only storing personal data for the minimum period necessary.

4. Scope

Everyone who is employed by ISG Limited and/or its subsidiary companies ("**ISG**") in any capacity is bound by this policy, including all directors, officers, employees, agency workers, contractors and freelancers (together referred to as the "**ISG Employees**"). This includes **ALL** ISG Employees working in the UK and the European Economic Area. Data retention schedules for ISG Middle East and ISG Asia will be released at a future date.

This also includes personal data processed for the performance of services to clients, collected from workers on construction sites, processed for marketing and business purposes, and personal data processed for recruitment and employment purposes.

All records, whether analogue or digital, are subject to the requirements of this Policy.

Records can take many forms including, but not limited to, the following:

- Hard copy data held on paper, where such data is kept in organised systems;
- Data stored, sent or received electronically on computer systems and mobile devices.

5. Responsibility for Implementation of and Compliance with The Policy

Data Owners are responsible for business processes that involve personal information; they are also accountable for the collection and use of that data and related assets and are required to ensure that all policies and best practices about retaining personal information are followed. The following roles have responsibility for the retention of records under this Policy because they are Data Owners.

Data Owners include:

- Project Directors, Project Managers, Site Managers will be responsible for the collection and retention of personal information on project sites;
- Enabling Departments are responsible for all personal information stored and/or processed within their respective areas of responsibility or on technology platforms that they manager, such as websites, CRM and mass emailing systems;
- Managers who store and/or process personal information within Business Units, e.g. line managers who conduct annual employee reviews and process payroll/expenses information.
- Office and Facility Managers with responsibility for access control, induction and security systems.

Other responsibilities within the organisation are defined below:

- The DPO be responsible for ensuring data is deleted or amended by the relevant Data Owners following a Data Subject Rights request;
- As well as providing technical support to Data Owners, the IT Department will ensure that new technology platforms comply with this policy and where practicable, automate the deletion of personal information when it is no longer required;
- All employees who receive personal information in the normal course of business, (such as via email) are responsible for deleting data as soon as possible, when no longer required. Any queries in this regard must be referred in the first instance to the data owner.

6. Retention Periods

Data Owners will ensure that Personal Information is only retained for the relevant retention periods as specified in Appendix 2.

Unless specifically identified, the relevant retention periods specified in Appendix 2 will be considered maximum and minimum retention periods.

The Data Protection Officer must be notified of any records that have not been identified in the Data Retention Schedule in Appendix 2. A relevant retention period will be recommended and added to the Data Retention Schedule upon review.

7. Deletion of Information

Where the records are no longer required to be kept due to statutory requirements or administrative needs and no other legal basis applies for further retention, they must be deleted or physically destroyed. Please refer to the Destruction Guidance in Appendix 2.

For the disposal of hardware, such as disk drives, laptops and USB devices, contact the IT Service Desk for advice. Destruction should be completed within 30 days of the planned retention period, regardless of what the period is.

For the secure disposal of hard copies, such as paper, microfiche etc, please refer to the Destruction Guidance in the Retention Schedule (Appendix 2).

Guide:

Scope

The following countries are included in this retention policy: Austria (AU), Belgium (BE), Finland (FI), France (FR), Germany (DE), Ireland (IE), Netherlands (NL), Spain (ES), Sweden (SE), United Kingdom (UK). Retention schedules for ISG Asia and Middle East will be issued later.

About this Spreadsheet

This Data Retention Schedule should be read in conjunction with the Data Retention Policy . Within the spreadsheet information categories of personal data have been separated for ease of use, but you will need to check each of the categories as there will be overlaps. A good example is the CCTV tab, which affects both our Offices and our Project Sites.

Omissions and Corrections

Please report any omissions or suggested corrections to the Data Protection Officer (DPO) at data.protection@isgltd.com . Where you believe a retention period is incorrect please identify the relevant legislation or industry best practice guidelines to support the suggested changes. The schedule will be updated every 6 months and the policy reviewed annually. Interim exemptions to the policy that have been agreed with the DPO and the Risk Committee will be valid until the policy is formally amended; they then cease to be valid.

Implementation

The Retention Policy and this Schedule do not address how we will deliver compliance. Delivery of procedures, processes and technologies to address the non-compliances generated by the adoption of a Retention Policy will be addressed by BUs and the EDs, with support from the ISG Risk Committee and the Business Change Board.

Data Owners:

Project Directors, Project Managers, Site Managers will be the data owners for all information stored on their respective projects and sites and are responsible for the compliance with this schedule.

Enabling Departments are responsible for all personal information stored and/or processed within their departments;

Managers who store and/or process personal information within Business Units, e.g. line managers who conduct annual employee reviews and process payroll/expenses information.

Office and Facility Managers with responsibility for access control, induction, archive and security systems.

Destruction:

Data Destruction Guidance

REF	Problem	Solution
1	Addressing Hoarding	Delete your electronic files that are: expired, duplicated, or not of business value
2	Finding your data	Consider all the types and locations your data may be: Paper held in desks, cupbaords, shared office space, project sites, offsite archives Electronic data held in your local PC, external hard drives,Sharepoint, Databases, other servers, the cloud, and applications Electronic data held in your emails on your work computer and personal devices Electronic data held in mobile devices, cameras, rewritable disks (CD, DVD's) and USB Drives
3	Deciding what to remove	Use the retention policy guidance to know how long you can keep your data Look at records most likely to be out of date, for example staff who have left, suppliers who have completed their work, past team events, folders that are infrequently accessed
4	Deleting Electronic Data and Disposal of IT Equipment	Remove the file using the existing delete mechanism, including copies and back-ups of the same file Do not destroy or dispose of IT Equipment without seeking the guidance of the IT Service Desk. Turn-on the automatic deletion features available on some applications Anonymise data you cannot delete so it is no longer personally identifiable
5	Destroying Paper Data	Shred paper files with your office shredder Contact your office manager for help Use a commerical organisation to shred large volumes of paper records. Your existing archiving company is likely to offer this service.
6	Managing Archived Data	Check the access permissions are uptodate, remove anyone who should no longer have access Check physical security measures are still working eg locks, PIN codes, site access control For a third party check that ISG data is segregated from that of other companies Check the third party is compliant with GDPR principles Securely destroy any archived data that is outside the retention period specified for that type. If the third party does this for you, ask them for a certificate of proof Set-up a routine to go through batches of archived materials every 6-12 months Check the service agreements with third parties used for archiving on an annual basis

CCTV

Country collected	Legal basis	Justification	Retention Period
Austria	Legitimate interest	To safeguard the security of individuals, property and facilities	30 days, unless needed for longer pursuant to a security or criminal investigation/incident
Belgium	Legitimate interest	To safeguard the security of individuals, property and facilities	30 days, unless needed for longer pursuant to a security or criminal investigation
Denmark	Legitimate interest	To safeguard the security of individuals, property and facilities	30 days, unless needed for longer pursuant to a security or criminal investigation/incident
France	Legitimate interest	To safeguard the security of individuals, property and facilities	For 30 days, unless needed in relation to the active investigation of disciplinary or criminal proceedings
Finland	Legitimate interest	To safeguard the security of individuals, property and facilities	Suggested 60 days (no period specified), unless needed in relation to the active investigation of disciplinary or criminal proceedings
Germany	Legitimate interest	To safeguard the security of individuals, property and facilities	2 days, unless needed for evidence for criminal proceedings
Luxemburg	Legitimate interest	To safeguard the security of individuals, property and facilities	For 30 days, unless needed in relation to the active investigation of disciplinary or criminal proceedings
Netherlands	Legitimate interest	To safeguard the security of individuals, property and facilities	30 days, unless needed for longer pursuant to a security or criminal investigation/incident
Ireland	Legitimate interest	To safeguard the security of individuals, property and facilities	30 days, unless needed for longer pursuant to a security or criminal investigation
Poland	Legitimate interest	To safeguard the security of individuals, property and facilities	30 days, unless needed for longer pursuant to a security or criminal investigation/incident
Portugal	Legitimate interest	To safeguard the security of individuals, property and facilities	30 days, unless needed for longer pursuant to criminal investigations
Spain	Legitimate interest	To safeguard the security of individuals, property and facilities	30 days, unless needed for evidence criminal acts against people, goods or facilities
Sweden	Legitimate interest	To safeguard the security of individuals, property and facilities	60 days, unless needed for longer pursuant to a security or criminal investigation/incident
Switzerland	Legitimate interest	To safeguard the security of individuals, property and facilities	Up to 3 days, unless needed for longer pursuant to a security or criminal investigation/incident
UK	Legitimate interest	To safeguard the security of individuals, property and facilities	30 days, unless needed for longer pursuant to an investigation/ incident

Site Records (Also see 'Health and Safety' tab)

REF	RECORD TYPE	Retention Period	Start of Retention Period	JUSTIFICATION
1	Basic personal information (Name, Company name, address)	Employees – For the full duration of the project, and up to 3 years following the end of the project Contractors – For the full duration of the project, and up to 3 years following the end of the project Other visitors – for up to one year GBL Site: Due to complaince requirements at this specific site - within 1 year of the closure of ISG's GBL project(s) on site	From the beginning of the employment/service contract/site visit	Legitimate interest – Site Security
2	Other basic personal information (emergency contact number, miles travelled to work, method of transport)	General: Employees – for the duration of the employment Contractors – for the duration of the project (Data may be retained for longer in a statistical format)	From the beginning of the employment/service contract	Legitimate interest – Sustainability reporting
3	CCTV Recordings	See CCTV Section	See CCTV Section	Legitimate Interest – Site security
4	Biometric records	Employees – for the duration of the employment Contractors – for the duration of the service contract Other visitors – for up to one year	From the beginning of the employment/service contract/site visit	Employees – Employment obligations/ Local legal exceptions and legitimate interests Contractors – Employment obligations/ Local legal exceptions/ Legitimate Interest Visitors: Consent (for biometrics)
5	Photographs	**Employees** – for the duration of the project **Contractors** – for the duration of the project **Other visitors** – for up to one year	From the beginning of the employment/service contract/site visit	Legitimate Interest - Site security
6	Operative Identification Information (including identity cards, NRNs, etc, etc.)	Employees: See identification information above Contractors – for the duration of the project GBL - Due to complaince requirements at this specific site - within 1 year of the closure of ISG's GBL project(s) on site	From the beginning of the employment/service contract/site visit	Legal obligation – Duty of care (e.g. under HASAW Act 1974 in the UK) Legitimate interest – Defending against a legal claim
7	Induction information (including trade, operative type, induction data, induction course, date of birth, fit to work information etc.)	**Employees/Contractors** (Shorter retention period applies to data generally collected. Longer retention period applies in the case of an accident) AU: Austria: For the duration of project and in some cases to 3 years to defend a legal claim BE: For the duration of project and in some cases to 10 years to defend a legal claim FI: For the duration of project and in some cases to 3 years to defend a legal claim (period runs from when claimant ought to have learnt of the damage) FR: For the duration of project and in some cases to 10 years to defend a legal claim DE: For the duration of project and in some cases to 30 years to defend a legal claim IE: For the duration of project and in some cases to 2 years to defend a legal claim LU: For the duration of project and in some cases to 3 years to defend a legal claim Netherlands: For the duration of the project and in some cases up to 10 years to defend against a legal claim ES: For the duration of the project and in some cases up to 15 years to defend against a legal claim SE: For the duration of the project and in some cases up to 10 years to defend against a legal claim UK: For the duration of project and in some cases to 3 years to defend a legal claim	From the date of the injury (incl. possible injury)	Legal obligation – Duty of care Legitimate interest – Defending against a legal claim
8	Security Vetting: Process Security and Background Screening (Vetting) to meet requirements of contracts for specific UK Gov clients.	UK: SQ deleted once sent to government. BPSS held for audit purposes for duration of project or as prescribed in contract	From the individual's enrolment on the project.	Article 6:Performance of a contract, Legal obligation. Article 9: "For substantial public interest purposes (the safety and security of the parliamentary estate and all those using it) For employment, social security, and social protection purposes"

COVID

REF	RECORD TYPE	Retention Period	Start of Retention Period	JUSTIFICATION
1	Temperature	0 days	Day of test	Legitimate Interest as per ICO's instructions. Temperature is checked to see if it is below 37.8 Deg C, otherwise the data subject cannot enter the office or project site. Temperature is not recorded.
2	Operatives Name/company details.company contact	30 days	Date of a positive temperature check	Legitimate Interest as per ICO's instructions. Temperature is checked to see if it is below 37.8 Deg C, otherwise the data subject cannot enter the office or project site. Temperature is not recorded, but we will inform the operatives employer and keep a note of the date of positive test.

Health and Safety Records (also see 'Project Site' Tab)

REF	RECORD TYPE	Retention Period	Start of Retention Period	JUSTIFICATION
1	Employee medical (occupational health and safety company doctor) files	AU: Standard - 30 years BE: Standard – 15 years. Up to 40 years for specific exposure FR: Standard – 10 years. Up to 50 years for specific exposure FI: 12 years after death of patient (See specific health legislation) DE: Standard – 10 years. Up to 40 years for specific exposure IE: Duration of the contract plus 7 years. Up to 40 years for specific exposure LU: Standard 10 years NL: Up to 15 years (limited to data needed to calculate sick pay, insurance, other statutory responsibilities related to compensation, etc.) ES: 5 years post-employment, except in the below cases, applicable per 'comunidad autónoma': - Cantabria: 15 years - Galicia: data about surgical procedures, births, anaesthesia, medical reports, discharge reports: indefinite retention. - Canarias: 20 years. - País Vasco: 15 years. SE: Up to 10 years (Up to 40 years for specific exposure) UK: Duration of the employment and dependent on applicable health regulations (up to a minimum of 5 years and up to 40 years from the accident for exposure to hazardous materials)	Date of the last entry made in the record	Specific legislation in relation to medical and health and safety obligations
2	Data concerning emergency medical care, individual treatment agreements, degree of incapacity for work, required workplace adaptations (employees)	AU: Duration of the employment (suggested) BE: Duration of the employment (suggested) FR: Duration of the employment (suggested) DE: Duration of the employment (suggested) FI: Duration of the employment (suggested) IE: Duration of the employment plus 7 years LU: Duration of the employment (suggested) NL: Duration of the employment (2 years after rehabilitation for information related to rehabilitation, duration of absence, whether causes by accident at work or third party liability, as needed to calculate insurance and make adjustments for rehabilitation of the employee) ES: Duration of the employment plus 4 years SE: Duration of the employment. UK: Max 6 years post-employment	The date that the documents are created	**Specific local law requirements** with regard to occupational health (e.g. Working Conditions Act 1999 in Netherlands) Employment obligations, such as those related to ensuring support for disabilities (e.g. Equality Act 2010 and Health at Safety at Work Act 1974 in the UK) (e.g. Employment Equality Acts 1998-2015 in Ireland) (e.g. Working Conditions Act 2017 in Netherlands) Local guidance from data protection campaigns conducted by the national governance bodies

Health and Safety Records (also see 'Project Site' Tab)

REF	RECORD TYPE	Retention Period	Start of Retention Period	JUSTIFICATION
3	Accident records and medical history (on-site operatives/contractors)	General: (Shorter retention period applies to medical history. Longer retention period applies to accident records) AU: For the duration of project and in some cases to 3 years to defend a legal claim Be: For the duration of project and in some cases to 10 years to defend a legal claim FI: For the duration of project and in some cases up to 3 years to defend a legal claim (period runs from when claimant ought to have learnt FR: For the duration of project and in some cases to 10 years to defend a legal claim DE: For the duration of project and in some cases to 30 years to defend a legal claim IE: For the duration of project and in some cases to 2 years to defend a legal claim LU: For the duration of project and in some cases to 3 years to defend against a legal claim NL: For the duration of project and in some cases to 10 years to defend a legal claim ES: : For the duration of the project and in some cases up to 15 years to defend against a legal claim SE: For the duration of project and in some cases to 10 years to defend a legal claim UK: For the duration of project and in some cases to 3 years to defend against a legal claim	From the date of the injury (incl. possible injury)	Legal obligation – Health and Safety obligations/ Duty of care (e.g. Health and Safety Act 1974 in the UK)

Company Records

REF	RECORD TYPE	Retention Period	Start of Retention Period	JUSTIFICATION
1	Certificate of incorporation Articles of association Register of Members and Directors Written Resolutions at general meetings Company Minute Books	AU: Permanently BE: Permanently FI: Permanently FR: Permanently DE: Permanently IE: Permanently LU: Permanently NL: Permanently ES: Permanently SE: Permanently UK: Permanently	The date on which the record was made	Legal requirement
2	Company accounts (for example, profit & loss accounts) Company books Company reports (for example, audit reports)	AU: 7 years BE: 10 years (Originals) BE: 5 years (Documents that do not constitute evidence against 3rd parties) FI: 6 years FR: 10 years DE: 10 years IE: 7 years LU: 10 years NL: 7 years ES: 6 years SE: 7 years UK: 3 years	The date on which the record was made	Legal requirement
3	Records of dissolved entity	AU: 7 years BE: 5 years FI: 10 years FR: 5 years DE: 10 years IE: 7 years LU: 10 years NL: 7 years ES: 6 years SE: 10 years (best practice) UK: 10 years (best practice)	The date on which the record was made following dissolution	Legal requirement Best practice

Accounting and Tax

REF	RECORD TYPE	Retention Period	Start of Retention Period	JUSTIFICATION
1	Budgets and periodic financial reports	AU: 7 years post financial year BE: 7 years post financial year FI: 10 years FR: 10 years DE: 10 years IE: 6 years post financial year LU: 10 years post financial year NL: 7 years ES: 6 years post financial year SE: 7 years UK: 6 years post financial year	End of the financial year to which the record relates	Legal requirement
2	Taxation returns and records	Au: 7 years BE: 7 years FR: 6 years post-transaction FI: 10 years FR: 6 years DE: 6 years IE: 6 years LU: 10 years NL: 7 years ES: 6 years post financial year SE: 7 years UK: 6 years post-transaction	End of the financial year to which the record relates	Legal requirement
3	VAT records	AU: 7 years BE: 7 years FI: 6 years FR: 6 years DE: 10 years IE: 6 years LU: 10 years NL: 7 years SE: 7 years ES: 6 years UK: 6 years	End of the financial year to which the record relates	Legal requirement
4	Customer invoices and receipts	AU: 7 years BE: 7 years FR: 10 years FI: 6 years DE: 10 years IE: 6 years LU:10 years NL: 7 years ES: 6 years post financial year SE: 7 years UK: 6 years	End of the financial year to which the record relates	Legal requirement
5	Contracts and rental agreements (including leases)	AU: 7 years BE: Duration of the contract plus 7 years FR: 30 years FI: Duration of the contract plus 10 years DE: 10 years IE: 13 years LU: 10 years NL: 7 years SE: Duration of the agreement plus 7 years ES: Duration of the contract plus 15 years UK: Duration of the contract plus 6 years	End of the agreement/service	Legal Requirement Best practice to defend against potential claims

Employee Records and Job Applicants' Records

REF	RECORD TYPE	Retention Period	Start of Retention Period	JUSTIFICATION
1	All Employee onboarding information (name, address, date of birth, contact details, NI number, Passport No. and copy, Driving License, CSCS card number (or EU equivalent),Bank Details, Salary details, Payroll ID, Photo, Next of Kin details, employment and education history etc.)	6 years post employment	The date that the documents are created	Performance of the employment contract
2	Employment contract terms and conditions and any changes thereof, working pattern.	AU: Duration of the contract plus 7 years BE: Duration of the contract FI: Duration of the contract plus 10 years FR: Duration of the contract plus 5 years DE: Indefinitely IE: Duration of the contract plus 7 years LU:Duration of the contract plus 3 years NL: Duration of the contract plus 7 years ES: Duration of the contract plus 4 years SE: Duration of the contract plus 7 years UK: Duration of the contract plus 6years	The date that the documents are created	Legal requirement with due consideration to the GDPR Best practice
3	Training records/Performance Reviews/Sick Leave Records	AU: Duration of the contract plus 7 years BE: Duration of the contract plus 1 year FR: Duration of the contract plus 2 years (recommended) FI: Duration of the contract plus 2 years (recommended) DE: Duration of the contract plus 2 years (recommended) IE: Duration of the contract plus 7 years LU:Duration of the contract plus 10 years NL: 2 years post-employment ES: Duration of the contract plus 4 years SE: Duration of the contract plus 2 years (recommended) UK: 6 years post-employment	The date of creation	Legal requirement with due consideration to the GDPR
4	Information evedencing the right to work in a country Identification documents of foreign nationals (specific to immigration check purposes) Visa Sponsorhip documents	AU: Duration of the contract plus 3 years BE: Duration of the employment plus one year FR: 5 years FI: 4 years DE: 1 year IE: Duration of the contract plus 7 years LU: 10 years NL: 5 years ES: Duration of the contract plus 4 years SE: Unknown (Suggested duration of the contract plus 2 years) UK: 2 years post-employment (recommended)	The date of onboarding	Legal requirement with due consideration to GDPR

Employee Records and Job Applicants' Records

REF	RECORD TYPE	Retention Period	Start of Retention Period	JUSTIFICATION
5	Identity proofs for banks/treasury purposes	AU: Duration they are a signatory/director plus 1 year (recommended) BE: Duration they are a signatory/director plus 1 year (recommended) FR: Duration they are a signatory/director plus 1 year (recommended) FI: Duration they are a signatory/director plus 1 year (recommended) DE: Duration they are a signatory/director plus 1 year (recommended) IE: Duration they are a signatory/director plus 1 year (recommended) LU: Duration they are a signatory/director plus 1 year (recommended) NL: Duration they are a signatory/director plus 1 year (recommended) ES: Duration they are a signatory/director plus 1 year (recommended) SE: Duration they are a signatory/director plus 1 year (recommended) UK: Duration they are a signatory/director plus 1 year (recommended)	Date of receipt	legitimate interest (Preventing the occurrence of fraud)
6	Pension schemes, career and talent development programmes, social plans	AU: 7 years post employment BE: 5 years FI: 10 years (for pension plans), otherwise permanently FR: 5 years DE: 6 years IE: Permanently LU: 6 years NL: 7 years ES: 4 years post-employment SE: 7 years UK:6 years	The end of the relevant financial year	Legal requirement
7	Data of rejected job applicants	AU: None BE: None (suggested 2 years) FR: 2 years FI: 2 years DE: None (suggested 2 years) IE: Duration of campaign + 18 months LU: 2 years NL: 4 weeks (or 1 year with consent) ES: 3 years SE: None (suggested 2 years) UK: 6 months post-campaign	The date that the documents are created or received	For the defense of legal claims (e.g. discrimination), talent pooling and with due consideration to the GDPR. Also consent.
8	Data collected on criminal convictions in the course of the recruitment process (Not actual criminal convictions)	**Employees (General and for Sustainability purposes):** AU: Duration of contract **BE: Not to be collected** FR: Duration of the contract FI: Duration of the contract **DE: Not to be collected** **IE: Not to be collected** LU: Duration of the contract NL: Duration of the contract **ES: Not to be collected** **SE: Not to be collected** UK: Duration of the contract **Rejected Applicants:** AU: None (suggested 2 years) BE: None (suggested 2 years) FR: 2 years **FI: Not to be collected** **DE: Not to be collected** IE:12 months post campaign LU: 2 years NL: 4 weeks (or 1 year with consent) **ES: Not to be collected** **SE: Not to be collected** UK: 6 months post-campaign	The date that the documents are created or received	Best practice based on Data Protection Legislation and legal obligation in relation to risk-assessing employees

Employee Records and Job Applicants' Records

REF	RECORD TYPE	Retention Period	Start of Retention Period	JUSTIFICATION
9	Data concerning temporary workers	AU: Duration of contract plus 7 years BE: Duration of contract plus 5 years FR: Duration of the contract FI: Duration of the contract (recommended) DE: Duration of the contract or 2 years (whichever is the longer) IRL: Duration of the contract plus 18 months LU: Duration of contract plus 10 years NL: Duration of contract plus 2 years ES: Duration of the contract plus 4 years (recommended) SE: Duration of the contract UK: Duration of the contract plus 6 years *General: Data may be kept for 1 year longer for talent pooling purposes, with consent*	The date that the documents are created	Legal requirement with due consideration to the GDPR. Also where applicable, consent.
10	Members of staff appraisal records References and sick leave records	AU: Duration of contract plus 7 years BE: Duration of the contract plus 1 year FR: Duration of the contract (recommended) FI: Duration of the contract (recommended) DE: Duration of the contract or 2 years (whichever is the longer) IE: Duration of the contract plus 7 years LU: Duration of contract plus 10 years NL: Duration of the contract plus 2 years ES: Duration of the contract plus 4 years SE: Duration of the contract plus 2 years (recommended) UK: Duration of the contract plus 6 years	The date that the documents are created	Legal requirement with due consideration to the GDPR
11	Work experience information (Name, address, Date of Birth, Contact Details, Next of Kin details) (for social value/work experience placements)	General: Duration of the work placement	The date that the documents are created	Consent (e.g. from students/through schools)

Payroll Records

REF	RECORD TYPE	Retention Period	Start of Retention Period	JUSTIFICATION
1	Payroll and wages records (including overtime, bonuses and expenses), benefits in kind Payroll for local employees, relocators and shadow payroll (Including childcare vouchers, cycle to work schemes, gym membership, medical insurance benefit, online shopping discount information and other benefits information) Corporate traveller or Click Travel documents/expenses	AU: 7 years BE: 5 years FI: 6 years FR: 5 years DE: 10 years 6 IE: Duration of the contract/employment plus 7 years LU: 5 years NL: 7 years ES:Duration of the contract/employment plus 4 years SE: 7 years UK: 6 years	The financial year in which the payments are made	Legal requirement
2	Maternity pay records	AU: 7 years BE: 5 years FI: 6 years FR: 5 years DE: 10 years IE: Duration of the contract/employment plus 7 years LU: 5 years NL: 7 years ES: Duration of the contract/employment plus 4 years SE: 7 years: UK: 6 years	The end of the tax year in which the maternity pay period ends	Legal requirement
3	Statutory sick pay and records	AU: Duration of the contract plus 7 years BE: Duration of the contract plus 1 year FR: Duration of the contract (recommended) FI: Duration of the contract (recommended) DE: Duration of the contract or 2 years (whichever is the longer) IE: Duration of the contract plus 7 years LU: Duration of the contract (recommended) NL: Duration of the contract plus 2 years ES: Duration of the contract plus 4 years SE: Duration of the contract plus 2 years (recommended) UK: Duration of the contract plus 6 years	The end of the tax year to which the records relate	Legal requirement

Insurance Policies

REF	RECORD TYPE	Retention Period	Start of Retention Period	JUSTIFICATION
1	Depending on the type (Employers' liability, amongst others)	Duration of the Contract /Validity (minimum 7 years)	Until all claims under the policy are barred and all outstanding claims are settled".	Evidence
2	Claims correspondence	All Countries - 3 Years after settlement		Evidence

Marketing and Purchasing Records

REF	RECORD TYPE	Retention Period	Start of Retention Period	JUSTIFICATION
1	Potential customer/ business partner contact information used for direct marketing by phone, text, email, post or fax Business Leads	General: 2 years from the first contact/consent	The date when the customer opted in to receive direct marketing/ contact with potential business partner	Consent (Potential customer) Legitimate Interest (Business partner)
2	Existing customer/ business partner/supplier information used for direct marketing by phone, text, email, post or fax	General: 2 years from the end of the contract/relationship (unless needed due to an ongoing contractual warranty period, etc.	The duration of the contract/relationship	Legitimate Interest of ISG in direct marketing

IT and Websites

REF	RECORD TYPE	Retention Period	Start of Retention Period	JUSTIFICATION
1	User browsing history	Customers/Website Users: Maximum 1 year Employees: Duration of the employment, unless needed for ongoing investigations	The date of collection	Legitimate interest – service optimisation or employment related disputes
2	IP Addresses	Customers/Website Users: Maximum 1 year Employees: Maximum 1 year, unless needed for ongoing investigations	The date of collection	Legitimate interest – service optimisation Legitimate interest – device management/security Legitimate interest - employment related disputes
3	Cookie IDs	Customers/Website Users: Maximum 1 year (exceptions can apply for specifically consented cookies or cookies that do not collect personal data) Employees: Maximum 1 year, unless needed for ongoing investigations	The date of collection	Consent Legitimate interest – service optimisation
4	Location Data/identifiers	Customers/Website Users: Maximum 1 year Employees: Maximum for the duration of the employment	The date of receipt	Consent Legitimate interest – device management/security
5	Device identifiers	Customers/Website Users: 1 year Employees: Maximum for the duration of the employment	The date of receipt	Consent Legitimate interest – device management/security

Other Records

REF	RECORD TYPE	Retention Period	Start of Retention Period	JUSTIFICATION
1	Company Directors'/Bank signatories' personal details (Name, date of birth, address, contact details, Driving licence number, Photo)	General: 1 year	The date of the creation of the document	Legitimate Interest – anti-money laundering and prevention of fraud
2	Bid records (CV, Name, Photo, Contact Details) Proposal References, Client Feedback	General: 10 years maximum (necessary period to use data for upcoming or potential bids)	The date of receipt	Consent (third parties/clients' employees/members of the public) Performance of a contract (employees)
3	Driving Licences (e.g. to check validity for FSS Fleet)	Maximum retention periods: AU: 3 years BE: 10 years FI: 3 years FR: 10 years DE: 30 years IE: 2 years LU: 3 years NL: 10 years ES: 15 years SE: 10 years UK 3 years (specific requirement)	From the date of collection	Legal Obligation Health and safety obligations Duty of care e.g National Health and Safety acts Legitimate Interest (defending against a legal claim)
4	Fuel cards	Duration of employment plus 1 year	The date of issue	Admin operations
5	Road and tax documents (e.g. for FSS Fleet)	UK: Duration of the employment and/or 3 years (statutory limitation on claim for breach of duty of care) (whichever is the longer)	The date of receipt	Legitimate Interest (defending against a legal claim)
6	Related intellectual property agreements	AU: Duration of their validity plus 7 years BE: Duration of their validity FI: Duration of their validity FR: Duration of their validity plus 6 years DE: Duration of their validity IE: Duration of their validity LU: Duration of their validity plus 7 years NL: Duration of their validity or 7 years (whichever is longer) ES: Duration of their validity or 6 years (whichever is longer) SE: Duration of their validity UK: Duration of their validity plus 6 years	The date of execution of the agreements	Legal requirement and to protect the legitimate interests of ISG
7	Permits, licences, certificates	General: As long as necessary for operations of business	The date that the records are created	To protect the legitimate interests of ISG
8	Correspondences containing Personal Data	General: 1 year maximum (yearly clearance should apply)	The date that the records are created	Business operations & Legal requirement with due consideration to the GDPR
9	Subject Access, Portability and Erasure Requests	UK: 6 years maximum ES: 1 year All other countries - 6 years suggested	The date that the request was made	Legal requirement To defend against a legal claim

Project Site Instructions

Appendix 3 to ISG's Data Protection policy

Securing personal information on project sites

1. Introduction

ISG collects large quantities of personal data at our Project Sites, such as identity and qualifications evidence, Health and Safety information and contact details for people entering the site. To ensure we are gathering this information in a secure way, collecting only the information we need, and deleting it when it serves no further purpose, this instruction provides guidance and support for the Project Leadership team. This will help prevent projects incurring additional costs if they have to mitigate data protection risks mid project. In the worst-case, UK and European Data protection legislation allows ISG to be fined up to 4% of its global turnover.

If you have any questions about these instructions, contact the Data Protection Team at data.protection@isgltd.com.

2. Scope

- All UK project sites
- Engineering Services and Logistics and Distribution project sites in Europe
- Other project sites at the discretion of ISG's Statutory Board
- For all other countries ISG operates in, please refer to your local instructions or contact the Data Protection Team for guidance

3. Audience

- Project Directors/Managers – Responsible for ensuring that resources are made available to the project site teams to meet the requirements of this instruction and that the procurement of pre-enrolment and access control systems meet with the data protection requirements listed here. Overall responsibility for data protection compliance on site;
- Site Managers – Ensuring that all inductions to the site follow these guidelines and that personal information/health/accident reports are stored securely and access to the documents is managed;
- Project Procurement/Commercial Managers – Where applicable, ensuring that all contracts have, as a minimum, the standard GDPR clauses. Ensuring that their supply chains adhere to data protection legislation in the regions they operate in;
- Document Controllers – May have delegated responsibility for collection, management, security and destruction of personal information in both electronic and hard-copy forms.

4. Policies

The following ISG policies inform and guide these instructions:

- Data Protection Policy
- Data Retention Policy
- Information Security Policy

- Acceptable Use Policy
- Right to Work Policy
- Global Surveillance Policy
- Surveillance Instructions

5. Before the project site becomes operational

Prior to work commencing on-site, the following key points will help ensure your project site is compliant with data protection legislation and that your project does not incur additional costs by having to mitigate risks mid project.

5.1 Pre-enrolment and Site Access Control systems

- Prior to any procurement being made and, in any event, as soon as possible, the Project Directors/Project Managers are to contact the Data Protection Team at data.protection@isgltd.com, to discuss which pre-enrolment and access control methods/systems are both complaint and suitable for the site. In the event that a system is procured that does not meet the data protection and security standards needed to be compliant with the legislation, the Project will incur additional costs, either to mitigate risks or by having to remove, then replace these systems mid project.
- In the UK, if Facial Recognition, Retina, or Fingerprint Scanners (collectively known as Biometric Readers) are used, you must offer a non-biometric alternative and not penalise the operative for their choice; UK legislation requires you to ensure consent is given freely by the individual. The Project Site Induction Form and the Project Site Privacy Notice reflect this legal requirement. There is one exception to this opt out, that applies to high security sites (nuclear facilities, some UK Government agencies, critical national infrastructure and life science facilities etc) – if you believe your project/site falls into one of these categories, you must contact the Data Protection Team for advice. (email data.protection@isgltd.com).

The European Union has much stricter controls over the use of biometrics, such as in the Netherlands, where they have in most cases been prohibited. For all project sites in the EU, if you believe there is a case for using Biometrics, you must consult with the Data Protection Team before use.

5.2. Privacy Notices

- Each site must have a 'Privacy Notice' displayed; the notice discloses the ways that ISG may gather, use, disclose and manage the personal data that is collected as part of on-site activities.
- The Project Site Privacy Notice can be found in the ISG Management Systems (both the Company Management System and the Retail Management System).
- No changes to the Project Site Privacy Notice can be made without agreement from the Data Protection Officer (DPO).
- Where the standard Project Site Privacy Notice needs amending to reflect more onerous compliance requirements on the project/site, contact the DPO. For example, when the client requires ISG to

undertake vetting and Right to Works, diversity monitoring, enhanced security and immigration checks.

5.3. On-site Health & Safety induction form

- Many sites now use biometric access control methods, such as facial recognition, fingerprint and retina scanners. Please note the requirement, already identified in this guidance, to ensure that everyone entering a site with biometric access controls has a genuine option to select an alternative method of entry, as shown on the induction form.
- Under no circumstances can additional fields be added to ISG's official Health & Safety induction form template without the prior written approval of ISG's Group Health & Safety Director and the DPO (for the data protection elements).
- If you are unsure, or need to make changes to the template induction form provided, or don't know how to find the correct version please contact the H&S Department

5.4. NDA

- If you believe these instructions compromise either the contract with the client, or an NDA, please contact the DPO immediately.

5.5 CCTV

- In the UK, prior to procurement or leasing of CCTV services, which for the avoidance of doubt includes drones, time-lapse photography and body worn cameras, you are to refer to the Surveillance Instructions INSERT HYPERLINK (or maybe appendix???). For more detailed information contact the Data Protection Team for advice.
- Every country ISG operates in has different surveillance guidance. For countries other than the UK, please refer to the Global Surveillance policy, or contact the Data Protection Team for Advice.

6. During the project

When collecting and using personal information ensure that:

- The individual whose personal data you have collected has access to the relevant on-site privacy notice, should they wish to know more about why we need to collect this data, what we do with it and how long we may keep it for.
- The personal information that has been collected is only being used for the reasons that you initially collected the data for, as per the privacy notice. For example, you can't use CCTV footage to monitor attendance on-site if the original reason for collecting this information was purely for security reasons. If you were to use the data that has been collected for additional purposes to those stated in the privacy notice this would be unlawful. If in doubt, contact the DPO.

- The information you hold is kept up to date and ensure that procedures are implemented on-site to allow for such information to be updated on a regular basis.
- Make sure that all hard copies of personal information held on-site are kept in locked cabinets and that only authorised people (Site Manager, HR, H&S team etc) have access to these documents. The location of these files should be where they are not likely to be lost or stolen. Do not store personal information in public spaces.
- You are keeping the information for no longer than is necessary or after its original purpose has expired. The ISG Data Retention Policy provides more detailed instructions. Insert hyperlink

6.1 Security of personal data on site

Security of personal data – for more detail refer to ISG's Acceptable use Policy

- Only use ISG supplied IT equipment on-site.
- Establish access rights to the personal information that is being collected – i.e. which employees/others will be authorised to view/process the data collected – access should be kept to a minimum and be subject to regular review.
- Notify ISG's IT department of any leavers who may have access to IT servers/IT files on-site in order that access rights can be cancelled. This will ensure that leavers cannot access ISG systems once they have left the business.
- Make sure that leavers ISG laptops are securely returned to the IT department without delay.
- Do not share user accounts and passwords to laptops, computers and other IT equipment.
- Laptops, tablets and mobile phones must never be left logged on when unattended and must be stored securely at the end of each working day.
- The use of devices such as memory sticks to transfer data from one laptop/computer to another should be kept to an absolute minimum and when there is no alternative, they must be encrypted.

6.2. Data Breaches and Subject Access Requests

- If you suspect that personal data has been shared with people who are not authorised to view it, or if you believe a systems security has been compromised, contact the IT Service Desk and the DPO immediately. ISG only has 72 hours to report data breaches to the authorities.
- Any ISG Employee, supply chain operative or member of the public may choose to request a copy of their personal data by sending a request to ISG in a number of ways, which could include emails, telephone calls, written letter, verbally, text. If you receive such a request, send it to the DPO immediately as we have to complete the disclosure within 1 month of receipt.

7. Project Completion

At the end of the project, Project/Site Managers/Senior ISG Staff on site will need to ensure the following:

- The information logged in Pre-Enrolment and Access Control systems is deleted, unless there is a requirement to keep it, in accordance with ISG's Data Retention Policy. Insert Hyperlink
- Make sure that all paper and electronic records containing personal information is securely archived or in the case of hard copies, destroyed using a supplier that is approved by UK Facilities – again in accordance with ISG's Data Retention Policy.
- Return all site-specific IT equipment to the IT department without delay – do not dispose of IT equipment yourself.
- Ensure Leavers tickets are raised for everyone who is leaving the employment/contract of ISG and ensure that their ISG provided IT equipment is collected before they leave.
- Ensure surveillance systems, such as CCTV, are decommissioned and images are deleted in a secure manner.

Frequently Asked Questions
Appendix 4 to ISG's Data Protection policy

Securing personal information

As well as the normal personal data collected by HR, Payroll, Line Managers and Finance, ISG collects large quantities of personal data at our Project Sites and Offices. Such as identity and qualifications evidence, Health and Safety information and contact details for people entering the site. To ensure we are collecting this information in a secure way, only collecting the information we need, and deleting it when it serves no further purpose, this addendum provides further detail to support ISG's data protection policy and objectives.

If you have further questions please contact the Data Protection Officer (DPO) at data.protection@isgltd.com.

Scope:

UK and Europe, where the GDPR and the UK Data Protection Act 2018 are enforced

Audience:

- All Employees of ISG, including PAYE, contractor, freelancer and agency staff
- All of ISG's supply chain when processing personal data on behalf of ISG

Policies:

The following ISG policies inform and guide this FAQ:

- Data Protection Policy
- Information Security Policy
- Acceptable Use Policy
- Data Retention Policy and Schedule
- Right to Work Policy
- Global Surveillance Policy
- Global Surveillance Guidance

Frequently asked questions

What is personal data?
Personal data is any information relating to a living person that is already identified or can be identified. There are some pieces of information that can identify a person on their own, including phone numbers, IP addresses, passport numbers and national insurance numbers.

Some pieces of information cannot identify a person on their own, but when you put them together with other pieces of information, you can then identify a person. For example, someone's age and their address do not normally allow you to identify someone on their own, but when you put them together, they may allow you to identify a single person.

What is Sensitive personal data
GDPR defines a subset of personal data as Special Category data, namely information concerning:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership
- Genetic or biometric data (including fingerprint, facial recognition and retina scanners)
- Physical or mental health
- Sexuality or sex life

Frequently Asked Questions
Appendix 4 to ISG's Data Protection policy

The rules regarding Special Category data are stricter, so before you collect or use any of the information mentioned here, you should contact the DPO for advice data.protection@isgltd.com .

Can anyone visiting a project site refuse to give personal information?
Where ISG rely on consent to process information, such as providing biometric information (fingerprints, retina scans and facial recognition, the individual may refuse to give their personal information without consequence and ISG must provide an alternative method of access. In the UK this applies in all cases to the collection of biometric data. Rules vary by country, check the local Privacy Notice or consult the Data Protection Team.

Where ISG relies on another legal basis, such as legitimate interest or legal obligation, an individual can refuse to give their personal information however that may result in refusal of admittance on the site.

ISG has a legitimate interest or legal obligation to ask for all fields of the Health & safety induction form to be completed prior to entry into a project site.

Why is the GDPR and the UK's Data protection Act 2018 so important?
The European Union's GDPR and the UK's Data Protection Act 2018 came into force in May 2018 and were designed to strengthen privacy rules and requirements around how information relating to individuals can be used. It has updated and unified data protection law across all member states of the European Union (EU) and the UK. It also establishes new rules governing how personal data is handled by organisations and extends the rights of individuals regarding their own personal data.

There are several reasons for spending money, time, and effort in ensuring the protection of personal information. These include:

- Protecting your personal data
- Avoiding regulatory fines
- Maintaining ISG's reputation with existing and future clients
- Compliance with regulatory requirements
- Maintaining high levels of productivity

As computers and technology have become integral to business operations, data requirements from regulators such as the Information Commissioner's Office (ICO), as well as from customers, have been imposed on businesses.

What are my responsibilities?
All ISG employees have some responsibility for ensuring that personal data is collected, stored and handled appropriately. Such responsibilities include:

- Ensuring that personal data is handled and processed in line with ISG's Data protection policy and the data protection principles highlighted in this guide and on Workspace
- Ensuring the transmission of personal data is appropriately secure
- The completion of appropriate data protection training as may be requested by ISG from time to time
- The immediate reporting of any suspected or actual data breaches
- The immediate reporting of any information security weaknesses or events
- Submitting any data protection requests to the data protection team

Security
ISG will implement technical and organisational measures to guard against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
The Information Security Policy sets out ISG's strategic intent to provide a high level of security for both its own and clients data. For more information please refer to the Information Security Policy:
These measures are meant to ensure that ISG;

- designs and organises its security to fit the nature of the personal data it holds and the harm that may result from a security breach;
- is clear about who in the organisation is responsible for ensuring information security;
- has the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
- is ready to respond to any breach of security swiftly and effectively.

In order to achieve the goals listed above, all ISG Employees are required to comply with ISG's Acceptable Use Policy.

What if I lose a device or share the wrong information?

Frequently Asked Questions
Appendix 4 to ISG's Data Protection policy

- If you lose any device, you must notify the UK IT Service Desk and the DPO as soon as possible;

- If you incorrectly share personal information with the wrong recipients, such as emailing the wrong people, immediately contact the recipients and ask for the email to be deleted. Also inform the DPO without delay.