Data Protection Policy

Contents

Introduction

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of GGL Security. This includes obligations in dealing with personal data, in order to ensure that GGL Security complies with the requirements of the relevant and applicable Data Protection Law.

Rationale

GGL Security must comply with the Data Protection principles set out in the relevant Data Protection Law.

- Data Protection Acts 1988 and 2003 (parts not repealed)
- Data Protection Act 2018
- ePrivacy Regulations 2011
- General Data Protection Regulation (EU Regulation 679/2016)
- *As and from date yet to be determined, ePrivacy Regulation currently in proposal form (EU Regulation Proposal)*

This Policy applies to all Personal Data collected, processed and stored by GGL Security in relation to its staff, service providers, clients and other connections in the course of its activities. GGL Security makes no distinction between the rights of Data Subjects who are employees, and those who are not. All are treated equally under this Policy.

Scope

The policy covers both personal and special category personal data held in relation to data subjects by GGL Security. The policy applies equally to personal data held in manual and automated form.

All Personal and Special Category Data will be treated with equal care by GGL Security. Both categories will be equally referred-to as Personal Data in this policy, unless specifically stated otherwise.

GGL Security is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions will apply within this Policy.

Data	This includes both automated and manual data. Automated data means data held on computer or stored with the intention that it is processed on computer.

	Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.
Pseudonymous Data	This data is still treated as personal data because it enables the identification of individuals albeit via a key.
Anonymous Data	This data Is rendered anonymous because there is no way that an individual can be identified from this data. Therefore, the GDPR does not apply to such data.
Personal Data	Information which relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of the Data Controller. (If in doubt, GGL Security refers to the definition issued by the Article 29 Working Party and updated from time to time.)
Special Category Personal Data	A particular category of Personal data, relating to: Racial or Ethnic Origin, Political Opinions, Religious, Ideological or Philosophical beliefs, Trade Union membership, Information relating to mental or physical health, information in relation to one's Sexual Orientation, information in relation to commission of a crime and information relating to conviction for a criminal offence.
Data Controller	A person or entity who, either alone or with others, controls the content and use of Personal Data by determining the purposes and means by which that Personal Data is processed.
Data Subject	A living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.
Data Processor	A person or entity who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract, but who is not an employee of the Data Controller, processing such Data in the course of his/her employment.
Data Protection Law	Includes EU Regulations and National Law as listed above
Data Protection Officer	A person appointed by GGL Security to monitor compliance with the appropriate Data Protection Law, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members and service recipients. If a Data Protection Co-Ordinator has been appointed, then they shall be referred to as a DPC in this document.
ePR	The proposal for a new EU electronic Privacy Regulation (ePR) which is still in proposal/draft form. This Regulation should come into effect together with the GDPR but there may be a delay in implementation.
GDPR	The new EU General Data Protection Regulation (GDPR) - Regulation 2016/679 which comes into effect in May 2018 and replaces the current Data Protection Directive 95/46/EC and the national legislation that has been implemented from the Directive.
Processing	Processing means performing any operation or set of operations on data, including: • Obtaining, recording or keeping data;

	• Collecting, organising, storing, altering or adapting the data; • Retrieving, consulting or using the data; • Disclosing the information or data by transmitting; • Disseminating or otherwise making it available; • Aligning, combining, blocking, erasing or destroying the data.
Relevant Filing System	Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.

GGL Security as a Data Controller

In the course of its daily organisational activities, GGL Security acquires, processes and stores personal data in relation to:

- Potential Employees of GGL Security
- Employees of GGL Security
- Potential Customers of GGL Security
- Customers of GGL Security
- Third party service providers engaged by GGL Security
- Associates of GGL Security
- Industry Contacts of GGL Security

In accordance with Data Protection Law, this data must be acquired and managed fairly. Not all staff members will be expected to be experts in Data Protection Law. However, GGL Security is committed to ensuring that its staff have sufficient awareness of the Law in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff must ensure that the Data Protection Officer or appointed Data Protection Co-Ordinator is informed, and in order that appropriate corrective action is taken.

Due to the nature of the services provided by GGL Security, there is regular and active exchange of personal data between GGL Security and its Data Subjects. In addition, GGL Security exchanges personal data with Data Processors on the Data Subjects' behalf.

This is consistent with the obligations of GGL Security under the terms of its contract with its Data Processors.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that a staff member of GGL Security is unsure whether such data can be disclosed. In general terms, the staff member should consult with the Data Protection Officer or appointed Data Protection Co-Ordinator to seek clarification.

Data Flow and Mapping

GGL Security has engaged in a data flow and mapping exercise in order to identify the elements of personal data that are being processed. GGL Security has documented data flows and data stores.

Third-Party Processors and Service Providers

In the course of its role as Data Controller, GGL Security engages a number of Third-Party Processors and Service Providers to process Personal Data on its behalf. Collectively, they are referred to as Data Processors. In each case, a formal, written contract is in place with the Processor, outlining their obligations in relation to the Personal Data, the specific purpose or purposes for which they are engaged, and the understanding that they will process the data in compliance with Data Protection Law.

The following categories of data processors are used in the course of business:

- Cloud web hosting services with providers to do analytics, forms and scheduling.
- Business administration services that do document management, accounting and document verification.
- Payment service providers including the bank and payment processors.
- Location and CCTV monitoring tools
- Video and voice recording tools
- Social Media platforms

These categories may be updated from time to time and for an updated list of categories of data processors please contact the Data Protection Co-Ordinator.

Implementation

As a Data Controller, GGL Security processes Personal Data in a manner compliant with the Data Protection Law. Further, as a Data Controller, GGL Security ensures that any entity which processes Personal Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection Law.

Failure of the staff of GGL Security to process Personal Data in compliance with this policy may result in disciplinary proceedings. Failure of a Data Processor to manage the data of GGL Security in a compliant manner will be viewed as a breach of contract and will be pursued through the courts.

The Data Protection Co-Ordinator

As part of the General Data Protection Regulation (GDPR), it is not mandatory for GGL Security to have a formally appointed DPO, however GGL Security has appointed a Data Protection Co-Ordinator to fulfil the role of a DPO. This role facilitates compliance and ensures that in carrying out its “core activities” – the primary services provided by GGL Security - all private individuals’ data held and processed by GGL Security, such as internal staff, GGL Security service users, and third parties, is appropriately protected in line with their regulatory rights.

The contact details of the DPC will be published to all data subjects (internal and external), and (if a DPO is appointed) also communicated to the relevant data protection authority. The latter is achieved by annually registering with the relevant data protection authority. The published details will include a postal address, a dedicated telephone number and a dedicated e-mail address. The name of the DPC does not need to be publicly published.

The DPC will be included in any matters involving data protection at the earliest possible stage, including privacy impact assessments, data processing activities that may affect data subjects and incidents which effect the data of subjects. This may involve the DPC attending middle and senior

management meetings. Where it is decided not to follow the DPC's advice, the matter of discussion, the discussion, the DPC recommendation, and the reasons for not adhering to the recommendation should be formally recorded.

Appointment of a DPC

GGL Security has appointed a DPC to co-ordinate and facilitate data protection matters within GGL Security. The DPC has been appointed on the basis of professional qualities and knowledge of data protection law and practices. The DPC has been and will continue to be educated and upskilled in order to ensure best practice within their role as DPC. As far as possible, GGL Security shall avoid a situation where the DPC is presented with a conflict of interest in their regular duty to GGL Security and their duty toward data protection.

Management Facilitation of the DPC

By Article 38(2) of the GDPR, GGL Security management will support the DPC by providing:

- the necessary resources to carry out his / her tasks, including finance, infrastructure (premises, facilities, and equipment), and staff where appropriate
- access to personal data and processing operations
- the resources for him / her to maintain their expert data protection knowledge such as continuous training
- active support by senior management
- adequate time to fulfil their DPC duties. A specific percentage of their weekly time should be dedicated to data protection activities
- communication of the DPC role and their activities to employees within GGL Security
- access to other services such as, but not limited to, HR, legal, IT, and security for support and information to fulfil their duties

The DPC will also not receive any instructions regarding the exercise of his / her tasks and must be in a position to perform his / her duties and tasks in an independent manner. The DPC cannot *"be dismissed or penalised by the controller GGL Security or the processor for performing [his / her] tasks."*

Responsibilities of the DPC

The GDPR specifies that the DPC's role is to *"assist the controller or the processor to monitor internal compliance with this Regulation [GDPR]".* As such, the DPC must monitor the ongoing data processing and storage of personal data by GGL Security via:

- collection of information to identify processing activities
    - If required to do so by law, the DPC must maintain the "record of processing operations", a document required by the GDPR which details all the personal data processing activities of GGL Security
- analysis and checking the compliance of processing activities with GDPR, the Data Protection Acts, and internal policies
    - This will be accomplished via technical controls, reviews, assessments, and audits

    - This also involves assigning responsibility for raising awareness and continuous internal data protection training for staff and management, and ensuring they are carried out adequately
- informing, advising, and issuing recommendations to management and employees of their obligations under the GDPR and the Data Protection Acts

Although the DPC is bound by secrecy / confidentiality concerning their tasks, they are encouraged to contact and seek advice from the relevant data protection authority.

Data Protection Impact Assessments

Note that it is the task of GGL Security, not the DPO, to carry out Data Protection Impact Assessments (DPIAs) as necessary; however, the DPC provides advice and guidance at each stage of the DPIA as follows:

- whether or not to carry out a DPIA
- what methodology to follow when carrying out a DPIA
- whether to carry out the DPIA in-house or whether to outsource it
- what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects
- whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR

Again, where adherence is not paid to the DPC's advice, this should be formally recorded in the DPIA documentation.

The Data Protection Principles

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. Article 5 in the GDPR states that all personal data must be:

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

statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;
- 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;
- Article 5(2) states that the Controller is responsible for and must be able to demonstrate compliance with the Data Protection Principles.

Lawful, Fair and Transparent Data Processing

The Regulation seeks to ensure that personal data is processed lawfully, fairly and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

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

GGL Security will ensure that at least one of the conditions outlined above will be satisfied whenever any processing activities take place.

In order to obtain personal data fairly and in a transparent manner, GGL Security will make the data subject aware of the following at the time the data is collected directly:

- Identity of the controller and the Data Protection Officer or appointed Data Protection Co-Ordinator
- Purpose and legal basis for processing. An explanation of the legitimate interest of GGL Security will be provided if it is being used as the legal basis.
- Data subject's rights to withdraw consent, request access, rectification or restriction of processing.
- Data subject's rights to complain to the relevant data protection authority
- Recipients of the personal data.
- Storage periods or criteria used to determine the length of storage.
- Legal basis for intended international transfer of data to a third country or organisation, including the fact that either the receiving country has an adequacy decision from the

relevant data protection authority or other appropriate safeguards are in place and how to obtain a copy.

In situations where the data is not being collected directly from the data subject, GGL Security will provide the source along with the other information listed above to the data subject within a reasonable period after obtaining the data but not more than one month. Information will not be provided to the data subject if it will require disproportionate effort or it would render it impossible or seriously impair the purpose of the data processing.

GGL Security will place a Fair Processing Notice in a highly visible position, if it intends to record activity on CCTV or video.

The Data Subject's data will not be disclosed to a third party other than to a party contracted to GGL Security and operating on its behalf.

Processed for Specified, Explicit and Legitimate Purposes

GGL Security follows this purpose limitation principle and only collects and processes personal data for the specific purposes set out in the "Record of Processing Activities" document held by GGL Security. The purposes for which we process personal data will be informed to data subjects at the time their personal data is collected or not more than a month if obtained from a third party.

GGL Security will not further process personal data in a manner that is incompatible with those purposes unless:

- the consent of the data subject has been obtained, or
- if the further processing is for archiving purposes in the public interest or scientific and historical research or statistical purposes and the appropriate safeguards are in place and there is no risk of breaching the privacy of the data subject.

Adequate, Relevant and Limited Data Processing

GGL Security follows this data minimisation principle and only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects.

Accuracy of Data and Keeping Data Up to Date

GGL Security will ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data will be checked when it is collected and thereafter, see below. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

- Remind Data Subjects on an annual basis to inform GGL Security of any changes to their details.
- Conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date.
- Conduct annual audit to establish the need to keep certain Personal Data.
- Amend inaccurate data which has been notified to GGL Security by the Data Subject or is revealed as a result of a subject access request.

Timely Processing

GGL Security follows this storage limitation principle and does not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed.

GGL Security will verify whether statutory data retention periods exist in relation to the type of processing e.g., personal data may need to be kept in order to comply with tax, health and safety, or employment regulations etc. If the law is silent, internal data retention periods will be set to meet the storage limitation principle.

Retention periods will be set considering the purpose or purpose for which the data is collected and used, and once the storage periods expire, data will be securely deleted/destroyed in the absence of a sound new lawful basis to retain it. However, personal data may be stored for longer periods by GGL Security insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific, historical research or statistical purposes ensuring appropriate safeguards are in place i.e. irreversibly anonymised.

GGL Security keeps record of this in a Data Retention Schedule.

Secure Processing

GGL Security will ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. The state of technological development, the cost of implementing the measures, the nature of the data concerned and the degree of harm that might result from unauthorised or unlawful processing are all considered when GGL Security are determining the security measures that are put in place.

Accountability

Under the GDPR, organisations are obliged to demonstrate that their processing activities are compliant with the Data Protection Principles. The principle of accountability seeks to guarantee the enforcement of the Principles.

GGL Security will demonstrate compliance in the following ways:

- If required by law, by keeping an internal record of all personal data collected, held or processed as per Article 30 - “Records of Processing Activities”. Upon request, these records will be disclosed to the relevant data protection authority. GGL Security is currently not required to maintain this record as GGL Security enjoys an exception in this regard.
    - When GGL Security is acting as a Data Controller this record will contain the following:
        - Contact details of the Controller/representative/Data Protection Officer
        - List of personal data being processed
        - Categories of data subjects
        - Processing activities
        - Categories of recipients with whom the data will be shared
        - Retention periods
        - Deletion methods
        - International transfers and measures in place to ensure they are lawful
        - Detailed descriptions of the security measures implemented in respect of the processed data

    - When GGL Security is acting as a Data Processor this record will contain the following:
        - Name of Controller
        - Name of Data Protection Officer
        - Categories of processing carried out on behalf of the Controller
        - International transfers and measures in place to ensure they are lawful
- In order to assess the potential risks arising out of any new processing activity the GDPR requires organisations to conduct a Data Protection Impact Assessment (DPIA). GGL Security will demonstrate its compliance by carrying out Assessments whenever any new processing activity is proposed, especially where it involves new technologies, resulting in a high degree of risk for data subjects. After the PIA has been carried out and if all the risks cannot be mitigated, then GGL Security will consult with the relevant data protection authority. The DPIA will be overseen by the Data Protection Officer or appointed Data Protection Co-Ordinator of GGL Security and the DPIAs will be filed and retained as proof of compliance.
- GGL Security will appoint a Data Protection Officer if required i.e. if its core data processing activities involve:
    - Regular and systematic monitoring of data subjects on a large scale; or
    - Processing special category personal data on a large scale.
- GGL Security maintains a data protection document framework i.e. policies & procedures, training records etc.
- GGL Security ensures that data protection by design is addressed throughout the life cycle of any processing activity but especially at the time of planning the means and type of processing and during the processing itself. Necessary safeguards are integrated into the systems of GGL Security with the use of data minimisation and pseudonymisation as privacy enhancing tools. GGL Security assess the risks of a process and tries to mitigate those risks in order to meet the data protection by design requirements.
- GGL Security also ensures that data protection by default is implemented by choosing the most data protective setting as the default i.e. users will have to opt in to any settings that presents greater risks. By default, only the personal data that is necessary is processed.

Special Category Data

At times GGL Security may be required to process special category data. The Data Subject will be notified of this at the data collection point. GGL Security will only process special category data on one of the following grounds:

- Explicit Consent – The individual has given their clear and unambiguous explicit consent.
- Legal obligation related to employment – The processing is necessary for the purposes of carrying out a legal obligation and exercising specific rights of GGL Security or of the individual in the field of employment, social security law or for a collective agreement.
- Vital interests – The processing is necessary to protect the vital interests of the individual or of another person where the data subject is physically or legally incapable of giving consent.
- Not-for-Profit bodies – The processing is carried out in the course of the legitimate activities, with appropriate safeguards by the Not-for-Profit body and on condition that the processing only relates to members or related persons, or to former members of the body, or to persons who have regular contact with it in connection with its purposes and the personal data is not disclosed outside that body without consent.

- Public Information – the processing relates to personal data which is manifestly made public by the individual.
- Legal Claims – The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- Substantial public interest - The processing is necessary for reasons of substantial public interest.
- Healthcare – The processing is necessary for the purposes of preventive or occupational medicine, (i.e., healthcare purposes), for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or Irish law, or pursuant to contract with a health professional and is subject to suitable safeguards.
- Public Heath- The processing is necessary for reasons of public interest purposes and is subject to suitable safeguards.
- Archiving – The processing is necessary for archiving scientific or historical research purposes or statistical purposes and based on EU or Irish law.

Data Subject Access Requests

As part of the day-to-day operation of GGL Security, the staff of GGL Security engage in active and regular exchanges of information with Data Subjects. Where a formal request is submitted by a Data Subject in relation to the data held by GGL Security, such a request gives rise to access rights in favour of the Data Subject. Data Subjects can exercise their rights by contacting the Data Protection Officer or appointed Data Protection Co-Ordinator utilising the contact details listed herein.

Where a formal request is submitted by a Data Subject in relation to the data held by GGL Security, such a request gives rise to access rights in favour of the Data Subject, the Regulation sets out the following rights applicable to data subjects:

- The right to be informed (see above);
- The right of access;
- The right of rectification;
- The right to erasure (also known as the “right to be forgotten”);
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights with respect to automated decision-making and profiling.
- The right to withdraw consent

There are specific time-lines (30 days) within which GGL Security must respond to the Data Subject, depending on the nature and extent of the request. The staff of GGL Security will ensure that, where necessary, such requests are forwarded to the Data Protection Officer or appointed Data Protection Co-Ordinator in a timely manner, and they are processed as quickly and efficiently as possible.

Transferring Personal Data to a Country Outside the EEA

At this stage, GGL Security as Data Controller does not transfer personal data to countries outside the EEA. However, if GGL Security does transfer (“transfer” includes making available remotely) other personal data to countries outside the Economic European Area (EEA) then the following will apply.

The transfer of personal data to a "third country" i.e. outside the EEA, will only take place if one or more of the following applies:

- Is a country that the European Commission has determined to have an adequate level of protection for personal data;
- The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority; certification under an approved certification mechanism as provided for in the Regulation; contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
- The transfer is made with the informed consent of the relevant data subject(s);
- The transfer is necessary for the performance of a contract between the data subject and GGL Security (or for pre-contractual steps taken at the request of the data subject);
- The transfer is necessary for important public interest reasons;
- The transfer is necessary for the conduct of legal claims;
- The transfer is necessary to protect the vital interests of the data subjects or other individuals where the data subject is physically or legally unable to give their consent; or
- The transfer is made from a register that, under relevant data protection law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

Data Breach Notification

If a Data Subject becomes aware of a Data Breach, then the Data Subject is encouraged to contact the Data Protection Officer or Data Protection Co-Ordinator immediately with all known information.

It should be noted that GGL Security treat data breaches very seriously and any employee who becomes aware of a likely data breach and fails to notify the Data Protection Officer or Data Protection Co-Ordinator or, if GGL Security has in place, a member of the Data Protection Committee may be subject to the disciplinary procedure of GGL Security depending on the severity of the breach.

Organisational and Technical Measures for Security and Safety

GGL Security shall ensure that the following organisational measures are taken with respect to the collection, holding, and processing of personal data:

- All employees, agents, contractors, or other parties working on behalf of GGL Security handling personal data:
    - Will be appropriately trained to do so;
    - Must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of GGL Security arising out of this Policy and the Regulation

    - Bound to do so in accordance with the principles of the Regulation and this Policy by contract
- All employees, agents, contractors, or other parties working on behalf of GGL Security:
    - Will be made fully aware of both their individual responsibilities and the responsibilities of GGL Security under the Regulation and under this Policy and will be provided with an opportunity to read this Policy. A document stating that this document has been read and understood should be signed by all relevant parties.
    - That need access to and use of, personal data in order to carry out their assigned duties correctly will have access to personal data held by GGL Security.
- Methods of collecting, holding and processing personal data will be regularly evaluated and reviewed;
- The performance of those employees, agents, contractors, or other parties working on behalf of GGL Security handling personal data shall be regularly evaluated and reviewed.
- Only people who are authorised to use the data can access it. GGL Security will ensure that only authorised persons have access to any personal or special category data held by GGL Security. Employees are required to maintain the confidentiality of any data to which they have access.

GGL Security shall ensure that the following technical measures are taken with respect to the collection, holding, and processing of personal data:

- Secure lockable desks and cupboards: Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- Methods of disposal: Paper documents should be shredded. Discs containing data should be physically destroyed when they are no longer required.
- Equipment: Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

Responsibilities

Everyone who works for or with GGL Security has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **board of directors** is ultimately responsible for ensuring that [GGL Security] meets its legal obligations.

- The Data Protection Co-Ordinator is responsible for:

    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.

- Dealing with requests from individuals to see the data [GGL Security] holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

Registration with the Supervisory Authority

GGL Security is not required to register with the Supervisory Authority and has officially documented reasons for not registering.

Appointed Data Protection Officer / Co-Ordinator and Contacting GGL Security

GGL Security shall accept communication address to either the Data Protection Officer or Co-Ordinator

via email at

info@gglsecurity.com

via post at

Harbour House

Lock Quay

Limerick

Ireland

Policy Review

GGL Security will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives on at least an annual basis and more frequently if required taking into account changes in the law and organisational or security changes.