Data Breach Policy & Procedures

Contents

Policy Statement

Aqqord is committed to our obligations under the regulatory system and in accordance with the GDPR. We maintain a robust and structured program for compliance adherence and monitoring. We carry out frequent risk assessments and gap analysis reports to ensure that our compliance processes, functions and procedures are fit for purpose and that mitigating actions are in place where necessary, however should there be any data breaches, this policy states our intent and objectives for dealing with such a breach.

Although we understand that not all risks can be completely mitigated, we operate a robust and structured system of controls, measures and processes to help protect data subjects and their personal information from the risks associated with processing data. The protection and security of the data that we hold and use, including personal information, is paramount to us and we have developed data specific controls and protocols for any breaches involving personal information and data subject to the GDPR requirements.

Purpose

The purpose of this policy is to provide Aqqord's intent, objectives and procedures regarding data breaches involving personal information. This policy is specific to personal information and the breach requirements set out in the GDPR.

As we have obligations under the GDPR, we also have a requirement to ensure that the correct procedures, controls and measures are in place and disseminated to all employees if a personal information breach occurs. This policy also notes our processes for reporting, communicating and investigating any such breach.

Whilst it is Aqqord's aim to prevent data breaches where possible, we do recognise that human error and risk elements occur in business that prevent the total elimination of any breach occurrence. We also have a duty to develop protocols for data breaches to ensure that employees, the supervising authority and associated bodies are aware of how we handle any such breach.

Scope

The policy relates to all staff *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with Aqqord in the UK or overseas)* within the organisation and has been created to ensure that staff deal with the area that this policy relates to in accordance with legal, regulatory, contractual and business expectations and requirements.

Data Security & Breach Requirements

Aqqord's definition of a personal data breach for the purposes of this policy is any breach of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Alongside our *'Privacy by Design'* approach to protecting data, we also have a legal, regulatory and business obligation to ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred. Our Information Security Policy & Procedures and GDPR Policy & Procedures provide the detailed measures and controls that we take to protect personal information and to ensure its continued security.

We carry out information audits to ensure that all personal data held and processed by us is accounted for and recorded, alongside risk assessments as to the scope and impact a data breach could have on data subject(s).

We have implemented adequate, effective and appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including *(but not limited to*): -

- Encryption of personal data
- Restricted access
- Reviewing, auditing and improvement plans for the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Disaster Recovery and Business Continuity Plan to ensure up-to-date and secure backups and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Audit procedures and stress testing on a regularly basis to test, assess, review and evaluate the effectiveness of all measures and compliance with the data protection regulations and codes of conduct
- Frequent and rolling training programs for all staff in the GDPR, its principles and applying those regulations to each role, duty and the company as a whole
- Staff assessments and testing to ensure a high level of competency, knowledge and understanding of the data protection regulations and the measures we have in place to protect personal information
- Recheck processes to ensure that where personal information is transferred, disclosed, shared or is due for disposal, it is rechecked and authorised by the Compliance Officer

Objectives

- To adhere to the GDPR and UK Data Protection laws and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any data breaches
- To develop and implement adequate, effective and appropriate technical and organisational measures to ensure a high level of security with regards to personal information
- To utilise information audits and risk assessments for mapping data and reducing the risk of breaches
- To have adequate and effective risk management procedures for assessing any risks presented by processing personal information
- To ensure that any data breaches are reported to the correct regulatory bodies within the timeframes as set out in their code of practice or handbooks
- To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring
- To use the Compliance Breach Incident Form for all data breaches, regardless of severity so that any patterns in causes can be identified and corrected
- To protect consumers, clients and staff – including their data, information and identity
- To ensure that where applicable, the Compliance Officer is involved in and notified about all data breaches and risk issues
- To ensure that the Supervisory Authority is notified of the data breach (*where applicable*) with immediate effect and at the latest, within 72 hours after having become aware of the breach

Data Breach Procedures & Guidelines

Aqqord has robust objectives and controls in place for preventing data breaches and for managing them in the rare event that they do occur. Due to the nature of our business, Aqqord process and stores personal information and confidential data and as such, we have developed a structured and documented breach incident program to mitigate the impact of any data breaches and to ensure that the correct notifications are made.

We carry out frequent risk assessments, reviews, audits and gap analysis reports on all processing activities and personal data storage, transfers and destruction to ensure that our compliance processes, functions and procedures are fit for purpose and are mitigating the risks wherever possible.

Breach Monitoring & Reporting

Aqqord has appointed Yaakov Smith as Compliance Officer who is responsible for the review and investigation of any data breach involving personal information, regardless of the severity, impact or containment. All data breaches are reported to this person with immediate effect, whereby the procedures and forms detailed in this policy are enacted.

All data breaches will be investigated, even in instances where notifications and reporting is not required and we retain a full record of all data breaches to ensure that gap and pattern analysis are used. Where a system or process failure has given rise to a data breach, revision to any such process is recorded in the Change Management and Document Control records.

Breach Incident Procedures

Identification of an Incident

As soon as a data breach has been identified, it is reported to the Compliance Officer immediately so that breach procedures can be initiated and followed without delay.

Reporting incidents fully and with immediate effect is essential to the compliant functioning of Aqqord and is not about apportioning blame. These procedures are for the protection of Aqqord, its staff, customers, clients and third parties and are of the utmost importance for legal regulatory compliance.

As soon as an incident has been reported, measures must be taken to contain the breach. Such measures are not in the scope of this document due to the vast nature of breaches and the variety of measures to be taken; however, the aim of any such measure should be to stop any further risk/breach to the organisation, customer, client, third-party, system or data prior to investigation and reporting.

Breach Recording

Aqqord utilises the Breach Incident Form for all incidents and is completed after every instance of a data breach, regardless of severity or outcome. Completed forms are logged in the Breach Incident Folder and reviewed against existing records to ascertain any patterns or reoccurrences.

In cases of data breaches, the Compliance Officer is responsible for carrying out a full investigation, appointing the relevant staff to contain the breach, recording the indecent on the breach form and making any relevant and legal notifications. The completing of the Breach Incident Form is only to be actioned after containment has been achieved.

A full investigation is conducted and recorded on the incident form, the outcome of which is communicated to all staff involved in the breach in addition to upper management. A copy of the completed incident form is filed for audit and record purposes.

If applicable, the Supervisory Authority and the data subject(s) are notified in accordance with the GDPR requirements (refer to Breach Notifications section this policy). The Supervisory Authority protocols are to be followed and their '***Security Breach Notification Form'*** should be completed and submitted. In addition, any individual whose data or personal information has been compromised is notified if required, and kept informed throughout the investigation, with a full report being provided of all outcomes and actions.

Breach Risk Assessment

Human Error

Where the data breach is the result of human error, an investigation into the root cause is to be conducted and a formal interview with the employee is to be held.

A review of the procedure/s associated with the breach is to be conducted and a full risk assessment completed in accordance with Aqqord existing Risk Assessment Procedures. Any identified gaps that are found to have caused/contributed to the breach are to be revised and risk assessed to mitigate any future occurrence of the same root cause.

Resultant employee outcomes of such an investigation can include, but are not limited to: -

- Re-training in specific/all compliance areas
- Re-assessment of compliance knowledge and understanding
- Suspension from compliance related tasks
- Formal warning *(in-line with Aqqord's disciplinary procedures)*

System Error

Where the data breach is the result of a system error/failure, the IT team is to work in conjunction with the Compliance Officer to assess the risk and investigation the root cause of the breach. A gap analysis is to be completed on the system/s involved and a full review and report to be added to the Breach Incident Form.

Any identified gaps that are found to have caused/contributed to the breach are to be revised and risk assessed to mitigate and prevent any future occurrence of the same root cause.

Full details of the incident should be determined and mitigating action such as the following should be taken to limit the impact of the incident:

- Attempting to recover any lost equipment or personal information
- Shutting down an IT system
- Removing an employee from their tasks
- The use of back-ups to restore lost, damaged or stolen information
- Making the building secure
- If the incident involves any entry codes or passwords, then these codes must be changed immediately and members of staff informed

Assessment of Risk and Investigation

The Compliance Officer should ascertain what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches.

The lead investigator should look at: -

- The type of information involved
- It's sensitivity or personal content
- What protections are in place (e.*g. encryption*)?
- What happened to the information/Where is it now?
- Whether there are any wider consequences/implications to the incident

The appointed lead should keep an ongoing log and clear report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation and any recommendations for future work/actions.

Breach Notifications

Aqqord understands that we have obligations and a duty to report data breaches in certain instances. All staff are aware of these circumstances and we have strict internal reporting lines to ensure that data breaches falling within the notification criteria are identified and reported without undue delay.

Supervisory Authority Notification

The Supervisory Authority is to be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals. These are situations which if the breach was ignored, it would lead to significant detrimental effects on the individual.

Where applicable, the Supervisory Authority is notified of the breach no later than 72 hours after us becoming aware of it and are kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible and always within any specified timeframes.

If for any reason it is not possible to notify the Supervisory Authority of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay. Where a breach is assessed by the Compliance Officer and deemed to be ***unlikely*** to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Supervisory Authority in accordance with Article 33 of the GDPR.

The notification to the Supervisory Authority will contain: -

- A description of the nature of the personal data breach
- The categories and approximate number of data subjects affected
- The categories and approximate number of personal data records concerned
- The name and contact details of our Compliance Officer and/or any other relevant point of contact (*for obtaining further information)*
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach *(including measures to mitigate its possible adverse effects)*

Breach incident procedures and an investigation are always carried out, regardless of our notification obligations and outcomes and reports are retained to be made available to the Supervisory Authority if requested.

Where Aqqord acts in the capacity of a processor, we will ensure that controller is notified of the breach without undue delay. In instances where we act in the capacity of a controller using an external processor, we have a written agreement in place to state that the processor is obligated to notify us without undue delay after becoming aware of a personal data breach.

Data Subject Notification

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written format and in a clear and legible format.

The notification to the Data Subject shall include: -

- The nature of the personal data breach
- The name and contact details of our Compliance Officer and/or any other relevant point of contact (*for obtaining further information)*
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach *(including measures to mitigate its possible adverse effects)*

We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational protection measures which render the data unintelligible to any person who is not authorised to access it *(i.e. encryption, data masking etc*) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

Record Keeping

All records and notes taking during the identification, assessment and investigation of the data breach are recorded and signed by the Compliance Officer and are retained for a period of 7 years from the date of the incident. Incident forms are to be reviewed monthly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

Responsibilities

Aqqord will ensure that all staff are provided with the time, resources and support to learn, understand and implement all procedures within this document, as well as their responsibilities and the breach incident reporting lines.

The Compliance Officer is responsible for regular compliance audits and gap analysis monitoring and their subsequent reviews and action follow ups.

Data Protection (GDPR) Policy & Procedure

Contents

1. Policy Statement

Aqqord needs to collect personal information to effectively and compliantly carry out our everyday business functions and activities and to provide the products and services defined by our business type. Such data is collected from employees, customers, suppliers and clients and includes *(but is not limited to),* name, address, email address, IP address, and telephone numbers.

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

Aqqord has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the GDPR and its principles, including staff training, procedure documents, audit measures and assessments. Ensuring and maintaining the security and safety of personal data belonging to the individuals with whom we deal is paramount to our company ethos and Aqqord adheres to the GDPR and its associated principles in every process and function.

We are proud to operate a 'Privacy by Design' approach and aim to be proactive not reactive; assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of our business.

2. Purpose

The purpose of this policy is to ensure that Aqqord is meeting its legal, statutory and regulatory requirements under the GDPR and to ensure that all personal information is safe, secure and processed compliantly whilst in use and/or being stored and shared by us. We are dedicated to compliance with the GDPR's principles and understand the importance of making personal date safe within our organisation.

The GDPR includes provisions that promote accountability and governance and as such Aqqord has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data.

2.1. Scope

The policy relates to all staff *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with Aqqord in the UK or overseas)* within the organisation and has been created to ensure that staff deal with the area that this policy relates to in accordance with legal, regulatory, contractual and business expectations and requirements.

2.2. Definitions

- ***GDPR*** means the General Data Protection Regulation and for the purposes of this document, the acronym is also used to collectively describe all of the data protection laws that Aqqord complies with.
- ***Personal data*** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- ***Processing*** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation,

structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- ***Data subject*** means an individual who is the subject of personal data
- ***Data controller*** means, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- ***Data processor***, means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- ***Third Party*** means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority
- ***Profiling*** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- ***Recipient*** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
- ***Consent*** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- ***Genetic data*** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
- ***Biometric data*** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
- ***Cross Border Processing*** means processing of personal data which: -
    - takes place in more than one Member State; or
    - which substantially affects or is likely to affect data subjects in more than one Member State
- ***Representative*** means a natural or legal person established in the EU who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation.
- ***Supervisory Authority*** means an independent public authority established by a Member State
- ***Binding Corporate Rules*** means personal data protection policies which are adhered to by Aqqord for transfers of personal data to a controller or processor in one or more third countries or to an international organization

3. General Data Protection Regulation (GDPR)

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

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

Information protected under the GDPR is known as *"personal data"* and is defined as: -

"Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Aqqord ensures that even greater care and attention is given to personal data falling within the GDPR's ***'special categories'***, due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

In relation to the 'Special categories of Personal Data' the GDPR advises that: -

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

The GDPR regulates the processing of personal data, which includes organisation, altering, adapting, retrieving, consulting on, storing, using, disclosing, transmitting, disseminating or destroying any such data.

3.1. The GDPR Principles

Article 5 of the GDPR requires that personal data shall be: -

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

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

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ***('data minimization')***

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

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject

to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ***('storage limitation')***

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ***('integrity and confidentiality').***

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

3.2. Data Protection Commission

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

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

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

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

However, where an organisation is based in more than one Member State and/or where cross border processing takes place, a lead Supervisory Authority will enforce the GDPR requirements in consultation with any associated Supervisory Authority. Under the GDPR, the *'lead'* is determined by the location of the *'main establishment'*.

4. Objectives

We are committed to ensuring that all personal data obtained and processed by Aqqord is done so in accordance with the GDPR and its principles, along with any associated regulations and/or codes of conduct laid out by the Supervisory Authority and local law. We are dedicated to ensuring the safe, secure, ethical and transparent use of all personal data and to uphold the highest standards of data processing.

Aqqord uses the below objectives to meet the regulatory requirements of the GDPR and to develop measures, procedures and controls for maintaining and ensuring compliance.

Aqqord ensures that: -

- We protect the rights of individuals with regards to the personal information known and held about them by Aqqord in the course of our business.

- We develop, implement and maintain a data protection policy, procedure, audit plan and training program for compliance with the GDPR.
- Every business practice, task and process carried out by Aqqord, is monitored for compliance with the GDPR and its principles.
- Data is only obtained, processed or stored when we have met the lawfulness of processing requirements
- We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested.
- All employees (*including new starters and agents*) are competent and knowledgeable about their GDPR obligations and are provided with in-depth training in the GDPR principles, regulations and how they apply to our business and services.
- Customers feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the GDPR.
- We maintain a continuous program of monitoring, review and improvement with regards to compliance with the GDPR and to identify gaps and non-compliance before they become a risk.
- We monitor the Supervisory Authority, European Data Protection Board (EDPB) and GDPR news and updates, to stay abreast of updates, notifications and additional requirements.
- We have robust and recorded Complaint Handling and Breach Incident controls and procedures in place for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection.
- We have appointed a Compliance Officer who takes responsibility for the overall supervision and implementation of the GDPR and its principles and remains informed on the regulations and how they relate to Aqqord.
- We have a dedicated Audit & Monitoring Program in place to perform regular checks and assessments on how the personal data we process is obtained, used, stored and shared. The audit program utilises this policy and procedure and the GDPR itself to ensure continued compliance.
- We provide clear lines of reporting and supervision with regards to data protection compliance.
- Develop and maintain strict and robust DPA procedures, controls and measures to ensure continued compliance with the Act.
- We store and destroy all personal information, in accordance with the GDPR timeframes and requirements.
- Any information provided to an individual in relation to personal data held or used about them, with be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- Employees are aware of their own rights under the GDPR and are provided with the Article 13 & 14 information disclosures

4.1. Data Protection Officer / Compliance Officer

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

- The processing is carried out by a public authority or body *(except for courts acting in their judicial capacity)*
- the core activities of the controller/processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale

- the core activities of the controller/processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10

Aqqord have not appointed an official DPO at this time as we are not carrying out any 'large scale' capture/processing of special category data. This may change as the company grows and will be regularly re-evaluated.

Aqqord has nominated a GDPR compliance officer (Yaakov Smith) to ensure a central point of contact and to carry out some of the tasks which would be undertaken by the data protection officer if that role was mandated.

5. Governance Procedures

5.1. Accountability & Compliance

Due to the nature, scope, context and purposes of processing undertaken by Aqqord, we carry out frequent risk assessments and information audits to identify, assess, measure and monitor the impact of such processing. We have also implemented adequate and appropriate technical and organisational measures to ensure the safeguarding of personal data and compliance with the GDPR and any codes of conduct that we have obligations under.

We can demonstrate that all processing activities are performed in accordance with the GDPR and that we have in place robust policies, procedures, measures and controls for the protection of data. We operate a transparent workplace and work diligently to guarantee and promote a comprehensive and proportionate governance program.

Our main governance objectives are to: -

- Educate senior management and employees about the requirements under the GDPR and the possible impact of non-compliance
- Provide a dedicated and effective data protection training program for all staff
- Identify key senior stakeholders to support the data protection compliance program
- Allocate responsibility for data protection compliance and ensure that the designated person has sufficient access, support and budget to perform the role
- Identify, create and disseminate the reporting lines within the data protection governance structure

The technical and organisational measures that Aqqord has in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct, are detailed in this document and associated policies. These measures include: -

- Data Protection Policy
- Data Breach Policy & Procedures
- Subject Access Request Procedures
- Data Map – Record of Processing Activities
- Data Retention Policy & Register

Privacy by Design

We operate a *'Privacy by Design'* approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities. We therefore have

additional measures in place to adhere to this ethos, including: -

Data Minimisation

Under Article 5 of the GDPR, principle (c) advises that data should be *'limited to what is necessary'*, which forms the basis of our minimal approach. We only ever obtain, retain, process and share the data that is essential to carry out our services and legal obligations and we only keep if for as long as is necessary.

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

Measures to ensure that only the necessary data is collected includes: -

- Electronic collection *(i.e. forms, website, surveys etc*) only have the fields that are relevant to the purpose of collection and subsequent processing. We do not include 'optional' fields, as optional denotes that it is not necessary to obtain
- Physical collection *(i.e. face-to-face, telephone etc*) is supported using scripts and internal forms where the required data collection is ascertained using predefined fields. Again, only that which is relevant and necessary is collected
- We have SLA's and bespoke agreements in place with third-party controllers who send us personal information (*either in our capacity as a controller or processor).* These state that only relevant and necessary data is to be provided as it relates to the processing activity we are carrying out.
- We have documented destruction procedures in place where a data subject or third-party provides us with personal information that is surplus to requirement.

Pseudonymisation

We utilise pseudonymisation where possible to record and store personal data in a way that ensures data can no longer be attributed to a specific data subject without the use of separate additional information (*personal identifiers*). Encryption and partitioning is also used to protect the personal identifiers, which are always kept separate from the pseudonymised data sets.

When using pseudonymisation, we ensure that the attribute(s) being removed and replaced, are unique and prevent the data subject from being identified through the remaining markers and attributes. Pseudonymisation means that the data subject is still likely to be identified indirectly and as such, we use this technique in conjunction with other technical and operational measures of risk reduction and data protection.

Encryption

Although we class encryption as a form of pseudonymisation, we also utilise it as a secondary risk prevention measure for securing the personal data that we hold. Encryption with a secret key is used to make data indecipherable unless decryption of the dataset is carried out using the assigned key.

We utilise encryption via secret key for transferring personal data to any external party and provide the secret key in a separate format. Where special category information is being transferred and/or disclosed, the Compliance Officer is required to authorise the transfer and review the encryption method for compliance and accuracy.

Restriction

Our *Privacy by Design* approach means that we use company-wide restriction methods for all personal data activities. Restricting access is built into the foundation of Aqqord's processes, systems and structure and

ensures that only those with authorisation and/or a relevant purpose, have access to personal information. Special category data is restricted at all levels and can only be accessed by the Aqqord senior management.

Hard Copy Data

Where it is necessary to process personal data in paper format, we will utilise a tiered approach to minimise the information we hold and/or the length of time we hold it for. ***Steps include: -***

- In the first instance, we always ask the initial data controller to send copies of any personal information records directly to the data subject
- Where step 1 is not possible or feasible, we will obtain a copy of the data and if applicable redact to ensure that only the relevant information remains (*i.e. when the data is being passed to a third-party for processing and not directly to the data subject*)
- Recipients (*i.e. the data subject, third-party processer*) are reverified and their identity and contact details checked
- The Compliance Officer authorises the transfer
- Once confirmation has been obtained that the recipient has received the personal information, where possible *(within the legal guidelines and rules of the GDPR*), we destroy the hard copy data and delete the sent message
- If for any reason a copy of the paper data must be retained, we use a physical safe to store such documents as oppose to our standard archiving system

Data Map

To enable Aqqord to fully prepare for and comply with the GDPR, we have carried out a company-wide data protection data flow assessment to better enable us to record, categorise and protect the personal data that we hold and process.

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

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

5.2. Lawfulness of Processing

At the core of all personal information processing activities undertaken by Aqqord, is the assurance and verification that we are complying with Article 6 of the GDPR and our lawfulness of processing obligations. Prior to carrying out any processing activity on personal information, we always identify and establish the legal basis for doing so and verify these with the regulations.

This legal basis is documented on our data map and where applicable, is provided to the data subject and Supervisory Authority as part of our information disclosure obligations. ***Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where: -***

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

Records of Processing Activities

As an organisation with ***less than*** 250 employees, Aqqord maintains records of all processing activities where: -

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

Acting in the capacity as a processor (*or a representative*), our internal records of the categories of processing activities carried out on behalf of a controller, contain the following information: -

- The full name and contact details of the processor(s) and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the Compliance Officer
- The categories of processing carried out on behalf of each controller
- Where applicable, transfers of personal data to a third country or an international organisation *(including the identification of that third country or international organisation and where applicable, the documentation of suitable safeguards)*
- A general description of the processing security measures *(pursuant to Article 32(1) of the GDPR)*

5.3. Codes of Conduct & Certification Mechanisms

Aqqord adheres to the data protection codes of conduct prepared by Ireland's Data Protection Commission to demonstrate that we comply with the GDPR rules and principles. These codes and certification mechanism are approved by the Supervisory Authority and have been disseminated throughout the company to ensure competency and compliance from all staff.

The codes of conduct that we adhere to help us to: -

- Improve transparency and accountability
- Demonstrate to the public and Supervisory Authority that we meet the requirements of the data protection law and that we can be trusted with personal data
- Mitigate against enforcement action(s)
- Improve standards by establishing best practice
- Carry out fair and transparent processing
- Ensure appropriate safeguards within the framework of personal data transfers to third countries or international organisations

We submit to frequent and unscheduled monitoring and audits by the codes of conduct association/trade body and by the data protection certification scheme and understand that where we are deemed to be non-compliant in any area relating to the GDPR, we may lose our certification/seal of approval and/or the Supervisory Authority will be informed.

5.4. Third-Party Processors

Aqqord utilise external processors for certain processing activities. We use information audits to identify, categorise and record all personal data that is processed outside of the company, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible. ***Such external processing includes*** *(but is not limited to)****: -***

- IT Systems and Services
- Payment Services

We have strict due diligence and Know Your Customer procedures and measures in place and review, assess and background check all processors prior to forming a business relationship. We obtain company documents, certifications, references and ensure that the processor is adequate, appropriate and effective for the task we are employing them for.

We audit their processes and activities prior to contract and during the contract period to ensure compliance with the data protection regulations and review any codes of conduct that they are obligated under to confirm compliance. The continued protection of the rights of the data subjects is our priority when choosing a processor and we understand the importance of outsourcing processing activities as well as our continued obligations under the GDPR even when a process is handled by a third-party.

That contract or other legal act shall stipulate, in particular, that the processor: -

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

- Allows and supports audits, monitoring, inspections and reporting as set out in the contract
- Informs Aqqord immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract

5.5. Data Retention & Disposal

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

Please refer to our ***Data Retention Policy*** for full details on our retention, storage, periods and destruction processes.

6. Data Protection Impact Assessments (DPIA)

Individuals have an expectation that their privacy and confidentiality will be upheld and respected at all times whilst their data is being stored and processed by Aqqord. We therefore utilise several measures and tools to reduce risks and breaches for general processing, however when the processing is likely to be high risk or cause significant impact to a data subject, we utilise proportionate methods to map out and assess the impact ahead of time.

Where Aqqord must or are considering carrying out processing that utilises new technologies, where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, we always carry out a Data Protection Impact Assessments (DPIA) *(sometimes referred to as a Privacy Impact Assessment*).

Note: Aqqord does not deem it likely that there will be a need to process any high risk personal data as described below. As a data processor we do not have complete control over the data entered into our platform by our clients, but the nature of the contracts are unlikely to cover these areas.

Pursuant to Article 35(3) and Recitals 84, 89-96, we consider processing that is likely to result in a high risk to include: -

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person(s)
- Processing on a large scale of special categories of data
- Processing on a large scale of personal data relating to criminal convictions and offences
- Systematic monitoring of a publicly accessible area on a large scale (i.e. CCTV)
- Where a processing operation is likely to result in a high risk to the rights and freedoms of an individual
- Those involving the use of new technologies
- New processing activities not previously used
- Processing considerable amounts of personal data at regional, national or supranational level, which could affect many data subjects
- Processing activities making it difficult for the data subject(s) to exercise their rights

Carrying out DPIAs enables us to identify the most effective way to comply with our data protection obligations and ensure the highest level of data privacy when processing. It is part of our Privacy by Design approach an

allows us to assess the impact and risk before carrying out the processing, thus identifying and correcting issues at the source, reducing costs, breaches and risks.

The PIA enables us to identify possible privacy solutions and mitigating actions to address the risks and protection the privacy and impact. Solutions and suggestions are set out in the PIA and all risks are rated to assess their likelihood and impact. The aim of solutions and mitigating actions for all risks is to ensure that the risk is either: -

- Eliminated
- Reduced
- Accepted

7. Data Subject Rights Procedures

7.1. Consent & The Right to be Informed

The collection of personal data is a fundamental part of the products/services offered by Aqqord and we therefore have specific measures and controls in place to ensure that we comply with the conditions for consent under the GDPR.

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

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

- Consent requests are transparent, using plain language and is void of any illegible terms, jargon or extensive legal terms
- It is freely given, specific and informed, as well as being an unambiguous indication of the individual's wishes
- Consent is always given by a statement or a clear affirmative action (*positive opt-in*) which signifies agreement to the processing of personal data
- Consent mechanisms are upfront, clear, granular (*in fine detail*) and easy to use and understand
- Pre-ticked, opt-in boxes are **never** used
- Where consent is given as part of other matters (*i.e. terms & conditions, agreements, contracts*), we ensure that the consent is separate from the other matters and is **not** be a precondition of any service (*unless necessary for that service)*
- Along with our company name, we also provide details of any other third party who will use or rely on the consent
- Consent is always verifiable, and we have controls in place to ensure that we can demonstrate consent in every case
- We keep detailed records of consent and can evidence at a minimum: –
    - that the individual has consented to the use and processing of their personal data
    - that the individual has been advised of our company name and any third party using the data
    - what the individual was told at the time of consent
    - how and when consent was obtained

- We have ensured that withdrawing consent is as easy, clear and straightforward as giving it and is available through multiple options, including: -
    - Opt-out links in mailings or electronic communications
    - Opt-out process explanation and steps on website and in all written communications
    - Ability to opt-out verbally, in writing or by email
- Consent withdrawal requests are processed immediately and without detriment
- For special category data, the consent obtained is explicit *(stated clearly and in detail, leaving no room for confusion or doubt*) with the processing purpose(s) always being specified.

Consent Controls

Aqqord maintain rigid records of data subject consent for processing personal data and are always able to demonstrate that the data subject has consented to processing of his or her personal data where applicable. We also ensure that the withdrawal of consent is as clear, simple and transparent as it is to give consent.

Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent is presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. All such written declarations are reviewed and authorised by the Compliance Officer prior to being circulated.

The GDPR states that where processing is based on consent and the personal data relates to a child who is below the age of 16 years, such processing is only carried out by Aqqord, where consent has been obtained by the holder of parental responsibility over the child. EU states may have additional reductions on this such as the UK's Data Protection Bill which reduces this age to ***13 years***, as per Article 8(1) of the GDPR what advises that *"Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."*

Consent to obtain, process, store and share (*where applicable*), is obtained by Aqqord through: -

- Email
- Electronic *(i.e. via website form*)

Electronic consent is always a double opt-in, enabling the individual to provide consent after the below information has been provided. This is then followed up with an email, SMS or written confirmation of the consent to process, store and share the personal information. Privacy Notices are used in all forms of consent to ensure that we are compliant in disclosing the information required in the GDPR in an easy to read and accessible format.

Alternatives to Consent

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

When reviewing the processing activity for compliance with the consent requirements, we ensure that none of the below are a factor: –

- Where we ask for consent, but would still process it even if it was not given *(or withdrawn).* If we would still process the data under an alternative lawful basis regardless of consent, we recognise it is not the correct lawful basis to use

- Where we ask for consent to process personal data as a precondition of a service we are offering, it is not given as an option and consent is not appropriate
- Where there is an imbalance in the relationship, i.e. with employees

Information Provisions

Where personal data is obtained directly from the individual *(i.e. through consent, by employees, written materials and/or electronic formats (i.e. website forms, subscriptions, email etc)*), we provide the below information in all instances, in the form of a consent/privacy notice: -

- The identity and the contact details of the controller and, where applicable, of the controller's representative
- The contact details of our compliance officer
- The purpose(s) of the processing for which the personal information is intended
- The legal basis for the processing
- Where the processing is based on point (f) of Article 6(1) *"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party",* details of the legitimate interests
- The recipients or categories of recipients of the personal data *(if applicable)*
- If applicable, the fact that Aqqord intends to transfer the personal data to a third country or international organisation and the existence/absence of an adequacy decision by the Commission
    - where Aqqord intends to transfer the personal data to a third country or international organisation without an adequate decision by the Commission, reference to the appropriate or suitable safeguards Aqqord has put into place and the means by which to obtain a copy of them or where they have been made available
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- The existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- Where the processing is based on consent under points (a) of Article 6(1) or Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- The right to lodge a complaint with the Supervisory Authority
- Whether providing personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
- The existence of any automated decision-making, including profiling, as referred to in Article 22(1) and (4) and explanatory information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

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

Privacy Notices

Where Aqqord obtains personal data from a data subject or a third-party, we utilise Privacy Notices to provide the information pursuant to Articles 13 and 14 of the GDPR. Our privacy notice is easily accessible, legible, jargon-free and inclusive of all information and is available on our website.

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

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

7.2. Personal Data Not Obtained from the Data Subject

Where Aqqord obtains and/or processes personal data that has **not** been obtained directly from the data subject, Aqqord ensures that the information is provided to the data subject within 30 days of our obtaining the personal data *(except for advising if the personal data is a statutory or contractual requirement).*

In addition to the information provided to the data subject, we also provide information about: -

- The categories of personal data
- The source the personal data originated from and whether it came from publicly accessible sources

Where the personal data is to be used for communication with the data subject, or a disclosure to another recipient is envisaged, the information will be provided at the latest, at the time of the first communication or disclosure. Where Aqqord intends to further process any personal data for a purpose ***other*** than that for which it was originally obtained, we communicate this intention to the data subject prior doing so and where applicable, process only with their consent.

Whilst we follow best practice in the provision of the information, we reserve the right not to provide the data subject with the information if: -

- They already have it and we can evidence their prior receipt of the information
- The provision of such information proves impossible and/or would involve a disproportionate effort
- Obtaining or disclosure is expressly laid down by Union or Member State law to which Aqqord is subject and which provides appropriate measures to protect the data subject's legitimate interest
- Where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy

7.3. The Right of Access

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 *(collectively, The Rights of Data Subjects*), relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

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

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

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

Subject Access Request

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

- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom the personal data have been or will be disclosed
- If the data has or will be disclosed to a third countries or international organisations and the appropriate safeguards pursuant to the transfer
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- The right to lodge a complaint with a Supervisory Authority
- Where personal data has not been collected by Aqqord from the data subject, any available information as to the source and provider
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Subject Access Requests (SAR) are passed to the Compliance Officer as soon as received and a record of the request is noted. The type of personal data held about the individual is checked against our Information Audit to see what format it is held in, who else has it has been shared with and any specific timeframes for access.

SARs are always completed within 30-days and are provided free of charge. Where the individual makes the request by electronic means, we provide the information in a commonly used electronic format, unless an alternative format is requested.

Please refer to our external ***Subject Access Request Procedures*** for the guidelines on how an SAR can be made and what steps we take to ensure that access is provided under the GDPR.

7.4. Data Portability

Aqqord provides all personal information pertaining to the data subject, to them on request and in a format that is easy to disclose and read. We ensure that we comply with the data portability rights of individuals by ensuring that all personal data is readily available and is in a structured, commonly used and machine-readable format, enabling data subjects to obtain and reuse their personal data for their own purposes across different services.

To ensure that we comply with Article 20 of the GDPR concerning data portability, we keep a commonly used and machine-readable format of personal information where the processing is based on: -

- Consent pursuant to point (a) of Article 6(1)
- Consent pursuant to point (a) of Article 9(2)
- A contract pursuant to point (b) of Article 6(1); and
- the processing is carried out by automated means

Where requested by a data subject and if the criteria meet the above conditions, we will transmit the personal data directly from Aqqord to a designated controller, where technically feasible.

We utilise the below format for the machine-readable data: -

- CSV

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

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

7.5. Rectification & Erasure

Correcting Inaccurate or Incomplete Data

Pursuant to Article 5(d), all data held and processed by Aqqord is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data subject or controller inform us that the data we hold is inaccurate, we take every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

The Responsible Persons are notified of the data subjects request to update personal data and are responsible for validating the information and rectifying errors where they have been notified. The information is altered as directed by the data subject, with the information audit being checked to ensure that all data relating to the subject is updated where incomplete or inaccurate. Once updated, we add an addendum or supplementary statement where applicable.

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

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

The Right to Erasure

Also, known as *'The Right to be Forgotten'*, Aqqord complies fully with Article 5(e) and ensures that personal data which identifies a data subject, is not kept longer than is necessary for the purposes for which the personal data is processed. All personal data obtained and processed by Aqqord is categorised when assessed by the information audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

These measures enable us to comply with a data subjects right to erasure, whereby an individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing. Whilst our standard procedures already remove data that is no longer necessary, we still follow a dedicated

process for erasure requests to ensure that all rights are complied with and that no data has been retained for longer than is needed.

Where we receive a request to erase and/or remove personal information from a data subject, the below process is followed: -

1. The request is allocated to the Compliance Officer and recorded on the Erasure Request Register
2. The Compliance Officer locates all personal information relating to the data subject and reviews it to see if it is still being processed and is still necessary for the legal basis and purpose it was originally intended
3. The request is reviewed to ensure it complies with one or more of the grounds for erasure: -
    a. the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
    b. the data subject has withdrawn consent on which the processing is based and where there is no other legal ground for the processing
    c. the data subject objects to the processing and there are no overriding legitimate grounds for the processing
    d. the personal data has been unlawfully processed
    e. the personal data must be erased for compliance with a legal obligation
    f. the personal data has been collected in relation to the offer of information society services to a child
4. If the erasure request complies with one of the above grounds, it is erased within 30 days of the request being received
5. The Compliance Officer writes to the data subject and notifies them in writing that the right to erasure has been granted and provides details of the information erased and the date of erasure
6. Where Aqqord has made any of the personal data public and erasure is granted, we will take every reasonable step and measure to remove public references, links and copies of data and to contact related controllers and/or processors and inform them of the data subjects request to erase such personal data

If for any reason, we are unable to act in response to a request for erasure, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy. ***Such refusals to erase data include: -***

- Exercising the right of freedom of expression and information
- Compliance with a legal obligation for the performance of a task carried out in the public interest
- For reasons of public interest in the area of public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing
- For the establishment, exercise or defence of legal claims

7.6. The Right to Restrict Processing

There are certain circumstances where Aqqord restricts the processing of personal information, to validate, verify or comply with a legal requirement of a data subjects request. Restricted data is removed from the normal flow of information and is recorded as being restricted on the information audit. Any account and/or

system related to the data subject of restricted data is updated to notify users of the restriction category and reason. When data is restricted it is only stored and not processed in any way.

Aqqord will apply restrictions to data processing in the following circumstances: -

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

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

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

7.7. Objections and Automated Decision Making

Data subjects are informed of their right to object to processing in our Privacy Notices and at the point of first communication, in a clear and legible form and separate from other information. We provide opt-out options on all direct marketing material.

Individuals have the right to object to: -

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

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

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

Where we are processing personal information for direct marketing purposes under a previously obtained consent, we will stop processing such personal data immediately where an objection is received from the data subject. This measure is absolute, free of charge and is always adhered to.

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

We have carried out a system audit to identify automated decision-making processes that do not involve human intervention. We also assess new systems and technologies for this same component prior to implementation. Aqqord understands that decisions absent of human interactions can be biased towards individuals and pursuant to Articles 9 and 22 of the GDPR, we aim to put measures into place to safeguard individuals where appropriate. Via our Privacy Notices, in our first communications with an individual and on our website, we advise individuals of their rights not to be subject to a decision when: -

- It is based on automated processing
- It produces a legal effect or a similarly significant effect on the individual

In limited circumstances, Aqqord will use automated decision-making processes within the guidelines of the regulations. ***Such instances include: -***

- Where it is necessary for entering into or performance of a contract between us and the individual
- Where it is authorised by law *(e.g. fraud or tax evasion prevention)*
- When based on explicit consent to do so
- Where the decision does not have a legal or similarly significant effect on someone

Where Aqqord uses, automated decision-making processes, we always inform the individual and advise them of their rights. We also ensure that individuals can obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it.

8. Oversight Procedures

8.1. Security & Breach Management

Alongside our *'Privacy by Design'* approach to protecting data, we ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred.

We carry out information audits to ensure that all personal data held and processed by us is accounted for and recorded, alongside risk assessments as to the scope and impact a data breach could have on data subject(s). We have implemented adequate and appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

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

Please refer to our ***Data Breach Policy & Procedures*** for specific protocols.

8.2. Passwords

Passwords are a key part of Aqqord protection strategy and are used throughout the company to secure information and restrict access to systems. We use a multi-tiered approach which includes passwords at user, management, device, system and network levels to ensure a thorough and encompassing approach. Whilst passwords are also directly related to Information Security and Access Control, Aqqord recognises to strong, effective and robust password controls and measures are imperative to the protection and security of personal information.

Passwords afford a high level of protection to resources and data and are mandatory requirements for all employees and/or third-parties who are responsible for one or more account, system or have access to any resource that requires a password.

8.3. Restricted Access & Clear Desk Policy

Aqqord may on occasions and at its discretion, place all or part of its files onto a secure computer network with restricted access to all/some personnel data. When implemented, access to personal information will only be granted to the person/department that has a specific and legitimate purpose for accessing and using such information.

Aqqord operates a zero-tolerance Clear Desk Policy and does not permit personal data to be left unattended on desks or in meeting rooms, or in visible formats, such as unlocked computer screens or on fax machines, printers etc. Access to areas where personal information is stored (both electronic and physical) are on a restricted access basis with secure controlled access functions throughout the building. Only staff authorised to access data or secure areas can do so. All personal and confidential information in hard copy is stored safely and securely.

9. Transfers & Data Sharing

Aqqord takes proportionate and effective measures to protect personal data held and processed by us at all times, however we recognise the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred. Data transfers within Spain and the EU are deemed less of a risk than a third country or an international organisation, due to the GDPR covering the former and the strict regulations applicable to all EU Member States.

Where data is being transferred for a legal and necessary purpose, compliant with all Articles in the Regulation, we utilise a process that ensures such data is encrypted with a secret key and where possible is also subject to our data minimisation methods. We use approved, secure methods of transfer and have dedicated points of contact with each Member State organisation with whom we deal. All data being transferred is noted on our information audit so that tracking is easily available, and authorisation is accessible. The Compliance Officer authorises all EU transfers and verifies the encryption and security methods and measures.

We conduct transfers of personal data to third countries or international organisations where the Commission has advised that adequate levels of protections are in place. Such transfers are reviewed by the Compliance Officer and carried out following the same process as those within the EU. The Compliance Officer is responsible for monitoring the approved third country list provided by the Commission and only transferring data under this provision to those countries, organisations or sectors listed.

9.1. Appropriate Safeguards

In the absence of a decision by the Commission on an adequate level of protection by a third country or an international organisation, we restrict transfers to those that are legally binding or essential for the provision of our business obligations or in the best interests of the data subject. In such instances, we develop and implement appropriate measures and safeguards to protect the data, during transfer and for the duration it is processed and/or stored with the third country or international organisation.

Such measures include ensuring that the rights of data subjects can be carried out and enforced and that effective legal remedies for data subjects are available. ***The appropriate safeguards can be provided without Supervisory Authority authorisation by: -***

- A legally binding and enforceable instrument between public authorities or bodies
- Binding corporate rules
- Standard data protection clauses adopted by the Commission
- Standard data protection clauses adopted by a Supervisory Authority and approved by the Commission
- An approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regard data subjects' rights
- An approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regard data subjects' rights

With authorisation from the Supervisory Authority, the appropriate safeguards may also be provided for by: -

- Contractual clauses between Aqqord and the controller, processor or the recipient of the personal data in the third country or international organisation
- Provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights

Aqqord does not transfer personal data to any third country or international organisation without one or more of the above safeguards being in place or without the authorisation of the Supervisory Authority where applicable. We verify that any safeguards, adhere to the GDPR Principles, enforce the rights of the data subject and protect personal information in accordance with the Regulation.

Pursuant to Article 46, we ensure that any agreement, contract or binding corporate rules for transferring personal data to a third country or international organisation, are drafted in accordance with any Supervisory Authority and/or the Commission's specification for format and procedures (*where applicable*). ***As a minimum standard, we verify that the below are specified: -***

- The structure and contact details of the group engaged in the activity and of each of its members
- The data transfers or set of transfers, including: -
    - the categories of personal data
    - the type of processing and its purposes
    - the type of data subjects affected
- the identification of the third country or countries in question
- Their legally binding nature, both internally and externally
- The application of the general data protection principles, in particular: -
    - purpose limitation
    - data minimisation
    - limited storage periods
    - data quality
    - data protection by design and by default
    - legal basis for processing
    - processing of special categories of personal data
    - measures to ensure data security

- the requirements in respect of onward transfers to bodies not bound by the binding corporate rules

- The rights of data subjects regarding processing and the means to exercise those rights, including the right: -
  - not to be subject to decisions based solely on automated processing (*inc profiling*)
  - to lodge a complaint with the competent Supervisory Authority and before the competent courts of the Member States
  - to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules
- Our acceptance (*and that of any processor acting on our behalf*) of liability for any breaches of the binding corporate rules by the third country or international organisation to whom the data is being transferred (*with exemption from that liability, in whole or in part, only where we prove that we are not responsible for the event giving rise to the damage*)
- How the information on the binding corporate rules and the information disclosures (Articles 13 & 14) is provided to the data subjects *(with particular reference to the application of the GDPR Principles, the data subjects rights and breach liability*)
- The tasks of any Compliance Officer and/or person(s) in charge of monitoring compliance with the binding corporate rules, as well as monitoring training and complaint-handling
- The complaint procedures
- The mechanisms within the group engaged in the activity, for ensuring the verification of compliance with the binding corporate rules, including: -
  - data protection audits
  - methods for ensuring corrective actions to protect the rights of the data subject
  - providing the Compliance Officer and controlling board with such verification results
- The mechanisms for reporting and recording changes to the rules and reporting those changes to the Supervisory Authority
- The cooperation mechanism with the Supervisory Authority to ensure compliance by any member of the group, in particular by making available to the Supervisory Authority, the results of verifications of the measures referred to above
- The mechanisms for reporting to the competent Supervisory Authority any legal requirements to which a member of the group is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules
- The appropriate data protection training to personnel having permanent or regular access to personal data

9.2. Transfer Exceptions

Aqqord do not transfer any personal information to a third country or international organisation without an adequacy decision by the Commission or with Supervisory Authority authorisation and the appropriate safeguarding measures; unless one of the below conditions applies. ***The transfer is: -***

- made with the explicit consent of the data subject, after having been informed of the possible risks and the absence of an adequacy decision and appropriate safeguards
- necessary for the performance of a contract between the data subject and Aqqord or the implementation of pre-contractual measures taken at the data subject's request
- necessary for the conclusion or performance of a contract concluded in the interest of the data subject between Aqqord and another natural or legal person
- necessary for important reasons of public interest
- necessary for the establishment, exercise or defence of legal claims
- necessary in order to protect the vital interests of the data subject or of other persons, where the data

subject is physically or legally incapable of giving consent

- made from a register which under UK or EU law is intended to provide information to the public (*and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register*). Transfer made under this exception must not involve the entire personal data or categories of the personal data in the register and if the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

Where a transfer is not valid under Article 45 or 46 and none of the above derogations apply, Aqqord complies with the Article 49 provision that a transfer can still be affected to a third country or an international organisation where all the below conditions apply. ***The transfer: -***

- cannot be made by a public authority in the exercise of its public powers
- is not repetitive
- concerns only a limited number of data subjects
- is necessary for the purposes of compelling legitimate interests pursued by Aqqord which are not overridden by the interests or rights and freedoms of the data subject
- Aqqord has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment, provided suitable safeguards with regard to the protection of personal data

Where the above transfer must take place for legal and/or compelling legitimate reasons, the Supervisory Authority is notified of the transfer and the safeguards in place, prior to it taking place. The data subject in such instances is provided with all information disclosures pursuant to Articles 13 and 14, as well as being informed of the transfer, the compelling legitimate interests pursued and the safeguards utilised to affect the transfer.

10. Audits & Monitoring

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

The Compliance Officer has overall responsibility for assessing, testing, reviewing and improving the processes, measures and controls in place and reporting improvement action plans to the Senior Management Team where applicable. Data minimisation methods are frequently reviewed and new technologies assessed to ensure that we are protecting data and individuals to the best of our ability.

All reviews, audits and ongoing monitoring processes are recorded by the Compliance Officer and copies provided to Senior Management and are made readily available to the Supervisory Authority where requested.

The aim of internal data protection audits is to: -

- Ensure that the appropriate policies and procedures are in place
- To verify that those policies and procedures are being followed
- To test the adequacy and effectiveness of the measures and controls in place
- To detect breaches or potential breaches of compliance
- To identify risks and assess the mitigating actions in place to minimise such risks
- To recommend solutions and actions plans to Senior Management for improvements in protecting data

subjects and safeguarding their personal data

- To monitor compliance with the GDPR and demonstrate best practice

11. Training

Through our strong commitment and robust controls, we ensure that all staff understand, have access to and can easily interpret the GDPR requirements and its Principles and that they have ongoing training, support and assessments to ensure and demonstrate their knowledge, competence and adequacy for the role. New and existing employees are trained, assessed and supported and include: -

- GDPR Workshops & Training Sessions
- Coaching & Mentoring
- Access to GDPR policies, procedures, checklists and supporting documents

Employees are continually supported and trained in the GDPR requirements and out own objectives and obligations around data protection.

12. Penalties

Aqqord understands our obligations and responsibilities under the GDPR and Supervisory Authority and comprehend the severity of any breaches under the Regulation. We respect the Supervisory Authority's authorisation under the legislation to impose and enforce fines and penalties on us where we breach the regulations, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

Employees have been made aware of the severity of such penalties and their proportionate nature in accordance with the breach. ***We recognise that: -***

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

13. Responsibilities

Aqqord have appointed a Compliance Officer whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up-to-date with all legislation and changes relating to data protection. The Compliance Officer will work in conjunction with the IT Manager and Training Officer to ensure that all processes, systems and staff are operating compliantly and within the requirements of the GDPR and its principles.

The Compliance Officer has overall responsibility for due diligence, privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the GDPR and our own internal objectives and obligations.

Staff who manage and process personal or special category information will be provided with data protection training and will be subject to continuous development support and mentoring to ensure that they are competent and knowledge for the role they undertake.

SUBJECT ACCESS REQUEST PROCEDURES

Contents

Introduction

This procedure document supplements the subject access request (SAR) provisions set out in Aqqord's Data Protection Policy document and provides the process for individuals to use when making a Subject Access Request and the protocols followed by Aqqord when a Subject Access Request is received.

Aqqord needs to collect personal information to effectively and compliantly carry out our everyday business functions and services and in some circumstances, to comply with the requirements of the law and/or regulations.

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

The General Data Protection Regulation

The General Data Protection Regulation (GDPR) gives individuals the right to know what information is held about them, to access this information and to exercise other rights, including the rectification of inaccurate data. The GDPR is a standardised regulatory framework which ensures that personal information is obtained, handled and disposed of properly.

As Aqqord are obligated under the GDPR and UK data protection laws, we abide by the Regulations principles, ***which ensure that personal information shall be: -***

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

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ***('purpose limitation')***

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

d) 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, are erased or rectified without delay ***('accuracy')***

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ***('storage limitation')***

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ***('integrity and confidentiality').***

The Regulation also requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the GDPR principles'* ***('accountability')***. Aqqord have adequate and effective measures, controls and procedures that protect and secure your personal information at all times and guarantee that it is only ever obtained, processed and disclosed in accordance with the GDPR.

What is Personal Information?

Information protected under the GDPR is known as *"personal data"* and is defined as: -

"Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Further information on what constitutes personal information and your rights under the data protection regulation and laws can be found on the Information Commissioner's Office (ICO) **website**.

The Right of Access

Under Article 15 of the GDPR, an individual has the right to obtain from the controller, confirmation as to whether or not personal data concerning them is being processed. We are committed to upholding the rights of individuals and have dedicated processes in place for providing access to personal information. ***Where requested, we will provide the following information: -***

- the purposes of the processing
- the categories of personal data concerned
- the recipients or categories of recipient to whom the personal data have been or will be disclosed
- If the data has been transferred to a third country or international organisations (*and if so, the appropriate safeguards used)*
- the envisaged period for which the personal data will be stored (*or the criteria used to determine that period)*
- where the personal data was not collected directly from the individual, any available information as to their source

How To Make a Subject Access Request (SAR)?

A subject access request (SAR) is a request for access to the personal information that Aqqord holds about an individual, which we are required to provide under the GDPR *(unless an exemption applies*).

You can make this request in writing using the details provided in the 'Submission & Lodging a Complaint' section of this document, or you can submit your access request electronically. Where a request is received by electronic means, we will provide the requested information in a commonly used electronic form *(unless otherwise requested by the data subject).*

What We Do When We Receive An SAR

Identity Verification

Subject Access Requests (SAR) are passed to the Compliance Officer as soon as received and a record of the request is noted. The person in charge will use all reasonable measures to verify the identity of the individual making the access request, especially where the request is made using online services.

We will utilise the request information to ensure that we can verify your identity and where we are unable to do so, we may contact you to provide evidence of your identity prior to actioning any request. This is to protect your information and rights.

If a third party, relative or representative is requesting the information on your behalf, we will verify their authority to act on your behalf and may again contact you to confirm their identity and authorisation prior to acting the subject access request.

Information Gathering

If you have provided enough information in your SAR to collate the personal information held about you, we will gather all forms (*hard-copy, electronic etc*) and ensure that the information required is provided in an acceptable format. If we do not have enough information to locate your records, we may contact you for further details. This will be done as soon as possible and within the Regulation timeframes set out below.

Information Provision

Once we have collated all of the personal information held about you, we will send this to you in writing (*or in a commonly used electronic form if requested*). The information will be in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Fees and Timeframes

SARs are always completed within 30-days and are provided free of charge. Where the request is made by electronic means, we provide the information in a commonly used electronic format, unless an alternative format is requested.

Whilst we provide the information requested without a fee, further copies requested by the individual may incur a charge to cover administrative costs.

Aqqord always aims to provide the requested information at the earliest convenience, but at a maximum, 30 days from the date the request was received. However, where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months. If this is the case, we will write to you within 30 days and keep you informed of the delay and the reasons.

Your Other Rights

Under the GDPR, you have the right to request rectification of any inaccurate data held by us. Where we are notified of an inaccuracy and agree that the data is incorrect, we will amend the details immediately as directed by you and make a note on the system (or record) of the change and reasons.
We will rectify the errors within 30-days and inform you in writing of the correction and where applicable, provide the details of any third-party to whom the data has been disclosed.

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

Individuals also have the right to request from Aqqord, the erasure of personal data or to restriction the processing of personal data where it concerns the data subject; as well as the right to object to such processing. You can use the contact details in the 'Submission & Lodging a Complaint' section to make such requests.

Automated Decision-Making

Aqqord does not utilise any automated decision-making or profiling of personal data.

Exemptions and Refusals

The GDPR contains certain exemptions from the provision of personal information. If one or more of these exemptions applies to your subject access request or where Aqqord does not act on the request, we shall inform you at the earliest convenience, or at the latest, within one month of receipt of the request.

Where possible, we will provide you with the reasons for not acting and any possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy. Details of contacting the supervisory authority are set out below.

Submission & Lodging a Complaint

To submit your SAR, you can contact us at admin@aqqord.com

If you are unsatisfied with our actions, wish to make an internal complaint, or wish to submit your SAR in writing, please write to us at this address: -

Aqqord Limited
4 Leicester Avenue
Salford
United Kingdom
M7 4HA

Supervisory Authority

If you remain dissatisfied with our actions, you have the right to lodge a complaint with the Supervisory Authority. ***The Information Commissioner's Office (ICO) can be contacted at: -***

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Website: https://ico.org.uk/