Title	Data Protection and Privacy Policy
Process Owner	Data Protection Office
Date Created	18/03/2021
Publish Date	23/07/2021
Approved By	Senior Management
Summary	Policy detailing the requirements for the organisation with regards to the Data Protection Act.
Classification	Public
Standard	All
Version	1.2

Change Record
Enter any changes to the document within the tag below…
Copied from v1.6 17/12/2020 Data Protection & Privacy Policy & Procedure
Overwrite the content of the tag, this will create each change you have made to the document and record it in ISOportal

Contents

1 Policy Statement

Rullion Ltd 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, Contractors, Temporary workers, customers, suppliers and clients and includes *(but is not limited to),* name, address, email address, data of birth, IP address, identification numbers, private and confidential information, sensitive information and bank details.

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

Rullion Ltd 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 and/or special category data belonging to the individuals with whom we deal is paramount to our company ethos and Rullion Ltd 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 Rullion Ltd is meeting its legal, statutory and regulatory requirements under the GDPR and to ensure that all personal and special category 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 data safe within our organisation.

The GDPR includes provisions that promote accountability and governance and as such Rullion Ltd 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.

3 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 Rullion Ltd 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.

4 Definitions

- ***GDPR*** means the General Data Protection Regulation and for the purposes of this document, the acronym is also used to collectively describe all the data protection laws that Rullion Ltd 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.
- ***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 which is established by a Member State

- ***Binding Corporate Rules*** means personal data protection policies which are adhered to by Rullion Ltd for transfers of personal data to a controller or processor in one or more third countries or to an international organisation

5 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 Rullion Ltd 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."

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

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

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

The GDPR regulates the processing of personal data, which includes organisation, altering, adapting, retrieving, consulting on, storing, using, disclosing, transmitting, disseminating or destroying any such data. As Rullion Ltd uses personal data in one or more of the above capacities, we have put into place robust measures, policies, procedures and controls concerning all aspects of personal data handling.

6 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 minimisation')***

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 unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ***('integrity and confidentiality').***

Article 5(2) requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the 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.

7 Controller and Processor Objectives

We are committed to ensuring that all personal data obtained and processed by Rullion Ltd is done so in accordance with the GDPR and its principles, along with any associated regulations and/or codes of conduct laid down 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.

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

Rullion Ltd ensures that: -

- We protect the rights of individuals with regards to the personal information known and held about them by Rullion Ltd 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 Rullion Ltd, 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 only process special category data in accordance with the GDPR regulations.
- All employees (*including new starters and agents*) are competent and knowledgeable about their GDPR obligations and are provided with 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 ***Data Protection Office*** 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 Rullion Ltd
- We have a 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
- Governance Procedures

8 Accountability & Compliance

Due to the nature, scope, context and purposes of processing undertaken by Rullion Ltd, we carry out 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 Rullion Ltd 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 (GDPR) Privacy Policy & Procedure
- Data Retention Policy
- Data Breach Policy
- HR Policy
- Staff Training & Development Procedures
- Internal Audits & Monitoring Policy & Procedures
- Information Security Policy & Procedures
- Outsourcing Policy & Due Diligence Procedures
- Clear Desk Policy
- Remote Access Policy
- Record Processing Activities
- Information Audit & Personal Data Register
- Appointed Data Protection Officer
- Business Continuity Plan & Daily Data Backups

9 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.
- Physical collection *(i.e. face-to-face, telephone etc*) is supported using internal forms where the required data collection is ascertained using predefined fields. Again, only that which is relevant and necessary is collected
- We have SLAs 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.

Encryption

Although we class encryption as a form of pseudonymisation, we also utilise it as a 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 separately.

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 Rullion Ltd's processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose, have access to personal information. designated personnel.

Hard Copy Data

Due to the nature of our business, it is sometimes essential for us to obtain, process and share personal and special category information which is only available in a paper format without pseudonymisation options (*i.e. copies of pay records, P45s or claims information*). Where this is necessary, we utilise a tiered approach to minimise the information we hold and/or the length of time we hold it for. ***Steps include: -***

- 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*)

- Once redacted and there is a requirement to hold a copy of the data to meet our legal obligations, a copy will be stored electronically, and the original destroyed.
- If for any reason a copy of the paper data must be retained by Rullion Ltd, we use a physical safe to store such documents as oppose to our standard archiving system

10 Information Flow Audit

To enable Rullion Ltd to fully prepare for and comply with the GDPR, we have carried out a company-wide data protection information 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/processor and has been compiled on a central register which includes: -

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

11 Legal Basis for Processing *(Lawfulness)*

At the core of all personal information processing activities undertaken by Rullion Ltd, 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 information flow register 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: -***

- Processing is necessary for the purposes of the legitimate interests pursued by Rullion Ltd 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).*
- 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
- The data subject has given consent to the processing of their personal data for one or more specific purposes
- 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 Rullion Ltd

12 Processing Special Category Data

Special categories of Personal Data is defined in the GDPR as: -

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.

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

We will only ever process special category data where: -

- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim
- The data subject has given explicit consent to the processing of the personal data
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

Schedule 1, Parts 1, 2 & 3 of The Data Protection Bill provide specific conditions and circumstances when special category personal data can be processed and dictated the requirements that organisations are obligated to meet when processing such data.

Where Rullion Ltd processes personal data that falls into one of the above categories, we have the specified provisions and measures in place prior to any processing. ***Measures include: -***

- Verifying our reliance on one of the GDPR Article 9(1), and where applicable The Data Protection Bill Sch.1, Pt.1, Pt.2 and/or Pt.3 conditions prior to processing
- Having an appropriate policy document in place when the processing is carried out, specifying our: -
    - procedures for securing compliance with the GDPR principles
    - policies as regards the retention and erasure of personal data processed in reliance on the condition
    - retention periods and reason *(i.e. legal, statutory etc)*

- procedures for reviewing and updating our policies in this area

Please refer to our Retention & Erasure Policy for further guidance and procedures.

13 Records of Processing Activities

As an organisation with ***approx*** 200 employees, Rullion Ltd maintains records of all processing activities and maintains such records in writing, in a clear and easy to read format and readily available to the Supervisory Authority upon request.

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

- Our full name and contact details and the name and contact details of the Data Protection Office. Where applicable, we also record any joint controller and/or the controller's representative
- The purposes of the processing
- A description of the categories of data subjects and of the categories of personal data
- The categories of recipients to whom the personal data has or will be disclosed *(including any recipients in third countries or international organisations)*
- 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)*
- Where possible, the envisaged time limits for erasure of the different categories of data

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 data protection 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 as outlined in section 13 of this document *(pursuant to Article 32(1) of the GDPR)*

As part of our obligations under the UK's Data Protection Bill, Sch.1, Pt.4, where we are required to maintain a record of our processing activities in our capacity as a controller and are processing special category or criminal conviction data, as specified in Sch.1, Pt.1-3 of the Bill, ***we also record the below information on the register: -***

- Which condition is relied on?
- How the processing satisfies Article 6 of the GDPR (lawfulness of processing)

Whether the personal data is retained and erased in accordance with the policies described in

paragraph 30(b) of the DP Bill (and if not, the reasons for not following those policies).

14 Third-Party Processors

Rullion Ltd utilises 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
- Legal Services
- Debt Collection Services
- Credit Reference Agencies
- Payroll Services Agencies
- Direct Marketing 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.

Where appropriate, 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.

We draft bespoke Service Level Agreements (SLAs) and contracts with each processor and among other details, outlines: -

- The processors data protection obligations
- Our expectations, rights and obligations
- The processing duration, aims and objectives
- The data subjects' rights and safeguarding measures
- The nature and purpose of the processing
- The type of personal data and categories of data subjects

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

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 Rullion Ltd 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 Rullion Ltd after the end of the provision of services relating to processing, and deletes existing copies where possible
- Makes available to Rullion Ltd, 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 Rullion Ltd immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract

15 Data Retention & Disposal

Rullion Ltd has 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 prioritises the protection of the personal data at all times.

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

16 Data Protection Impact Assessments (DPIA)

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by Rullion Ltd. 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 Rullion Ltd must, or are considering carrying out processing that utilises new technologies, and/or where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, we always carry out a Data Protection Impact Assessment (DPIA) *(sometimes referred to as a Privacy Impact Assessment*).

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
- 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 and 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 DPIA enables us to identify possible privacy solutions and mitigating actions to address the risks and reduce the impact. Solutions and suggestions are set out in the DPIA 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

17 Data Protection Impact Assessment Process (DPIA)

A lead is always appointed to carry out the DPIA, follow the process, record the necessary information and report the results to the Senior Management Team. All DPIAs are carried out in conjunction with the Data Protection Office who provides advice and support for the compliance of the processes with the GDPR rules.

The DPIA lead ascertains if an assessment is required by assessing the answers to the below questions. Where one or more questions result in a ***'yes'*** answer, the assessment is carried out.

Screening questions include: -

- Does the processing require systematic and/or extensive evaluation *(via automated means*) of personal aspects an individual(s)?
- Will decisions be based on such evaluations that are likely to produce legal effects concerning the individual(s)?

- Is the processing on a large scale and involves special categories of data?
- Is the processing on a large scale and involves data relating to criminal convictions and offences?
- Does the processing involve systematic monitoring of a publicly accessible area on a large scale? (*i.e. CCTV*)
- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Is the information about individuals likely to raise high risk privacy concerns or expectations?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information or a third-party without adequate safeguards in place?
- Does the processing involve the use of new technology or systems which might be perceived as being privacy intrusive?
- Could the processing result in decisions being made or action being taking against individual(s), in ways that could have a significant impact on them?
- Will the project require you to contact individuals in ways which they may find intrusive?

The DPIA is carried out using our predefined document and each stage is recorded to demonstrate compliance and to show that all high-risk processing activities have been assessed prior to being operational. DPIAs are retained for 6 years from the date they were first carried out and are readily available for the Supervisory Authority upon request.

The DPIA includes: -

1. The aims and objectives of the DPIA
2. The scope of the DPIA (*if covering more than one processing activity*)
3. Clarify the legal basis for processing
4. Which activity/high risk reason is the DPIA required for *(i.e. which of the initial screening questions above have been identified)*
5. A description of the processing operations
6. The purpose(s) of the processing and where applicable, the legitimate interests pursued by the controller
7. An assessment of the necessity and proportionality of the processing in relation to the purpose
8. An assessment of the risks to individuals (*including possible intrusions on privacy where appropriate)*
9. Assess the corporate risks (*including regulatory action, non-compliance, reputational*

damage, loss of public trust etc)

10. Conduct a compliance check against the GDPR, relevant legislation and any Codes of Conduct
11. Maintain a record of the identified risks
12. Where appropriate, we seek the views of data subject(s) or their representatives on the intended processing
13. The measures in place to address, reduce or remove the risk (*i.e. security, proposed solutions, mitigating actions etc)*
14. Data flow – what the information is, where it is coming from, who it is going to
15. Authorisation from the DPO and sign off by Senior Management
16. Record all PIA outcomes & add risk rating & next action

18 Data Subject Rights Procedures

19 Legal Reason for processing

The collection of personal and sometimes special category data is a fundamental part of the products/services offered by Rullion Ltd and we therefore have specific measures and controls in place to ensure that we comply with the Legal Reasons for Processing under the GDPR.

Rullion, a Data Controller, will rely on **legitimate interests'** as the initial reason for holding and processing data to introduce candidates to clients and vice versa. In addition where processing is necessary for **compliance with a legal obligation** eg the Conduct of Employment Agencies and Employment Business Regulations 2003 and **Purposes of a contract** is relied upon when a perm or contract placement is made.

Where processing is based on legitimate interests', Rullion Ltd has reviewed and carried out a legitimate interest assessment to review the necessity of the processing of data and the balance of interests between all parties.

	Task	Record Findings
1	Define the purposes of processing this data:	• The core function of the Rullion business is recruitment and therefore is reliant upon candidates providing their personal information relevant to job opportunities.
2	Identify whether one or more specific business objectives relies upon the processing of this data	• The core function of the Rullion business relies on candidates providing their details for Consultants to assess for relevant opportunities. Rullion will then use their data to match a candidate's experience & skill-set to a job role requirement from our clients.

	Task	Record Findings
3	Identify one or more specific business objective of any third party which relies on the processing of the data	• The candidate's objective is to identify their next opportunity. • The client's objective is to secure the correct talent into their organisation for that role. • Rullion's objective is to facilitate and manage the introduction of key talent to organisations. • HMRC and other legal obligations dictate that, when requested, Rullion must be able to provide details regarding an individual's pay, internally or externally. • Individual contractors require remuneration for the work completed and therefore must provide payment details to Rullion to include their own personal bank details, Limited Company Bank Details or those of an Umbrella organisation.
4	Explain if processing is specifically identified as legitimate by GDPR, PECR or other applicable law	• GDPR states that processing is lawful when it is necessary for the purposes of legitimate interests pursued by the controller (Rullion) or by a third party (Candidate and client). The data processing completed by Rullion follows a standard and expected recruitment process and therefore provides a balanced interest and benefit across all parties involved. • Rullion complies with the Employment Conduct Regulations, as well as other legal obligations, that identify our Ways or Working and ensure we follow such processes as obtaining Right to Representation prior to presenting a candidate to a client.

- We have ensured that withdrawing consent to process data is easy, clear and straightforward 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 with the processing purpose(s) always being specified

20 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 data protection office
- 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 Rullion Ltd 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 Rullion Ltd 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 Rullion Ltd 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 or available 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.

21 Privacy Policy & Notices

22 Privacy Policy

Rullion Ltd recognises the difference between a Privacy Policy and a Privacy *Notice (or statement)* and ensures that we meet the regulatory, legal and best practice requirements for both formats. For the purposes of this document, we use the term Privacy Policy to provide the business, its staff and any associated entities with our operational and organisational approach to protecting data and complying with the General Data Protection Regulation (GDPR) and any relevant data protection laws.

This document is our Data Protection & Privacy Policy and includes how we comply with the GDPR principles, the manner in which we process data, guidelines and procedures for ensuring that data subjects can exercise their rights and our approach to data protection by design and default. This policy provides detail on how we apply the principles, what procedures we follow in the compliance with the Regulation and any specific individual and/or departmental responsibilities, including those of the Data Protection Office (DPO) and is fundamentally used as an internal reference document.

We have a user-friendly version of our Privacy Policy on our website, which also includes details about the cookies used on the site. The Privacy Policy on the site is in an easy to see and accessible place and is in addition to our legally required Privacy Notice; more details of which are noted below.

23 Privacy Notice

Our Privacy Notice is separate from our Data Protection & Privacy Policy and is available to individuals at the time we collect their personal *data (or at the earliest possibility where that data is obtained indirectly)*. Our Privacy Notice includes the Article 13 & 14 requirements as set out in the GDPR and provides individuals with all the necessary and legal information about how, why and when we process their data, along with their rights and obligations.

Our Privacy Notice is designed to be a public declaration of how Rullion Ltd applies the data protection principles to data that we process. It is provided to all individuals whose data we process and contains only the information specific to the individual and as required by law. The notice is easily accessible, legible, jargon-free and is available in several formats, dependant on the method of data collection: -

- Via our website
- Worded in full in agreements, contracts, forms and other materials where data is collected in writing or face-to-face
- In employee contracts and recruitment materials
- Via SMS
- Digital Products/Services
- On Mobile Apps

With lengthy content being provided in the privacy notice, we have tested, assessed and reviewed our privacy notice to ensure usability, effectiveness and understanding. Privacy Notices are drafted by the Data Protection Office using the GDPR requirements and with Supervisory Authority guidance.

❖ ***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

24 Employee Personal Data

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

All employees are provided with our Staff Handbook which informs them of their rights under the GDPR and how to exercise these rights.

25 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 is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

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

26 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 Rullion Ltd 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 Data Protection Office 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.

27 Data Portability

Rullion Ltd 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 Rullion Ltd to a designated controller, where technically feasible.

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

- HTML
- CSV
- XML
- RDF
- XHTML

- 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.

28 Rectification & Erasure

29 Correcting Inaccurate or Incomplete Data

- Pursuant to Article 5(d), all data held and processed by Rullion Ltd 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 Data Protection Office is 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.

30 The Right to Erasure

- Also, known as *'The Right to be Forgotten'*, Rullion Ltd 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 Rullion Ltd 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.

31 The Right to Restrict Processing

- There are certain circumstances where Rullion Ltd 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.

- ***Rullion Ltd 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 Data Protection Office reviews and authorizes 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 nd to a judicial remedy.

32 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 and provide an online objection form where processing is carried out online. ***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 Rullion Ltd 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, Rullion Ltd 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. Rullion Ltd 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, Rullion Ltd 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 Rullion Ltd 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.

33 Oversight Procedures

34 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. Our ***Information Security Policy & Procedures*** provide the detailed measures and controls that we take to protect personal information and to ensure its security from consent to disposal.

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 are taken to reduce the risk of data breaches, Rullion Ltd 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.

35 Passwords

Passwords are a key part of Rullion Ltd's 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, Rullion Ltd 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. Full procedures and guidelines for passwords, access and security can be found in our ***Information Security Program***.

36 Restricted Access & Clear Desk Policy

Rullion Ltd 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.

Rullion Ltd 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.

37 Transfers & Data Sharing

Rullion Ltd 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 the UK and 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 Data Protection Office 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 DPO and carried out following the same process as those within the EU. The DPO 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.

38 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 Rullion Ltd 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

Rullion Ltd 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 Data Protection 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 Data Protection 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

39 Transfer Exceptions

Rullion Ltd does 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 Rullion Ltd 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 Rullion Ltd 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 applies, Rullion Ltd 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 Rullion Ltd which are not overridden by the interests or rights and freedoms of the data subject
- Rullion Ltd 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.

40 Audits & Monitoring

This policy and procedure document details the extensive controls, measures and methods used by Rullion Ltd 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 that are detailed in our ***Compliance Monitoring & Audit Policy & Procedure***, 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 Data Protection Office 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 Data Protection Office 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

41 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. Our ***Training & Development Procedures*** detail how new and existing employees are trained, assessed and supported and include: -

- GDPR Training Sessions
- Assessment Tests
- Coaching & Mentoring
- 1:1 Support Sessions
- Scripts and Reminder Aids
- Access to GDPR policies, procedures, checklists and supporting documents

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

42 Penalties

Rullion Ltd understands our obligations and responsibilities under the GDPR and Supervisory Authority and comprehends 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.

43 Responsibilities

Rullion Ltd has appointed a Data Protection Office 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 DPO will work in conjunction with the IT Manager, Head of HR & Talent and Quality Lead to ensure that all processes, systems and staff are operating compliantly and within the requirements of the GDPR and its principles.

The DPO 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 extensive 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.

Corporate Adherence Clause

The Company considers that all Rullion policies and procedures provide our employees with the company's expectations in respect of our code of conduct. As such, should an employee disregard or wilfully ignore the terms of a policy or contravene the approved process, disciplinary action may be taken against them, which can be up to and including dismissal should a serious breach take place. Disciplinary action may be taken against any individual or group of employees where the contravention of a Company policy occurs.