Tourmaline Europe, LLP
(the "**Firm**")

General Data Protection Policies in compliance with the General Data Protection Regulation ("**GDPR**")

.

CONTENT

1. INTRODUCTION

1.1 The GDPR Overview

The General Data Protection Regulation ("EU GDPR") replaces the Data Protection Directive 95/46/EC; it was designed to harmonise Data privacy laws across the European Union ("EU") but also to protect the privacy of EU citizens and to reshape the way organisations across the region approach Data privacy. The GDPR becomes enforceable on 25 May 2018.

GDPR was onshored in the United Kingdom and adopted as retained EU law by way of the European Union (Withdrawal Agreement) Act 2020 and later merged with the existing Data Protection Act 2018 (as amended) (the "Act") to form the "**UK GDPR**". As a result of the United Kingdom leaving the European Union, UK GDPR operates as its standalone data privacy regime alongside the EU GDPR (as amended).

The UK GDPR applies to organisations located within the UK but also to organisations located outside of the UK if they offer goods or services to or monitor the behaviour of UK residents. It applies to all companies processing any Personal Data of Data Subjects residing in the UK, regardless of the company's location. Compliance and monitoring processes but also providing evidence of compliance (including training our staff on privacy laws and requirements to ensure that all employees are fully aware and trained on Data protection requirements as may be applicable to their roles) are the key elements of any potential future defence and they both demand some adjustments within our organisation.

Organisations can be fined up to 4% of their annual global turnover for breaching the UK GDPR or GBP 17.5m, whichever is greater. This is the maximum fine that can be imposed for the most serious infringements (e.g., not having sufficient customer consent to process Data or violating the core of Privacy by Design concepts). There is a tiered approach to fines though. A company can be fined 2% of their global turnover for not having their compliance records in order (Article 28), not notifying the supervising authority or Data Subjects about a Data Breach, or not conducting impact assessments. It is important to note that these rules apply to both Controllers and Processors.

Hereinafter, any mentions of "GDPR" shall be deemed to refer to the UK GDPR unless otherwise stated.

1.2 Definitions

Data Controller (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 UK law. the Controller or the specific criteria for its nomination may be provided for by UK law.

Data Privacy Framework (DPF) means the self-certification programme developed and administered by the International Trade Association, United States (U.S.) Department of Commerce in accordance with Executive Order 14086 to provide US organisations with a reliable mechanism for the transfer of Personal Data between the US and the EU while ensuring that Data Subjects continue to benefit from effective safeguards and protection as required under the GDPR with respect to the processing of their Personal Data when they have been transferred to non-EU countries. For the purpose of these policies, the meaning of Data Privacy Framework shall include the UK Extension to the DPF which purports to govern the transfer of Personal Data between the US and the UK in compliance with Data Protection Legislation.

Data Processing (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 Processor (Processor) means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

Data Protection Legislation means all laws relating to Data protection and privacy which are from time to time applicable to the Firm or any of the subsidiaries (or any part of their business), including (but not limited to): (i) the Data Protection Act 2018; (ii) "the UK GDPR", meaning Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018. All other applicable national laws, regulations and secondary data protection legislation, in each case as amended, replaced or updated from time to time and together with any subordinate or related legislation made under any of the foregoing.

Data Protection Officer (DPO) is an independent officer appointed under the UK GDPR in order to monitor internal compliance, inform and advise on Personal Data, provide advice regarding Data Protection Impact Assessments (DPIA); must be appointed when Data Processor or Controller are a public authority; an organisation processes special categories of Data on large scale; or which monitors systematically large number of Data Subjects (e.g. CCTV or collecting biometric Data).

Data Subject (Data, individual) means a natural person whose Personal Data are processed by a Controller or Processor.

EC means the European Commission.

EEA means the European Economic Area.

EU Adequacy Decision means the Commission Implementing Decision of 10 July 2023 (C(2023) 4745 final) in which the European Commission concluded, pursuant to Article 45(3) of EU GDPR, that the DPF ensured an adequate level of protection, equivalent to that of the EU, for Personal Data transferred from the EU to US organisations certified under the DPF.

ICO is the Information Commissioner's Office of the UK, with whose guidance this policy was supported.

Personal Data (Data, personal information) 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.

Privacy by Design means Data protection through technology design, integrated in the technology when at the creation stage, and included in the thought process before introducing any new processes within the organisation.

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.

Responsible Officer means the person taking on any UK GDPR responsibilities. For the purpose of these policies, the Responsible Officer refers to the Firm's Compliance Officer.

Special Categories of Data are Personal Data which the UK GDPR deems more sensitive, and which is afforded more protection. In order to lawfully process Special Categories of Data, you must identify both a lawful basis for processing it under Article 6 and a separate condition for Processing Special Categories of Data under Article 9. These do not have to be linked.

Supervisory Authority means an independent public authority which is established by the UK pursuant to Article 51 of the UK GDPR. In the UK, this is the ICO.

UK means, for the purpose of defining the territorial scope of the UK GDPR, the United Kingdom of Great Britain and Northern Ireland and the British Overseas Territory of Gibraltar.

UK Extension means the supplemental self-certification programme to the DPF issued and administered by the US Department of Commerce on 17 July 2023 (as amended) enabling the Firm to process transfers of Personal Data between the US and the UK, in compliance with Data Protection Legislation.

Working Party ("WP") is an advisory body made up of representatives from the Data protection authority of each member state of the EU whose guidance is considered in these policies as good practice (Article 29).

2. DATA BREACH POLICY

2.1 What is a Personal Data breach?

A Personal Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. This includes breaches that are the result of both accidental and deliberate causes. Note that a Data breach is more than just the loss of Personal Data.

2.2 Purpose

The purpose of this policy is to state the Firm's objectives and procedures applicable to Data breaches involving personal information; it follows requirements set out in the GDPR.

Under the GDPR, the Firm is required to ensure that correct procedures, controls and measures are in place in case a Personal Data breach occurs; it requires all employees to be made aware of the policy and procedures, and notes the Firm's processes for reporting, communicating and investigating any such breach.

2.3 Notification of a Personal Data breach to the ICO (within 72 hours)

In accordance with Article 33 of the GDPR, in the case of a Personal Data breach, the Controller shall without undue delay and, where feasible, no later than 72 hours after having become aware of the breach, notify the Personal Data breach to the competent Supervisory Authority. In accordance with Article 5(5) of GDPR, this notification is not required where the Personal Data breach is unlikely to result in a risk to the rights and freedoms of natural persons. This will have to be assessed by the Responsible Officer upon any breach occurring.

Organisations that have sustained a Data breach should use the ICO's self-assessment tool to determine the level of risk posed to the rights and freedoms of individuals (Self-assessment for data breaches | ICO).

Where the notification to the Supervisory Authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The notification to the Supervisory Authority shall contain at least:

a) a description of the nature of the Personal Data breach including where possible, the categories and approximate number of Data Subjects affected and the categories and approximate number of Personal Data records concerned;

b) the name and contact details of the Data protection officer or other contact point where more information can be obtained;

c) likely consequences of the Personal Data breach; and

d) a description of the measures, taken or proposed to be taken by the Controller, to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

See Appendix A for a copy of the Firm's Data breach reporting form and Appendix B for the employees' Data breach incident form.

Note that when submitting a Data breach to the Supervising Authority, organisations are required to use the ICO's standardised form (Report a breach | ICO).

2.4 Notification in phases

Depending on the nature of a breach, further investigation by the Firm may be necessary to establish all relevant facts relating to the incident.

Article 33(4) of the GDPR states that:

> *"Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay"*.

This means that the GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours.

2.5 Documenting all Data breaches

Although the GDPR introduces the obligation to notify a breach, it is not a requirement in all circumstances. The ICO places an obligation on the Firm to document any Personal Data breaches, (regardless of whether you are required to notify) comprising the facts relating to the Personal Data breach, its effects and the remedial action taken. That documentation shall enable the Supervisory Authority to verify compliance with the regulation (Article 33(5) of GDPR)

Communication of a Personal Data breach to the Data Subjects.

In certain cases, as well as notifying the Supervisory Authority, the Controller is required to communicate a breach to the affected Data Subjects.

Article 34(1) GDPR states:

> *"When the Personal Data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall communicate the Personal Data breach to the Data Subject without undue delay"*.

2.6 Information to be provided when notifying a Data Subject of Data breach

If the Firm has not already communicated the Personal Data breach to the Data Subject, the Supervisory Authority, having considered the likelihood of the Personal Data breach resulting in a high risk, may require it to do so.

When notifying a Data Subject, Article 34(2) of the GDPR specifies that:

> *"The communication to the Data Subject […] shall describe in clear and plain language the nature of the Personal Data breach and contain at least the information and measures"* set out below:

a) a description of the nature of the breach;

b) the name and contact details of the DPO or other contact point;

c) a description of the likely consequences of the breach; and

d) a description of the measures taken or proposed to be taken by the Controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

2.7 Conditions where notification is not required to the Data Subject

Article 34(3) states three conditions that, if met, do not require notification to individuals in the event of a breach. These are:

a) the Controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the Personal Data affected by the Personal Data breach, in particular those that render the Personal Data unintelligible to any person who is not authorised to access it, such as encryption;

b) the Controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of Data Subjects referred to in is no longer likely to materialise; or

c) it would involve disproportionate effort to inform the individuals; in such a case, there shall instead be a public communication or similar measure whereby the Data Subjects are informed in a effective manner.

2.8 Processor's obligation (when the Firm uses a third-party Processor to process Personal Data)

The Firm retains overall responsibility for the protection of Personal Data, but the Processor has an important role to play to enable the Firm's compliance with the GDPR requirements; and this includes notification of a Data breach to the Controller.

Article 33(2) states:

> "*The Processor shall notify the Controller without undue delay after becoming aware of a Personal Data breach*".

If the Processor used by the Firm becomes aware of a breach of Personal Data processed on behalf of the Firm, it must notify the Controller – the Firm *"without undue delay* The Controller is considered to be *"aware"* of the breach as soon as the Processor is.

The Firm's policy is to ensure that any Processor notifies it of a breach as promptly as possible and where possible it is suggested to encourage any Processors to agree to notifying the Firm of any breach within 48 hours of Processors becoming aware of it. As such, the Firm includes necessary provisions to that effect in any contract with Processors.

The obligation of the Processor to notify the Controller allows the Controller to address the breach and to determine whether or not it is required to notify the Supervisory Authority in accordance with Article 33(1) and potentially the affected individuals in accordance with Article 34(1).

3. DATA RETENTION AND ERASURE POLICY

3.1 Purpose and scope

This policy sets the required retention periods for Personal Data.

This policy applies to:

- all business units' processes and systems in which the Firm conducts business, and
- all business relationships with third parties.

This policy applies to Personal Data used by the Firm. Examples of where Personal Data are held include:

- emails
- hard copy documents
- soft copy documents
- Data generated by access control systems
- back ups
- systems
- third party systems and Data

The Firm's Data Retention policy and processes comply fully with Article 5(d), which states as follows:

> *"Personal Data shall be 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 for the purposes outlined in Article 89".*

Article 89 outlines exceptions to the GDPR rule on Data retention as follows:

> *"Where Processing is for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, it shall be subject to appropriate safeguards, in accordance with the GDPR, for the rights and freedoms of the Data Subject. Those safeguards shall ensure that* ***technical and organisational measures*** *are in place in particular in order to ensure respect for the principle of Data minimisation".*

These measures may include pseudonymisation, provided that the purposes of Processing can be fulfilled despite Personal Data being deprived of direct identifiers.

The Firm notes that where Personal Data are processed for scientific, historical research or statistical purposes, Data Protection legislation may provide for derogations from the rights of data subjects subject to relevant conditions and safeguards, insofar as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes (Schedule 1, Part 1, para. 4 of the Act).

Further, where Personal Data is processed for archiving purposes in the public interest. Such derogations from safeguarding the rights of Data Subjects are listed under Schedule 2, Part 6, para. 28 of the Act.

3.2 Responsibilities for Data destruction

Heads of business units and system owners shall have the overall responsibility for the management of the destruction of Data. When Personal Data are due for destruction, the system owner shall review, sign off and document such destruction. This will be reported to the Responsible Officer.

3.3 Data retention periods

Appendix C to this policy contains regulatory, statutory, and business retention periods. Where no defined or legal period exists for a Personal Data, the default standard period of 10 years shall apply.

3.4 Right to erasure ("Right to be forgotten")

In addition to the retention policy, the GDPR also includes a right to erasure, where a Data Subject can request deletion of their Personal Data.

Article 17 states that:

> "*The Data Subject shall have the right to obtain from the Firm the erasure of Personal Data concerning him or her without undue delay and the Firm shall have the obligation to erase Personal Data without undue delay where one of the following grounds applies (…)*".

The main applicable grounds are:

- where the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- where the Data Subject withdraws consent on which the Processing is based on;
- where the Data Subject objects to the Processing and the Processing is for direct marketing purpose, the Data Subject shall have the right to object at any time to Processing of Personal Data concerning him or her for such marketing, which includes Profiling to the extent that is related to such marketing and there are no overriding legitimate grounds for the Processing, or the Data Subject objects to the Processing pursuant to Article 21(2);
- when Personal Data has been unlawfully processed; and
- where Personal Data has to be erased for compliance with a legal obligation under Data Protection Legislation.

Please note that the Firm, taking into account available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other third parties which are Processing the Personal Data that the Data Subject has requested the erasure of any links to, or copy or replication of, those Personal Data.

Article 19 notes that:

> "*The Firm shall communicate any erasure of Personal Data carried out to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves*

disproportionate effort. The Controller shall inform the Data Subject about those recipients if the Data Subject requests".

The above Data erasure rules shall not apply to the extent that Processing is necessary:

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation which requires Processing by Data Protection Legislation to which the Controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;
- 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; or
- for the establishment, exercise or defence of legal claims.

Please refer to the Firm's policies on Data Subject rights for further guidelines.

4. INTERNATIONAL DATA TRANSFER POLICY

4.1 Overview

The Firm understands that any transfer of Personal Data undergoing Processing or intended for Processing after transfer to a third country (a country outside the UK and not deemed adequate by the ICO) or to an international organisation, shall only take place in compliance with Chapter 5 of the GDPR.

The Firm takes proportionate and effective measures to protect Personal Data held and processed by it, however we recognise the high-risk nature of disclosing and transferring Personal Data to a third country or to an international organisation. This policy outlines the measures and controls that we take to comply with the GDPR and provides guidance on to our employees and associated third parties.

4.2 General principles of transfer

Article 44 states that:

> *"Any transfer of Personal Data which are undergoing Processing or are intended for Processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this policy are complied with by the Controller and Processor, including for onward transfers of Personal Data from the third country or an international organisation to another third country or to another international organisation. All provisions in this policy shall be applied in order to ensure that the level of protection of natural persons guaranteed by the GDPR regulation is not undermined".*

4.3 Transfer on the basis of adequacy decision

Under Article 45 of the **EU GDPR,** a transfer of Personal Data to a third country or an international organisation may take place where the European Commission ("EC") has decided that the third country, a territory, or one or more specified sectors within that third country, or the relevant international organisation ensures an adequate level of protection. Such transfers shall not require any specific authorisation.

As a result of the GDPR becoming retained EU law, the following countries and territories are deemed to provide adequate safeguards by way of incorporating previous adequacy decisions issued by the European Commission:

- Andorra
- Argentina
- Canada (commercial organisations only)
- Faroe Islands
- Guernsey
- Isle of Man
- Israel
- Japan (private sector organisations only)

- Jersey
- New Zealand

  Uruguay

As a result of the United Kingdom's withdrawal from the EU, approvals concerning data transfers to the EEA as issued by the relevant countries and territories no longer apply. The UK Government is working with the above countries to enter into UK-specific arrangements for the purpose of adequacy decisions under Article 45 of the UK GDPR.

The following countries and territories have issued statutory instruments to extend their existing data transfer approval to the UK:

- Argentina
- Canada
- Faroe Islands
- Guernsey
- Isle of Man
- Israel
- Japan
- Jersey
- New Zealand
- Switzerland
- Uruguay

In addition, the ICO has issued adequacy decisions in its own rights:

- Contracting States of the EEA
- South Korea (Republic of Korea)

The Firm acknowledges that the substantive transfer rules under the UK GDPR and the EU GDPR may diverge in the foreseeable future and will closely monitor related developments from the ICO, the EC and foreign governmental agencies.

4.3 Transfers between the United Kingdom and the EEA

The ICO and the EC have issued mutual adequacy decisions under Article 45 of their respective GDPR. Both decisions are expected to last until 27 June 2025, subject to any material amendments to the relevant GDPR which would contravene the requirements for adequacy.

For the purpose of Personal Data transfers between the United Kingdom and the EEA, the EC's adequacy decision extends to England, Wales, Scotland, and Northern Ireland, to the preclusion of other Crown Dependencies and British Overseas Territories such as Gibraltar.

Under the current regime, organisation need not implement specific transfer tools (as discussed below) to continue transfers of Personal Data incoming from and outgoing to the EEA.

The Firm's processing activities does not come within the purview of the UK immigration control exemption under Schedule 2, Part 1, para.4 of the Act.

4.4 Transfers between the United Kingdom and the United States

As a result of the EU Adequacy Decision, organisations certifying to the U.S. Department of Commerce their adherence to the Data Privacy Framework Principles with regard to the processing of Personal Data received from the EU (the "Principles") under the DPF may process Personal Data incoming from the EU without the need to utilise additional transfer tools.

The Firm complies with the DPF, and the UK Extension thereto as set forth by the U.S. Department of Commerce and certifies to the latter that it fully adheres to the Principles under the DPF.

The Firm acknowledges that the UK Extension to the DPF is a voluntary add-on for the purpose of ensuring that international transfers of Personal Data comply with the UK GDPR. Although the UK Government and the U.S. Department of Commerce have agreed to establish a 'data bridge' for the UK Extension to the DPF in June 2023, no formal adequacy decision has been issued by the ICO at the time of writing.

Where required, the Firm is committed to comply fully with any future decision and requirements issued by the ICO under the UK GDPR and Schedule 21 of the Act.

Where there is any conflict between the terms in these policies and the Principles under the DPF, the Principles shall prevail. To learn more about the DPF, its Principles, and to verify the Firm's certification status, please visit https://www.dataprivacyframework.gov/.

The Firm further remains subject to the general investigatory and enforcement powers of the U.S. Federal Trade Commission (the "FTC") under Section 5 of the FTC Act (15 U.S.C. § 45).

The Firm remains liable under the EU-U.S. DPF Principles for any losses and damages resulting from the processing of personal data by third parties unless it can prove that it is not responsible for such losses or damages being caused.

4.6 Transfer subject to appropriate safeguards

Where a country is not listed as an adequate country, according to Article 46 of the GDPR, the Firm or Processor may transfer Personal Data to that country or an international organisation only if the Firm or Processor has provided appropriate safeguards ensuring secure Data transfer. Note that the other condition is that the legal regime of such country must allow effective legal remedy for the Data Subject in case of a Data breach.

The appropriate safeguards, also known as transfer tools, referred to above may be provided for, without requiring any specific authorisation from a Supervisory Authority, through:

- a legally binding agreement between public authorities or bodies;

- Binding Corporate Rules (BCR) in accordance with Article 47 (agreements governing transfers made between organisations within a corporate group);
- standard Data protection clauses adopted by the EC in accordance with the examination procedure referred to in Article 93(2) in the form of template transfer clauses adopted by the EC for transfers outbound from the EEA (**EU GDPR only**);
- standard Data protection clauses adopted by a Supervisory Authority and approved by the EC pursuant to the examination procedure referred to in Article 93(2) (**EU GDPR only**);
- standardised 'International data transfer agreement' and 'International data transfer addendum' issued by the Secretary of State and approved by Parliament under Section 119A of the Act (as amended) (**UK GDPR only**);
- an approved code of conduct (see Article 40) together with binding and enforceable commitments of the Firm and Processor in the third-party country to apply the appropriate safeguards as regards Data Subject rights;
- certification under an approved certification mechanism as provided for in the GDPR;
- an approved certification mechanism pursuant to Article 42, together with binding and enforceable commitments of the Controller or Processor in the third country to apply the appropriate safeguards, including Data Subjects' rights;
- subject to the authorisation from the competent Supervisory Authority, the appropriate safeguards referred to in the above may also be provided for, in particular, through: standard contractual clauses between the Controller or Processor and the Controller, Processor or the recipient of the Personal Data in the third country or international organisation; or
- provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective Data Subject rights.

The **UK GDPR** requires organisations from the UK to conduct a Transfer Risk Assessment prior to entering into any transfer tool mechanism for international transfers to third countries. Please refer to the ICO's guidance on Transfer risk assessments | ICO.

4.6 Derogations from the prohibition on transfers of Personal Data outside of the EU

In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including Binding Corporate Rules, a transfer or a set of transfers of Personal Data to a third country or an international organisation shall take place in the following conditions specified in Article 49:

- the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the Data Subject and the Controller or the implementation of pre-contractual measures taken at the Data Subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;

- the transfer is 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; or
- the transfer is made from a register which, according to Data Protection Legislation, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Data Protection Legislation for consultation are fulfilled in the particular case.

4.7 One-off (or infrequent) transfer of Personal Data concerning relatively few individuals

Where a transfer could not be based on a provision in Article 45 or 46 (please see above) including the provisions on binding corporate rules, and none of the derogations referred to above, a transfer to a third country or an international organisation may take place only if the Data transfer:

- is not repetitive (similar transfers are not made on a regular basis);
- involves Data related to only a limited number of Data Subjects;
- is necessary for the purposes of the compelling legitimate interests of the organisation (provided such interests are not overridden by the interests of the individual); and
- is made subject to suitable safeguards put in place by the organisation (in the light of an assessment of all the circumstances surrounding the transfer) to protect the Personal Data.

The Firm shall inform the Supervisory Authority of the transfer. The Firm shall, in addition to providing the information referred to in Articles 13 and 14, inform the Data Subject of the transfer and on the specific compelling legitimate interests pursued.

4.8 Responsibilities

The Responsible Officer has the overall responsibility for reviewing Data that is to be transferred to a third country or international organisation and is tasked with the continued review of the Commission's adequacy decisions, along with Supervisory Authority communication and authorisations, where applicable.

Any employee involved in the transfer of Personal Data, as categorised in this policy, must adhere to the conditions of this document and the regulations laid out in Chapter 5 of the GDPR.

5. INDIVIDUAL RIGHTS OF DATA SUBJECTS

This policy covers the individual rights covered by the GDPR Articles. These rights are enforceable by the Data Subject. The Firm has in place processes enabling to meet the different rights outlined below.

The GDPR provides the following rights for any Data Subject:

1. the right to be informed;
2. the right of access;
3. the right to rectification;
4. the right to erasure;
5. the right to restrict Processing;
6. the right to Data portability;
7. the right to object;
8. the rights in relation to automated decision-making and Profiling.

The Firm has processes to meet any request sent in by any Data Subject within one month. If the Firm requires additional time to respond or it will not take the requested action, the Data subject must be informed of it promptly.

5.1 Right to be informed

Under Article 13 of the GDPR, a Data Subject needs to be informed about how we use their Data. This information must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

The Firm shall be deemed to comply with the right to be informed by providing the Data Subject with a copy of its Privacy Notice, see Appendix F.

5.2 Right of access

Article 15 states:

> "*The Data Subject shall have the right to obtain from the Firm confirmation as to whether or not Personal Data concerning him or her are being processed, and, where that is the case, access to the Personal Data".*

When a valid access request is received by the Firm from a Data Subject, the Data Subject shall have access to 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, in particular recipients in third countries or international organisations;
- 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 from the Controller 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 are not collected from the Data Subject, any available information as to their source;
- where Personal Data are transferred to a third country or to an international organisation, the Data Subject shall have the right to be informed of the appropriate safeguards applied to the transfer; and
- the Controller shall provide a copy of the Personal Data undergoing Processing.

Where the Data Subject makes a request by electronic means, and unless otherwise requested by the Data Subject, the information shall be provided in a commonly used electronic form.

Where any further copies are requested by the Data Subjects, the Firm may charge a reasonable fee based on administrative costs.

5.3 Right to rectification

This is a right for Data Subjects to have inaccurate Personal Data rectified.

Article 16 states that:

> "*The Data Subject shall have the right to obtain from the Controller without undue delay the rectification of inaccurate Personal Data concerning him or her. Taking into account the purposes of the Processing, the individual shall have the right to have incomplete Personal Data completed, including by means of providing a supplementary statement".*

5.4 Right to erasure

The GDPR introduces a right for Data Subjects to have their Data erased. The right to erasure is also known as *"the right to be forgotten"*. The Data Subjects can request their personal Data in writing or verbally.

Guidelines on the right of erasure can be found in the Firms 's Data deletion and erasure policy.

5.5 Right to restriction of Processing

Data Subjects have a right to request the restriction of Processing of their Personal Data.

Article 18 states that:

"*The Data Subject shall have the right to obtain from the Controller restriction of Processing where one of the following applies*":

- the accuracy of the Personal Data is contested by the Data Subject, for a period enabling the Controller to verify the accuracy of the Personal Data;
- the Processing is unlawful, and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;
- the Controller no longer needs the Personal Data for the purposes of the Processing, but they are required by the Data Subject for the establishment, exercise, or defence of legal claims; or
- the Data Subject has objected to Processing pending the verification whether the legitimate grounds of the Controller override those of the Data Subject.

Where Processing has been restricted by the Data Subject, all Personal Data belonging to the Data Subject with the exception of storage, can be processed:

- only with the Data Subject's consent;
- for the establishment, exercise or defence of legal claims; or
- for the protection of the rights of another natural or legal person or for reasons of important public interest of the United Kingdom.

5.6 Right to Data portability

Article 20 states:

> *"The Controller shall have the obligation to provide the Data Subject with a right to receive the Personal Data concerning him or her, which he or she has provided to a Controller, in a structured, commonly used and machine-readable format and have the right to transmit those Data to another Firm without hindrance from the Firm to which the Personal Data have been provided, where technically feasible".*

The above right applies where the Processing is based on:

- one of the lawful reasons of Processing; and
- the Processing is carried out by automated means.

The right described shall not apply where the Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Firm.

5.7 Right to object

The GDPR rules introduce the right of a Data Subject to object.

Article 21 notes that:

> *"The Data Subject shall have the right to object, on grounds relating to his or her particular situation, at any time to Processing of Personal Data concerning him. The Firm shall no longer process the Personal Data unless the Firm demonstrates compelling legitimate grounds for the*

Processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims".

The right to object, on grounds relating to a Data Subject's particular situation is only exercisable where lawful basis for Data Processing are:

- necessity for the performance of tasks carried out in the public interest or in the exercise of official authority vested in the controller, or

- where the Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the 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.

5.8 *Right to object in regards to direct marketing*

Article 21 notes that:

> *"*Where the Data Subject objects to Processing for direct marketing purposes, the Personal Data shall no longer be processed for such purposes."

5.9 Automated individual decision-making, including Profiling

Article 22 states that:

> "*The Data Subject shall have the right not to be subject to a decision based solely on automated Processing, including Profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".*

The above paragraph shall not apply to the Firm where Profiling:

- is necessary for entering into, or performance of, a contract between the Data Subject and the Data Controller;

- is authorised by the Data Protection Legislation to which the Controller is subject and which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests; or

- is based on the specific consent given by the Data Subject.

In the above instances, the Firm shall ensure it has implemented suitable measures to safeguard the Data Subject's rights, freedoms and legitimate interests.

In cases of *"Special Categories of Data"*, automated individual decision shall only apply where the Data Subject has given explicit consent or where Processing is necessary for reasons of substantial public interest, on the basis Schedule 1, Part 2 of the Act, which shall be proportionate to the aim pursued. In such instances, the Firm shall apply suitable measures to safeguard the Data Subject's rights and freedom.

5.10 Rights under the DPF

Data Subjects whose Personal Data are processed by U.S. organisations certified under the DPF may lodge complaints in accordance with the **EU GDPR** with their national Supervising Authority. The complaint will be transmitted to the U.S. via the European Data Protection Board.

Under the DPF, redress and enforcement proceedings follow a two-tier review. First, complaints are investigated by Civil Liberties Protection Officer ("CLPOs") within the relevant U.S. intelligence agencies. Data Subjects will be able to appeal against the decision of CLPOs before the Data Protection Review Court (the "DPRC") established under 28 C.F.R. § 201.

By way of the EU Adequacy Decision, the EC considers the DPRC to be an independent tribunal and to provide adequate access to remediation. Proceedings are brought by the U.S. Attorney General on behalf of individuals from 'Qualifying States' which includes EEA, Iceland, Lichtenstein, and Norway.

The DPRC has powers to investigate complaints from individuals residing in Qualifying States, including to obtain relevant information from intelligence agencies, and can take binding remedial decisions.

The Firm acknowledges that it is subject to the jurisdiction of the International Centre for Dispute Resolution as prescribed under Annex I to the EU-U.S. DPF Principles. Where a complaint is not resolved by either the Firm and/or the Supervising Authority, data subjects have the right to invoke binding arbitration. The arbitral tribunal is competent to issue individual-specific and non-monetary equitable remedies.

Pre-dispute protocols are further set out at ICDR-AAA DPF Annex I Services EU-US and UK | How to File | ICDR.org (adr.org). Data subjects may visit Assistance Services (dataprivacyframework.gov) for more resources.

For more information, please review the Supplemental Principles under the DPF at https://www.dataprivacyframework.gov/.

When the ICO issues an adequacy decision concerning the UK Extension to the DPF, the Firm anticipates that Data Subjects in the UK will gain access to the same remediation process.

6. SUBJECT ACCESS REQUEST POLICY

6.1 What is a Subject Access Request (SAR)?

A SAR is a written request for information on what, if any, Personal Data is the Firm processing. It is made by or on behalf of a Data Subject.

6.2 Responding to a SAR

The Firm shall facilitate the exercise of Data Subjects' rights under Articles 15-22.

In cases where the Firm is unable to confirm the identity of a Data Subject who is submitting a SAR, the Firm shall inform the Data Subject accordingly. In such cases, the Firm has a justified right to reject the Data Subject's request, unless the Data Subject provides additional information enabling his or her identification (Article 11 (2c)).

The Firm shall provide information on any action taken on a SAR without undue delay and, in any event, within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of requests. Where the Data Subject makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the Data Subject. Information provided under this policy shall be provided free of charge.

Where SARs from a Data Subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Firm may either:

- charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested; or
- refuse to act on the request.

The Firm shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

The information to be provided to Data Subjects pursuant to this policy must be intelligible and clearly legible, and it must constitute a meaningful overview of the Processing.

6.3 Submission and lodging a complaint

To submit a SAR to the Firm, a Data Subject should be instructed to contact the Firm at the email below:

ts@tourmalinellc.com

The Data Subject may also be told that they can submit their request in writing by sending the request to:

c/o Tom Sisterson
Tourmaline Europe LLP
5th Floor
8 Waterloo Place
London

SW1Y 4BE

6.5 Supervisory Authority

If the Data Subject remains dissatisfied with the Firm's actions, they have the right to lodge a complaint with the Supervisory Authority.

The ICO can be contacted at following address:

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

Telephone: 0303 123 1113 (local rate) or 01625 545 745 (national rate)
Fax: 01625 524 510

7. DATA PROTECTION IMPACT ASSESSMENT POLICY

7.1 Overview

A Data Protection Impact Assessment (DPIA) is a key risk assessment process required under the GDPR. It helps organisations make an early evaluation of the impact that Processing might have on a Data Subject. It also helps manage the risks to the rights and freedoms of natural persons resulting from the Processing of Personal Data.

DPIAs are important tools for accountability, as they help the Firm to not only comply with the requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance.

An effective DPIA will allow the Firm to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

The use of DPIAs is seen by the Firm as an integral part of taking a Privacy by Design approach.

7.2 When do I need to conduct a DPIA?

In accordance with Article 35(1) of the GDPR, a DPIA must be carried out:

> *"Where a type of Processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the Processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall, prior to the Processing, carry out an assessment of the impact of the envisaged Processing operations on the protection of Personal Data. A single assessment may address a set of similar Processing operations that present similar high risks."*

The GDPR does not require a DPIA to be carried out for every Processing operation. The carrying out of a DPIA is only mandatory where Processing is *"likely to result in a high risk to the rights and freedoms of natural persons"*.

A DPIA referred to in Article 35(1) shall in particular be required in cases of:

- 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;
- Processing of Special Categories of Data referred to in Article 9(1) on a large scale or of Personal Data relating to criminal convictions and offences referred to in Article 10; or
- systematic monitoring of a publicly accessible area on a large scale.

Article 35(11) GDPR also states:

> *"Where necessary, the Firm shall carry out a review to assess if Processing is performed in accordance with the Data protection impact assessment at least when there is a change of the risk represented by Processing operation".*

7.3 Which Processing operations are subject to a DPIA

According to WP, taking into account Article 35(1) and Article 35(3), the situations in which the Firm should consider conducting a DPIA are as follows:

- evaluation or scoring, including Profiling: an example is a company that screens its customers against a credit reference Data base;
- automated decision-making with legal or similar significant effect on the individual, for example, where the Processing may lead to the exclusion or discrimination against individuals;
- systematic monitoring: Processing used to observe, monitor or control Data Subjects, including collected through *"a systematic monitoring of a publicly accessible area*"; e.g., CCTV cameras;
- Processing of Special Categories of Data: 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;
- personal Data processed on a large scale;
- combining or matching of Datasets;
- Personal Data concerning vulnerable Data Subjects;
- innovative use or applying technological, for example combining use of finger prints and face recognition for improved physical access control, etc;
- personal Data transfers across borders outside the EEA: taking into consideration, amongst others, the envisaged country or countries of destination, the possibility of further transfers, or
- when the Processing in itself prevents Data Subjects from exercising a right or a contract, or using a service .

In cases where it is not clear whether a DPIA is required, the WP recommends that a DPIA is carried out as it is a useful tool to help Data Controllers comply with Data protection law.

7.4 Instances where a DPIA is not required

According to WP a DPIA will not be required in the following cases:

- where the Processing is not *"likely to result in a high risk to the rights and freedoms of natural persons"* (Article 35(1));
- when the nature, scope, context and purposes of the Processing are very similar to the Processing for which a DPIA has already been carried out. In such cases, results of DPIA for similar Processing can be used (Article 35(1));
- where a Processing operation has a legal basis in the Data Protection Legislation, which has stated that an initial DPIA does not have to be carried out; and
- where the Processing is included on the optional list (established by the Supervisory Authority) of Processing operations for which no DPIA is required (Article 35(5)).

7.5 How to carry out a DPIA

When should a DPIA be carried out?

The Firm shall carry out a DPIA prior to intended Processing (Article 35(1)). This is consistent with the principle of Data Privacy by Design. The Firm will start its DPIA as early as practical in the design of the Processing operation even if some of the Processing operations are still unknown. The DPIA is a working document and should be updated throughout the lifecycle of Processing. This will ensure that Data protection and privacy are considered and promoted within the process of creation of the Processing operations.

Who is responsible for conducting a DPIA?

The Firm is responsible for ensuring that a DPIA is carried out (Article 35(2)). Carrying out a DPIA may be done by the Responsible Officer inside or outside the organisation, but the Firm remains ultimately accountable for the task.

It is worth noting that Article 35(9) states that:

> *"Where appropriate, the Firm shall seek the views of Data Subjects or their representatives on the intended Processing, without prejudice to the protection of commercial or public interests or the security of Processing operations".*

7.6 Overview of the DPIA process

Article 35(7) sets the minimum elements that each DPIA must contain:

- a description of the envisaged Processing operations and the purposes of the Processing, including, where applicable, the legitimate interest pursued by the Controller;
- an assessment of the necessity and proportionality of the Processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of Data Subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of Data Subjects and other persons concerned.

Appendix D to this policy contains a DPIA template which will be used to carry out all assessments as required by the GDPR.

When residual risks are high and the Firm cannot find sufficient security measures to protect the Personal Data processed, the Firm may take steps to consult the Supervisory Authority. When the residual risks remain high the consultation becomes obligatory.

8. SPECIAL CATEGORIES OF DATA POLICY

8.1 Overview

Article 9 (1) of the GDPR defines Special Categories of Data as Personal Data revealing:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic Data;
- biometric Data for the purpose of uniquely identifying a natural person;
- health or Data concerning a natural person's sex life or sexual orientation.

8.2 Scope

As a rule, under the GDPR, Processing of Special Categories of Data is prohibited (Article 9(1)).

8.3 Exceptions to the rule: when Processing of Special Categories of Data is allowed

The prohibition on Processing of Special Categories of Data in Article 9(1) will not be applied in certain conditions as set out in Article 9(2):

a) where the Data Subject has given explicit consent to Processing of Personal Data falling under the category of Special Data for one or more specified purposes, except where Schedule 1 of the Act provides that the prohibition referred to in Article 9(1) may not be lifted by the Data Subject;

b) 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 in so far as it is authorised by Schedule 1 of the Act providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject;

c) Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the 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.

   Recital 46 provides further insight on the use of vital interest as a ground for Processing. Vital interest here can be relied on where it is necessary to protect an interest which is essential for the life of the Data Subject or other natural persons;

d) 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 and on condition that the Processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed outside that body without the consent of the Data Subjects;

e) Processing relates to Personal Data which are manifestly made public by the Data Subject;

f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g) Processing is necessary for reasons of substantial public interest, on the basis of Schedule 1, Part 2 of the Act which shall be proportionate to the aim pursued, respect the essence of the right to Data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;

h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services on the basis of Schedule 1, Part 1 of the Act or pursuant to contract with a health professional and subject to the conditions and safeguards;

i) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Schedule 1, Part 1 of the Act, which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy;

j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Schedule 1, Part 2 of the Act which shall be proportionate to the aim pursued, respect the essence of the right to Data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

Personal Data referred to in Paragraph 1 of this policy may be processed for the purposes referred to in sub paragraph (h) above: *"Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis"* when these Data are processed by or under the responsibility of a professional, subject to the obligation of professional secrecy under Schedule 1, Part 1 of the Act.

9. CONSENT POLICY

9.1 Overview

Consent remains one of six lawful bases for processing of Personal Data, as listed in Article 6 of the GDPR. When initiating activities that involve Processing of Personal Data, a Controller must always take time to consider whether consent is the appropriate lawful ground for the envisaged Processing or whether another ground should be chosen instead.

Generally, consent can only be an appropriate lawful basis if a Data Subject is offered full control over their consent and genuine choice with regard to accepting or declining the offered term without any detriment. When asking for consent, the Firm has a duty to assess whether it will meet all the requirements to obtain a valid consent.

The GDPR places the onus on the Firm to prove that consent has been validly obtained. In order to comply with this requirement, the Firm must keep a record of consent collection.

The GDPR definition of consent is:

> *"[…] 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."*

9.2 Guidance on obtaining valid consent:

Consent requests must be:

Unbundled: ensure that consent requests are separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service.

Named: state which organisation and third parties will be relying on consent.

Documented*:* keep records to demonstrate what an individual has consented to, including what they were told, and when and how they consented.

Easy to withdraw: tell people they have the right to withdraw their consent at any time, and how to do this. It must be as easy to withdraw the consent as it was to give it. This means you will need to have simple and effective withdrawal mechanisms in place.

Active opt-in: pre-ticked opt-in boxes are invalid – use unticked opt-in boxes or similar active opt-in methods.

9.3 Consent as valid lawful basis for Processing

For Processing to be lawful under the GDPR, you need to identify (and document) your lawful basis for the Processing of Data. There are six lawful grounds for the Processing of Data listed in Article 6(1), and consent is one of them.

> *"Processing shall be lawful only if the Data Subject has given consent to the Processing of his or her Personal Data for one or more specific purpose".*

Where the Firm relies on consent as a basis of lawful Processing, the Firm should ensure that Data are only processed for that specific reason. Any further Processing shall be subject to obtaining further consent from the Data Subject.

9.4 Conditions for consent

Article 7 also sets out the conditions of a valid consent to the Processing of Data:

- where Processing is based on consent, the Controller shall be able to demonstrate that the Data Subject has consented to Processing of his or her Personal Data.
- if the Data Subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this shall not be binding.
- the Data Subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of Processing based on consent before its withdrawal. Prior to giving consent, the Data Subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
- when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the Processing of Personal Data that is not necessary for the performance of that contract.

All the requirements for consent have been captured in a consent register, which you can find in Appendix E.

10. CONTROLLER AND PROCESSOR POLICY

This policy sets out the obligations, responsibilities and agreements between the Controller and the Processor.

The Firm as Data Controller takes guidance from Article 28 and Article 29 of the GDPR.

10.1 Controller and Processor's responsibilities

The Data Controller shall ensure that the Processor is GDPR-compliant where the Processor is carrying out Processing on the Controller's behalf. It is the responsibility of the Controller to ensure that the Processor takes all relevant steps to be compliant.

The ICO guidance also notes that Controllers are ultimately responsible for ensuring that Personal Data are processed in accordance with the GDPR. Unless the Controller can demonstrate that they are *"not in any way responsible for the event giving rise to the damage"* they will be fully liable for any damage caused by non-compliant Processing; it is so to ensure a Data Subject receives effective compensation.

Article 28 states:

> *"Where Processing is to be carried out on behalf of a Controller, the Controller shall use only Processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of this Regulation and ensure the protection of the rights of the Data Subject".*

Whenever the Controller uses the Processor, they need to have a written contract in place. Similarly, if the Processor employs another Processor (sub-Processor) – this relationship must be governed by a similar contract.

10.2 What should be included in the Controller-Processor agreement

Under Article 28(3) the contract shall cover:

The subject matter and duration of Processing, the nature and purpose of Processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of Data Controller and Data Processor.

Further, the Processor shall:

- not engage another Processor without prior specific or general written authorisation of the Controller. In the case of general written authorisation, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of other Processors, thereby giving the Controller the opportunity to object to such changes;
- process the Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Data Protection Legislation to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest;

- ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- take all security measures required as set out under Article 32 (see 9.2);
- respect the conditions referred to above when engaging with another Processor;
- the Processor taking into account the nature of the Processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter 3 of the GDPR;
- assist the Controller in ensuring compliance with the obligations such as the security of Processing, Data breach reporting, communicating Personal Data breach to the Data Subject and carrying out Data protection impact assessment;
- at the choice of the Controller, delete or return all Personal Data to the Controller after the end of the provision of services relating to Processing, and delete existing copies unless laws require storage of the Personal Data;
- make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller;
- where a Processor engages another Processor for carrying out specific Processing activities on behalf of the Controller, impose the same Data protection obligations as set out in the contract or other legal act between the Controller and the Processor on that other Processor by way of a contract or other legal act under relevant law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of the GDPR. Where that other Processor fails to fulfil its Data protection obligations, the initial Processor shall remain fully liable to the Controller for the performance of that other Processor's obligations;
- adhere to an approved code of conduct as set out in Article 40 around transparent Processing, collection of Data, pseudonymisation of Personal Data, exercise of Data Subject rights;
- have the contract in writing, including electronic form;
- be considered to be a Controller in respect of Processing if a Processor infringes the GDPR by determining the purposes and means of Processing.

The responsibilities of the Processor listed in Article 28(3)(c) of the GDPR refers to the Processor taking all necessary security measures.

Article 32 provides guidance on the security measures expected to be implemented.

Article 32(1) states that:

> *"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Controller and the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate".*

The appropriate level of security shall be assessed based on the risks that are presented in Processing the relevant Data. The Controller will consider as part of its due diligence process conducted on any Processor:

- whether the Processor has put in place technical and organisational measures covering risk to rights and freedoms of an individual which may include pseudonymisation and encryption of Personal Data;
- whether the ongoing confidentiality, integrity, availability and resilience of Processing systems and services is ensured;
- whether the Processor has the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
- whether the Processor has devised a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures and for ensuring the security of the Processing.

11. PRIVACY NOTICE

The Firm will issue a Privacy Notice detailing its Processing activities and ensuring transparency and accessibility of information for Data Subjects. It will also be added to relevant websites and otherwise distributed to relevant parties. A Privacy Notice template is set out in Appendix F and will be adapted where it will be distributed to employees.

12. STAFF TRAINING

The GDPR aims to change the culture around the handling of Personal Data within organisations. The Privacy by Design principle expressed in Article 25 of the GDPR requires the Firm to implement appropriate technical and organisational measures to ensure security for any Personal Data. For these measures to be effective, the Firm must ensure that the personnel working with the Personal Data are trained appropriately in this area.

Further, Article 39 and Article 47 of the GDPR indicate that staff training should be done by the Firm. Although Article 39 refers to the Data Protection Officer role which is not required in the Firm and Article 47 to the establishment of the binding corporate rules mechanism, in combination with the Privacy by Design principle they both suggest that in order to achieve full compliance, personnel should be trained.

Therefore, the Firm implements training for all staff members to raise their awareness around Data protection issues and to equip them with knowledge allowing them to conduct their professional activities with privacy and security in mind.

The Firm follows the below training programme:

- the Firm embraces the Privacy by Design and Personal Data security in all company-wide communications; and
- the Firm provides general training emphasising Data protection issues for all personnel on an annual basis.

APPENDICES

Appendix A: Data breach reporting template

REPORT PREPARED BY:	
NAME OF THE FIRM:	DATE & TIME:
[FOR THE RESPONSIBLE OFFICER] INCIDENT INFORMATION:	
SUMMARY OF INCIDENTS THAT CAUSED THE DATA BREACH:	
INDICATE IF THE BREACH IS RELATED TO A PROCESSOR:	
NUMBER OF INDIVIDUALS INVOLVED:	
TYPE OF PERSONAL DATA (PERSONAL OR SENSITIVE):	
SUMMARY OF INCIDENTS THAT CAUSED THE DATA BREACH:	
INDICATE THE TECHNICAL AND ORGANISATIONAL MEASURES YOU HAVE APPLIED TO SECURE THE AFFECTED DATA:	
WHAT SAFEGUARDS ARE IN PLACE WITHIN THE ORGANISATION TO MITIGATE THE BREACH?	
HAVE THE DATA SUBJECTS BEEN INFORMED OF THIS BREACH? (IF NO, PLEASE EXPLAIN RATIONALE)	

HAVE ALL EMPLOYEES COMPLETED A DATA BREACH TRAINING?
HAS THE SUPERVISORY AUTHORITY BEEN NOTIFIED WITHIN 72 HOURS OF BECOMING AWARE OF THE BREACH?

Appendix B: Data breach incident form for employees

RESPONSIBLE OFFICER/INVESTIGATOR DETAILS:	
Name:	**Position:**
INCIDENT INFORMATION:	
DATE/TIME OF BREACH:	
DESCRIPTION & NATURE OF BREACH:	
STAFF INVOLVED IN BREACH:	
NO OF DATA SUBJECTS AFFECTED:	
CATEGORIES OF DATA SUBJECTS AFFECTED:	
IMMEDIATE ACTION TAKEN TO CONTAIN/MITIGATE BREACH:	

Appendix C: Retention register

RECORD	RETENTION PERIOD	DATA OWNER	METHOD OF DELETION	NOTES
HMRC Records	6 years due to HMRC regulation	Finance	System Alert in place to alert Data owners	Deletion completed / Actions taken
AML Records	7 years- AML regulations	Compliance team	System Alert in place to alert Data owners	Deletion completed / Actions taken

Appendix D: DPIA Template

Step 1: Identify the need for a DPIA

EXPLAIN BROADLY WHAT THE PROJECT AIMS TO ACHIEVE AND WHAT THE PROCESSING INVOLVES:

Step 2: Describe the information flow

DESCRIBE THE NATURE OF PROCESSING: HOW WILL YOU COLLECT, USE, STORE, SHARE AND DELETE DATA. DOES IT INCLUDE ANY SENSITIVE DATA?

Step 3: Identify and assess risks

DESCRIBE THE SOURCE OF RISK AND NATURE OF POTENTIAL IMPACT ON DATA SUBJECT	LIKELIHOOD	SEVERITY

Step 4: Identify measures to reduce risk

IDENTIFY ADDITIONAL MEASURES YOU COULD TAKE TO REDUCE OR ELIMINATE RISKS IDENTIFIED IN STEP 3:

RISK	OPTIONS TO REDUCE OR ELIMINATE RISK	EFFECT ON RISK	RESIDUAL RISK	MEASURES APPROVED (if high risk cannot be mitigated, contact the Supervisory Authority):

Step 5 : Sign off and record of outcome

ITEM	NAME/DATE	NOTES

Step 6: Integrate the DPIA outcomes into a project plan:

PLEASE EXPLAIN HOW THIS IS INCORPORATED INTO THE PROJECT PLAN:

Summary by Responsible Officer:

Next review date:

Appendix E: The Legitimate Interests Assessment (LIA) – the "3-stage test"

An essential part of the concept of the legitimate interests lawful basis to Processing Data (Legitimate Interests) is the balance between the interests of the Controller and the rights and freedoms of the individual:

If a Controller wishes to rely on legitimate interests for Processing Personal Data it must carry out an appropriate assessment, which is called a Legitimate Interests Assessment, or LIA. When carrying out an assessment, the Controller must balance its right to process the Personal Data against the individuals' Data protection rights.

In certain circumstances, a LIA may be straightforward. However, it is advisable for the Controller, in order to ensure compliance with Article 5(2), to maintain a written record that they have carried out a LIA and the reasons why they came to the conclusion that it met the balancing test elements.

These LIAs may be disclosed to other Controllers in the event of a sale or acquisition of Personal Data, where legitimate interests is the lawful basis of Processing, as part of the due diligence process. It may be needed when asked by the Supervisory Authority, or an individual concerned, to demonstrate compliance with the GDPR.

The 3 key stages of an LIA are:

1. **Identify a legitimate interest:** What is the purpose for Processing the Personal Data and why is it important to you as a Controller?
2. **Carry out a necessity test:** Controllers should consider whether the Processing of Personal Data is *"necessary"* for the pursuit of its commercial or business objectives.
3. **Carry out a balancing test:** A Controller can only rely on a genuine legitimate interest where the rights and freedoms of the individual whose Personal Data will be processed have been evaluated and these interests do not override the Controllers' legitimate interest.

1. Identifying a legitimate interest:

	QUESTION	ANSWER
1.	What legitimate interest have you identified?	
2.	What is the purpose for Processing the Personal Data?	
3.	Has the legitimate interest been articulated clearly to the Data Subject?	
4.	Explain the nature of the legitimate interest (e.g. is it fundamental right, commercial business or public interest)	

2. Necessity test:

5.	Does this Processing actually help to further your legitimate interest?		
6.	Is it a reasonable way to go about it		
7.	Is there a less intrusive way to achieve the same result?		

3. Carrying out a balancing test:

8.	Would or should the individual expect the Processing to take place? If they would, then the impact of the individual is likely to have already been considered by them and accepted. If they have no expectation, then the impact is greater.		
9.	Is it also in the interests of the individual?		
10.	What the type of data are (i.e. does that data require additional protection in the GDPR, such as data relating to a child or a special category)		
11.	Is there any harm that could be caused as a result of the Processing, is it Unwarranted?		
12.	What is the nature of your relationship with the individual?		
13.	What controls are in place to protect the individual or reduce any negative impact?		
14.	Are you happy to explain conclusions of your balancing test to the Data Subject or the Supervisory Authority?		

If the outcome of an LIA remains that the Controller cannot rely on legitimate interests as a lawful basis for the Processing, then the Controller must find an alternative legal basis or not proceed with such Processing.

Keep a record of your LIA and the outcome. Use the table above as a guide, and because it is important to record your process of decision making to demonstrate that you have proper decision-making processes in place and to justify the outcome.

Keep your LIA under review and refresh it if there is a significant change in the purpose, nature or context of the Processing.

If you are not sure about the outcome of the balancing test, it may be safer to look for another lawful basis. Legitimate interests will not often be the most appropriate basis for Processing which is unexpected or high risk.

If your LIA identifies significant risks, consider whether you need to do a more complete DPIA to assess the risk and potential mitigation in more detail.

Appendix F: The Privacy Notice template

I. Privacy Notice (general, to be placed on the website)

Overview

Article 5 of the GDPR States that Personal Data must be processed lawfully, fairly and in a transparent manner. In line with the GDPR changes, we are updating our Privacy Notice so you can better understand why and how we collect, process and destroy your Data. We are committed to protecting and respecting your privacy. This policy together with the Terms and Conditions and any other documents referred to in it sets out the legal basis on which any Personal Data we collect from you, or that you provide to us, will be processed by us. Please read the following carefully to understand our views and practices regarding your Personal Data and how we will treat it.

What types of Personal Data do we collect?

We may control, process and use your Personal Data, which may include names, postal addresses, email addresses, telephone numbers or any other Personal Data that you provide to us. We may also, in appropriate cases and to the extent permitted by law, control, process and use certain special categories of Personal Data which are more sensitive in nature (e.g. when undertaking "Know Your Customer" (KYC) or anti-money laundering (AML) checks, we may collect information about any criminal conviction offence that you or the directors of any company might have committed).

Identity of the Firm

Tourmaline Partners, LLC
680 Washington Blvd.
10th Floor
Stamford, CT 06901
United States of America

Tourmaline Partners, LLC is the parent company of Tourmaline Europe LLP, which is authorised and regulated by the Financial Conduct Authority, with FRN: 552917.

Tourmaline Europe LLP
5th Floor
8 Waterloo Place
London, SW1Y 4BE
United Kingdom

Lawful basis for Processing

Where we act as Data Controller, we rely on the following legal basis for Processing your Personal Data:

- consent – if you access our password protected centralized commission management system;
- legitimate interests – if you are our client or prospect client, business affiliate or our website visitor;
- performance of contract – if you are our client, supplier, employee, akin to employee or business affiliate or our website visitor;
- legal obligation – if we process Personal Data according to requirements of domestic legislation;

Where we act as Data Processor, we process Personal Data on behalf of a Data Controller and we act on their written instructions.

Data Protection Officer

The Firm has no regulatory obligations under the GDPR to appoint a DPO; the Firm has no DPO currently appointed. The GDPR sets out guidelines on when the appointment of a DPO shall be required as follows:

- where the scope or purpose of collecting Data requires a regular systematic monitoring of the Data Subjects;
- where the Firm processes Special Categories of Data on a large scale;
- where Processing is carried out by a public authority.

The Firm has instead agreed to name a Responsible Officer who may be reached at ts@tourmalinellc.com.

Purpose of Data collected

The personal information we collect is for the following legitimate interest:

- provision of financial products and services;
- promotion of ideas and events relating to services we provide;
- accuracy of client records,
- maintenance of records of communication and management of your relationship with us;
- to respond to you enquires;
- to comply with any present or future law, rule, regulation, guidance, decision or directive (including those concerning anti-terrorism, fraud, AML and anticorruption);
- to carry out, in appropriate cases, KYC checks and other procedures that we undertake prior to you becoming a customer of ours;
- prevention and detection of fraud and other illegal activity or misconduct; and
- for informing you about compliance with legal and regulatory obligations and provide related guidance.

Who we share our information with

We will not share personal information about you with third parties without your consent. We are required, by law, to sometimes pass on some of this Personal Data to:

- law enforcement agencies; financial regulators and other relevant regulatory authorities; government bodies; tax authorities; courts tribunals and complaints/dispute resolution bodies;
- other bodies as required by law or regulation; or
- related financial institutions such as trustees, custodians and sub-custodians; insurers; fraud protection agencies; and/or similar suppliers or service providers.

To fulfil our contract with you, the Firm may sometimes pass information to:

- IT services including client relationship management platforms;
- government and self-regulatory agencies as required; and
- intragroup to related affiliates also working on providing you with related services.

International transfer outside the EEA and the UK

The Firm does not transfer your personal information outside of the EEA (respectively, the UK) unless the transfer is necessary for one of the reasons set out in the GDPR, including the performance of a contract between the Firm and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving consent and, in some limited cases, for our legitimate interest.

In these cases, we will follow the GDPR guidelines in protecting the transfer of Data to countries outside the EEA (respectively, the UK) to ensure that the level of Data protection afforded to individuals by the GDPR is not undermined.

The Firm will only transfer Personal Data outside the EEA (respectively, the UK) if one of the following conditions applies:

- the European Commission (respectively, the ICO) has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects. This refers to (individual's resident rights and freedoms);
- appropriate safeguards are in place such as BCRs, standard contractual clauses approved by the EC (respectively, the international data transfer agreement as issued by the ICO), an approved code of conduct or a certification mechanism, a copy of which can be obtained from the Responsible Officer;
- the Data Subject has provided Explicit Consent (i.e. where permission has been given by the Data Subject in writing to the proposed transfer after being informed of any potential risks).

Onward transfers to third parties

In accordance with the DPF Principles, Tourmaline Partners, LLC may transfer personal data onward to a third party provided that it (i) informs the data subject and obtain their consent for such a transfer, and (ii) enter into a formal agreement with the third party which ensures that the latter will provide the same level of protection and safeguards to the rights and freedoms of data subjects as that which is prescribed under the DPF Principles.

Tourmaline Partners, LLC may be exempt from entering into a formal data processing agreement (or the functional equivalent thereto) in the following situations:

- the receiving third party is a participating organization in and certified under the DPF and, where applicable, under the UK Extension to the DPF;
- the receiving third party is subject to laws and regulations under which it is obligated to confer safeguards and protection which are equivalent to those provided under the DPF Principles; and/or

- the receiving third party is an entity under the control of the Firm and is subject to other transfer tools as defined under Article 46 of GDPR, such as Binding Corporate Rules.

The Firm remains liable under the EU-U.S. DPF Principles for any losses and damages resulting from the processing of personal data by third parties unless it can prove that it is not responsible for such losses or damages being caused.

EU-U.S. Data Privacy Framework and the UK Extension

The Firm complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF as set forth by the U.S. Department of Commerce.

The Firm has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF.

The DPF and UK Extension to the DPF Annex I Binding Arbitration Mechanism is for EU/EEA and UK (or Gibraltar) individuals who seek to determine whether an organisation participating in the EU-U.S. DPF and, as applicable, the UK Extension to the EU-U.S. DPF has violated its obligations under the EU-U.S. DPF Principles as to that individual, and whether any such violation remains fully or partially unremedied.

As described in Annex I of the DPF Principles, the arbitral tribunal has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction deletion, or return of the individual's data in question) necessary to remedy the violation of the DPF Principles only with respect to the individual.

The option to invoke binding arbitration is subject to pre-dispute protocols. For more information, please visit the International Centre for Dispute Resolution's website at https://go.adr.org/dpfeufiling.html.

If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern.

To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

Retention

We will keep your Personal Data for no longer than reasonably necessary. We will retain your personal information in accordance with legal and regulatory requirements as set out in our Data retention policy.

Your rights and your Personal Data

You have a right:

- to request a copy of your Personal Data which the Firm or related Data Controller holds about you;

- to request the Firm or any related Data Controller to correct any Personal Data if it is found to be inaccurate or out of date;
- to request your Personal Data is erased where it is no longer necessary for the Firm or related Data Controller to retain such Data;
- to withdraw your consent to the Processing at any time if consent constitutes the lawful basis for processing;
- to object to Processing based on grounds relating to the Data Subject's situation if the processing is necessary for the performance of a task carried out in the public interest or the processing is necessary for the purposes of the legitimate interest by us or a third party, unless such interest is overridden by your fundamental rights and interests;
- to request a restriction is placed on further Processing;
- to lodge a complaint with the Information Commissioner's Office (the UK Supervisory Authority); you can contact the Information Commissioner's Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF;
- not to be subject to a decision based on automated Processing; the Firm does not practice such decision-making.

Further Processing

Where we may seek to further process your Data other than for the original purpose for which it was collected, the Firm shall only further process such Data where the new Processing is compatible with the original purpose.

Safeguarding measures

We take your privacy seriously and take every reasonable measure and precaution to protect and secure your Personal Data. We work hard to protect you and your information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures in place, including, without limitation, encryptions.

Special Categories of Data

Owing to the products and services that we offer, such as performance of brokerage services and other background checks, we sometimes need to process special categories of Data which are deemed to be more sensitive in nature. Where we collect such information, we will only request and process the minimum necessary for the specified purpose and identify a compliant legal basis for doing so. Where we rely on your consent for Processing Special Categories of Data, we will obtain your explicit consent through electronic means.

Legitimate Interests (if applicable)

We occasionally process your personal information under the Legitimate Interests' legal basis. Where this is the case, we have carried out a LIA to ensure that we have weighed your interests and any risk posed to you against our own and that such interests are proportionate and appropriate such as for the purposes of HR, marketing and day-to-day operations.

Marketing

When sending marketing materials to customers, we may have the option to rely on your consent or legitimate interest.

We only use legitimate interests for marketing if we have assessed that the information being sent is beneficial to the customer, and have weighed our interests against your own and there is little to no risk posed, the method and content is non-intrusive, and the material being sent is something you would usually expect to receive.

Cookies, analytics and traffic Data

Cookies are small text files which are transferred from our website, applications or services and stored on your device. We use cookies to help us provide you with a personalised service, and to help make our website, applications and services better for you.

We provide the following information with some explanations to ensure transparency to our users:

- what types of cookies are set;
- how long they persist on our user's browser;
- what Data they track;
- for what purpose (functionality, performance, statistics, marketing, etc.);
- where the Data is sent and with whom it is shared;
- how to reject cookies, and how to subsequently change the status regarding the cookies.

Changes to our Privacy Notice

Any changes we may make to our Privacy Notice in the future will be posted on this page and, where appropriate, you will be notified by email.

II. Privacy Notice (employees and prospect employees, to be placed in the handbook and /or emailed to the employees)

Overview

The Firm is fully committed to promoting privacy and ensuring the highest standards of Personal Data protection.

Personal Data of our employees consist of sensitive information and therefore the Firm puts particular emphasis on the security safeguards.

We have written this Privacy Notice, so the Firm's employees have a clear point of reference when it comes to how we process their Data.

For the purposes of the Data Protection Legislation, the Firm is a Data Controller in regard to the Personal Data of its employees – the Firm determines the means and purposes of Processing your Personal Data.

Please note that the Firm reserves the right to amend this notice at any time as this notice does not form part of your contract of employment.

What types of Personal Data do we collect?

Due to the nature of the employment relationship, the Firm processes a number of personal information which is more sensitive than other and falls under the category of Special Categories of Data.

Special Categories of Personal Data

Special Categories of Personal Data are Data revealing your 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.

We process Special Categories of Personal Data in order to carry out our legal obligations or exercise rights in connection with employment. If we need to process such Data in connection with anything other than employment, we shall seek your written consent. There are limited circumstances when we can process the Special Categories of Personal Data; when we need it in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

The Firm processes your health Data to:

- assess your fitness to work;
- ensure health and safety at work;
- provide appropriate workplace adjustments if applicable;
- administer maternity pay, statutory sick pay, pensions and permanent health insurance;
- assess entitlements under the share plan in relevant circumstances;
- assess your application for ill-health pension.

The Firm processes your Data revealing your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation to be able to appropriately monitor the equal opportunities obligations.

The Firm processes information about your trade union membership in order to comply with its obligations under the employment law.

Personal Data

The Firm also processes the following types of your Personal Data which do not constitute part of the Special Categories of Personal Data:

- information obtained during the recruitment process;
- name, title, addresses, telephone numbers, and personal email addresses;
- date of birth;
- gender;
- marital status and dependants;
- next of kin and emergency contact information;
- national Insurance number;
- bank account details, payroll records and tax status information;
- salary, annual leave, and benefits information;
- leaving date and your reason for leaving;
- place of work;
- copy of photo identification document;
- employment records (including job titles, work history, working hours, holidays, training records and professional memberships);
- evaluation of your performance;
- any disciplinary and grievance information;
- information obtained through electronic means such as swipe card records;
- record of your use of the Firm's communication channels.

How is your personal information collected?

We obtain your Personal Data:

- directly from you during the recruitment process;
- from employments agencies; or
- other third parties, such as former employers.

Legal basis for Processing of your Personal Data

The Firm processes your Personal Data lawfully and relies on the following basis for Processing:

- performance of the employment contract to which the Firm and you are parties when:
    - establishing and administering terms of your employment contract;
    - paying your wages;
    - providing benefits and bonuses;
    - conducting appraisals and performance reviews.

- legal obligation imposed on the Firm when:
    - checking you right to work;
    - preventing fraud and bribery;
    - complying with health and safety regulations.

- legitimate interest when:
    - analysing data in order to evaluate the business needs and performance;
    - defining your future terms of work;
    - conducting recruitment process.

Please note that the Firm shall inform you if the purpose of Processing of your Personal Data is to become incompatible with the originally defined purposes.

Automated decision-making

Automated decision-making means that the decision is taken using Personal Data processed solely by automatic means.

The Firm does not conduct automated decision-making, however, if that was to take place at any point in the future, then the Firm is entitled to do it when:

- we notify you of the decision and give you 21 days to request a reconsideration;
- automated decision-making is necessary to perform a contract to which you are a party to and we have put the security measures to do that safely; and
- you consent to it.

The Firm shall inform you in writing of such a decision process taking place.

Data sharing

The Firm may share your Personal Data with third parties where:

- it is required by law e.g., regulator, disclosures to shareholders and directors, or

- the third party supports exercising of the employment contract that the Firm and you are parties to, e.g. service providers, payroll, benefits provision and administration, IT services.

All our service providers are under the obligation to treat your Personal Data with the same level of security as we do.

Some of the providers may be outside of the UK and the EEA, however, they all are contractually obliged to implement the same security standards as the Firm's.

The third parties providers are prohibited to use your Personal Data for any other purposes than the ones which are compatible with the original purpose for Data Processing.

Onward transfers to third parties under the DPF

In accordance with the DPF Principles, Tourmaline Partners, LLC may transfer personal data onward to a third party provided that it (i) informs the data subject and obtain their consent for such a transfer, and (ii) enter into a formal agreement with the third party which ensures that the latter will provide the same level of protection and safeguards to the rights and freedoms of data subjects as that which is prescribed under the DPF Principles.

Tourmaline Partners, LLC may be exempt from entering into a formal data processing agreement (or the functional equivalent thereto) in the following situations:

- the receiving third party is a participating organization in and certified under the DPF and, where applicable, under the UK Extension to the DPF;
- the receiving third party is subject to laws and regulations under which it is obligated to confer safeguards and protection which are equivalent to those provided under the DPF Principles; and/or
- the receiving third party is an entity under the control of the Firm and is subject to other transfer tools as defined under Article 46 of GDPR, such as Binding Corporate Rules.

The Firm remains liable under the EU-U.S. DPF Principles for any losses and damages resulting from the processing of personal data by third parties unless it can prove that it is not responsible for such losses or damages being caused.

Data security

To ensure Data security, the Firm has implemented organisational and technical measures which are detailed in the Electronic Communication Policy, Data Protection Policy and Business Continuity and Recovery Plan.
These are available on request.

Data retention

The Firm will process your personal information for as long as necessary to fulfil the original purposes that they were collected for. These purposes may mean compliance with legal and accounting requirements.

The Firm maintains a separate Data Retention Schedule which details the exact retention periods. It is available on request.

Your rights under the Data protection legislation

- **Right to access** to your personal information enables you to receive a copy of the personal information we hold about you and to check the legal basis for Processing it.
- **Right to rectification** of the incorrect personal information that we hold about you.
- **Right to be forgotten** allows you to have your personal information deleted if the Firm has no legitimate reason to further process your Personal Data.
- **Right to object to Processing** of your personal information where we are relying on a legitimate

interest (or those of a third party) and there is something about your particular situation which makes you want to object to Processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- **Right to restriction of Processing** of your personal information allows you to request suspension of processing when the Processing is being contested.
- **Right to data portability** allows you to request your Data to be transmitted to another party in commonly used electronic format.

Please note that you are obliged to keep the Firm informed of any changes to your Personal Data.

If you wish to exercise any of the rights, please contact Tom Sisterson. The submission of the request is free of charge.

We may ask you for some form of verification of your identity in order to ensure that your Data is not disclosed to anyone else but you.

Right to withdraw consent

If basis for Processing is consent, you have the right to withdraw it at any point. Please contact Tom Sisterson in order to withdraw your consent for Processing of Personal Data.

Right to lodge a complaint with the Supervisory Authority

To lodge a complaint with the Information Commissioner's Office (the UK Supervisory Authority); you can contact the Information Commissioner's Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Right to escalate to complaints to the Arbitration Mechanism

The DPF and UK Extension to the DPF Annex I Binding Arbitration Mechanism is for EU/EEA and UK (or Gibraltar) individuals who seek to determine whether an organisation participating in the EU-U.S. DPF and, as applicable, the UK Extension to the EU-U.S. DPF has violated its obligations under the EU-U.S. DPF Principles as to that individual, and whether any such violation remains fully or partially unremedied.

As described in Annex I of the DPF Principles, the arbitral tribunal has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction deletion, or return of the individual's data in question) necessary to remedy the violation of the DPF Principles only with respect to the individual.

The option to invoke binding arbitration is subject to pre-dispute protocols. For more information, please visit the International Centre for Dispute Resolution's website at https://go.adr.org/dpfeufiling.html.

Changes to this Privacy Notice

We reserve the right to update this Privacy Notice at any time, and we will provide you with a new Privacy Notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this Privacy Notice, please contact Tom Sisterson at

ts@tourmalinellc.com