Data Protection Policy

Edition Date: May 2024

1. Introduction

Turley Associates Limited ("**we**", "**our**", "**us**", "**Turley**") will use Personal Data in accordance with data protection and privacy laws applicable to the us including, as applicable: the Data Protection Act 2018, the UK General Data Protection Regulation ("**UK GDPR**") and the General Data Protection Regulation (EU) 2016/679 ("**EU GDPR**") (all as amended, updated or re-enacted from time to time).**Note:** The EU GDPR is an EU Regulation and it no longer applies directly in the UK, except in certain circumstances. The EU GDPR may still apply directly to Turley where we operate in the European Economic Area ("**EEA**"), offer goods or services to individuals in the EEA, or monitor the behaviour of individuals in the EEA. Please speak to the Turley data protection contacts below is you require further information.

It is important for all our co-owners, workers and contractors ("**you**", "**your**") to understand the principles of the data protection legislation to enable us to comply with the law. This policy sets out the responsibilities of anyone who Processes Personal Data on behalf of Turley, including directors, full and part-time employees ("**co-owners**"), workers and contractors.

Breaching the UK GDPR can lead to fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, and/or claims for compensation. There is also a reputational risk of negative publicity. Any co-owners, workers and contractors failing to comply with the requirements of this policy may be subject to disciplinary action.

We rely on using Personal Data, amongst other things, so that staff can be paid, financial records maintained, our services monitored and regulated, client relationships fostered, and new business obtained. It is critical to our business that we are able to use Personal Data in this way. In order to continue to be able to do so, we must comply with our obligations under the data protection laws.

All co-owners, workers and contractors must familiarise themselves with this policy. Any questions or concerns about the interpretation or operation of this policy should be addressed to **Alison Browne (alison.browne@turley.co.uk)** or **Carol Maughan (carol.maughan@turley.co.uk)** in the first instance.

Further guidance on Turley's data protection procedures can be found on our intranet.

Content: This policy includes information on:

(a) The scope of the data protection legislation

(b) The data protection principles

(c) Lawfulness, fairness, transparency of data Processing

(d) Purpose limitation

(e) Data minimisation

(f) Accuracy

(g) Storage limitation

(h) Security, integrity and confidentiality

(i) Reporting a Personal Data Breach

(j) Transfer limitation

(k) Data Subject's rights and requests

(l) Accountability

(m) Direct marketing

(n) Definitions of key terms used in this policy

2. Scope of the data protection legislation

Data protection laws apply to many formats of information including information stored on computers and in certain manual (for example, paper) filing systems, if they are structured in a way that enables easy access to information about a Data Subject.

2.1 What is "Personal Data"?

Personal Data means any information relating to an identified or identifiable natural (living) person (a "**Data Subject**").

An identifiable natural person is someone 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 person.

We use Personal Data relating to a number of categories of Data Subject, including co-owners, clients, potential clients, business contacts, suppliers and contractors. For example Personal Data may include names, addresses, email addresses and telephone numbers; it may also include images in photographs or films and recorded telephone conversations.

There are special categories of Personal Data to which additional safeguards apply. These special categories of Personal Data include information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

Please refer to the "Public Consultation" page on Turley's intranet regarding procedures for Processing information provided during public consultations.

2.2 What does "Processing" Personal Data mean?

Processing has a broad definition and includes almost anything we might do with Personal Data, including obtaining, recording, organising, structuring, holding, using, disclosing and destroying Personal Data.

2.3 What are "Controllers" and "Processors"?

A Controller determines the purposes for which and the manner in which Personal Data are Processed. For example, Turley is a Controller in respect of Personal Data it holds relating to its Company Personnel. Turley is also a Controller in respect of certain Personal Data it holds relating to its clients (e.g. where the data is used to send billing, marketing and administrative information).

A Processor is any person (not an employee/co-owner of the Controller) who Processes Personal Data on behalf of the Controller. Turley uses Processors such as service providers who access our IT systems to provide support and maintenance service.

A Controller remains responsible for the use of Personal Data by a Processor in respect of the Personal Data it has passed to the Processor. We are also required to put in place a written contract with any Processors we use. Anyone wishing to appoint a Processor should first speak to Alison Browne (alison.browne@turley.co.uk) or Carol Maughan (carol.maughan@turley.co.uk) to ensure that an appropriate contract is used.

3. The data protection principles

We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner *(Lawfulness, Fairness and Transparency)*.

(b) Collected only for specified, explicit and legitimate purposes *(Purpose Limitation)*.

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed *(Data Minimisation)*.

(d) Accurate and where necessary kept up to date *(Accuracy)*.

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed *(Storage Limitation)*.

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage *(Security, Integrity and Confidentiality)*.

(g) Not transferred to another country without appropriate safeguards in place (*Transfer Limitation*).

(h) Made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (*Data Subject's Rights and Requests*).

(i) We are responsible for and must be able to demonstrate compliance with the data protection principles listed above *(Accountability)*.

4. Lawfulness, fairness, transparency

4.1 Lawfulness and fairness

Personal Data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The UK GDPR allows Processing for specific purposes, the most relevant of which are set out below:

(a) the Data Subject has given his or her Consent; or

(b) the Processing is necessary for the performance of a contract with the Data Subject; or

(c) to meet our legal compliance obligations; or

(d) to protect the Data Subject's vital interests; or

(e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we Process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

We have to identify and document these legal grounds we are relying on for each Processing activity.

4.2 Consent

A Controller must only Process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR, which include Consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

You will need to evidence Consent captured and keep records of all Consents so that we can demonstrate compliance with Consent requirements.

4.3 Transparency (notifying Data Subjects)

The UK GDPR requires Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Controller and relevant data protection manager accountable for data privacy, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

A checklist setting out the information that must be included in Privacy Notices is included at the end of this policy (**Appendix A**).

Please note Privacy Notices cannot be amended without consultation and agreement with Carol Maughan.

5. Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

6. Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with our data retention guidelines.

7. Accuracy

Personal Data must be accurate and, where necessary, kept up-to-date. It must be corrected or deleted without delay when inaccurate.

You must ensure that the Personal Data we use and hold is accurate, complete, kept up-to-date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

8. Storage limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is Processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

We will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

You must take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all Turley's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

You must ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

9. Security integrity and confidentiality

9.1 Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting special categories of Personal Data from loss and unauthorised access, use or disclosure (see Section 2.1 above for more information).

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is Processed.

(c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data.

Please also refer to the "IT GDPR Procedures" page on Turley's intranet for further details on the procedures to be followed.

10. Reporting a Personal Data Breach

The UK GDPR requires Controllers to notify any Personal Data Breach to the UK's regulator for data protection - the Information Commissioner's Office (ICO) - and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or the ICO where we are legally required to do so.

The UK GDPR introduces a duty on all organisations to report certain types of Personal Data Breach to the ICO. Turley must do this within 72 hours of becoming aware of the breach.

Common examples of events leading to Personal Data Breaches include (but are not limited to):

- misdirected email correspondence or documents;
- misplacing or theft of paperwork;
- inadequate disposal of information;
- leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information;
- loss or theft of laptop or mobile device;
- CDs/USBs missing in post;
- physical security e.g. forcing of doors or windows into secure area or restricted information left unsecured in accessible area;
- unauthorised use of a Turley login and password;
- attempts to gain unauthorised access to Turley systems and information i.e. hacking;
- virus or other malicious (suspected or actual) security attack on IT equipment systems or networks; or
- disruption to, failure or loss of access to information or services due to (non-exclusive list) fire, flood, power outage, cyber-attack or theft.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact Alison Browne (*alison.browne@turley.co.uk*) or Carol Maughan (carol.maughan@turley.co.uk) as the key point of contact for Personal Data Breaches. You should preserve all evidence relating to the potential Personal Data Breach.

11. Transfer limitation

11.1 Data sharing

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another co-owner, agent or representative of Turley (which includes our subsidiary) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions (see the section on **International transfers** below for more information on this).

You may only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains UK GDPR approved and, where relevant, EU GDPR approved third party clauses has been obtained.

11.2 International transfers

The UK GDPR restricts data transfers to countries outside the UK in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer Personal Data outside the UK if one of the following conditions applies:

(a) the UK Government 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' rights and freedoms, a list of countries where a decision has been issued is available at the ICO website;

(b) appropriate safeguards are in place, such as: binding corporate rules (BCR); standard contractual clauses approved for use in the UK; an approved code of conduct; or a certification mechanism applies;

(c) the Data Subject has provided Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the UK GDPR, including the performance of a contract between us 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 relation to the standard contractual clauses mentioned in (b) above, the ICO has issued two sets of standard data protection clauses for restricted transfers which Turley can use as its 'appropriate safeguard' under the UK GDPR:

(a) the International Data Transfer Agreement (IDTA); and

(b) an International Data Transfer Addendum (Addendum) – this is a UK addendum to the standard contractual clauses issued by the European Commission under the EU GDPR on 04 June 2021 (EU SCCs). The EU SCCs are not valid for restricted transfers under UK GDPR on their own but using the Addendum allows you to rely on the EU SCCs for your transfers under UK GDPR.

If there is a need to transfer Personal Data outside the UK (other than to our office in Dublin) you must contact Alison Browne (alison.browne@turley.co.uk) or Carol Maughan (carol.maughan@turley.co.uk) as this is restricted unless the specific legal conditions above are met.

12. Data Subject's rights and requests

Data Subjects have rights when it comes to how we handle their Personal Data.

These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Controller's Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the UK;

(i) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(j) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(k) make a complaint to the supervisory authority; and

(l) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to your supervisor and comply with Turley's Data Subject response process.

A summary of Data Subject's rights under the UK GDPR is included at the end of this policy (**Appendix B**).

13. Accountability

The Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

We must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

(a) appointing a data protection manager accountable for data privacy;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Data Protection Policy, Privacy Notices;

(d) regularly training Company Personnel on the UK GDPR, this Data Protection Policy, and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. We must maintain a record of training attendance by Company Personnel; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

13.1 Record keeping

The UK GDPR requires us to keep full and accurate records of all our data Processing activities. You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

These records should include, at a minimum, the name and contact details of the Controller and the relevant data protection manager accountable for data privacy, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

13.2 Training and audit

We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training in accordance with our mandatory training guidelines.

You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

13.3 Privacy by Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

(a) the state of the art;

(b) the cost of implementation;

(c) the nature, scope, context and purposes of Processing; and

(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

Controllers must also conduct DPIAs in respect to high risk Processing.

You should conduct a DPIA when implementing major system or business change programs involving the Processing of Personal Data including:

(e) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(f) large scale Processing of Sensitive Data; and

(g) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

(h) a description of the Processing, its purposes and the Controller's legitimate interests if appropriate;

(i) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

(j) an assessment of the risk to individuals; and

(k) the risk mitigation measures in place and demonstration of compliance.

14. Direct marketing

We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows us to send marketing texts or emails if we have obtained contact details in the course of a sale to that person, we are marketing similar products or services, and we gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

Please also refer to the “Events and GDPR” page on Turley’s intranet for further details on the procedures to be followed.

15. Definitions of key terms used in this policy

In this Data Protection Policy, the following terms shall mean as follows:

Company Personnel	all co-owners, workers, contractors, agency workers, consultants, directors, members and of Turley.
Consent	agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.
Controller	the person or organisation that determines when, why and how to Process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. Turley is the Controller of all Personal Data relating to its Company Personnel and Personal Data used in the business for its own commercial purposes.
Data Privacy Impact Assessment (DPIA):	tools and assessments used to identify and reduce risks of a data Processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.
Data Subject	a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.
EU GDPR	the General Data Protection Regulation (EU) 2016/679).
Personal Data	any information relating to an identified or identifiable natural, living, person (Data Subject). An identifiable natural person is someone 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 person. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
Personal Data Breach	any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.
Privacy by Design	implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.
Privacy Notices	separate notices setting out information that may be provided to Data Subjects when Turley collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee Privacy Notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.
Processing or Process	any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.
Pseudonymisation or Pseudonymised	replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.
UK GDPR	the retained EU law version of the General Data Protection Regulation ((EU) 2016/679), as defined in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

16. Changes to this Data Protection Policy

Alison Browne and Carol Maughan has been appointed to oversee compliance with this Data Protection Policy. If you have any questions about this Data Protection Policy or how we handle personal information, please contact alison.browne@turley.co.uk or carol.maughan@turley.co.uk**.**

We reserve the right to change this Data Protection Policy at any time so please check back regularly to obtain the latest copy of this Data Protection Policy. We will notify you when we update this policy.

Appendix A – Privacy Notice Checklist (UK GDPR-compliant)

✓	Information to include in Privacy Notice	Notes
	Turley's identity and contact details and details of our data protection representatives.	*Turley has nominated representatives for the purposes of the DPA/UK GDPR - alison.browne@turley.co.uk and carol.maughan@turley.co.uk.*
	Identity and contact details of the data protection officer (DPO).	*Turley is not legally obliged to appoint a DPO currently.*
	The purpose for the Processing.	*Avoid generalisations that are open to a variety of interpretations (e.g. "improving user experience", "marketing", "IT security", and "future research").*
	The legal basis for the Processing.	*Under the UK GDPR, it is more difficult to obtain consent and note that public authorities cannot use the legitimate interest basis for Processing.*
	Any legitimate interests that Turley is relying on.	*The recitals to the UK GDPR identify certain legitimate activities (e.g. Processing for preventing fraud, information security and intra-group transfers). However, this must be weighed against individuals' rights and freedoms.*
	The categories of Personal Data.*	
	Recipients or categories of recipients of the Personal Data.	*For example credit reference agencies.*
	Details of transfers outside the UK and any safeguards taken.	*The data transfer mechanism used to legalise the transfer must be specified.*
	The period for which data will be retained or the criteria used to determine this period.	
	Details of the Data Subject's rights.	*This includes the right to be forgotten, restrict Processing and to object to Processing, the right to data portability and the right to object to direct marketing.*
	The right to withdraw consent at any time (if consent is used as the basis for Processing).	*Include details of how the Data Subject can exercise the right.*
	The right to lodge a complaint with a supervisory authority.	*In the UK, this is the Information Commissioner's Office.*
	The source of the Personal Data (and whether it was a publicly accessible source).*	

	Whether the provision of Personal Data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the Personal Data.**
	Details of any automated decision making (eg, profiling), the auto-decision logic used, the significance and consequences.

* not needed where data is obtained directly from Data Subject

** only needed where data is obtained directly from Data Subject

Appendix B – Data Subject rights under the UK GDPR

Right provided by UK GDPR	Notes
Right to be informed **See our Privacy Notice checklist for the details required to be communicated to the Data Subject.**	If data is obtained **directly from the Data Subject**, the information should be provided at the time of collection of the data. If data is **not obtained directly** the information should be provided: ✓ within a reasonable period of obtaining the data (within one month); ✓ if the data are used to communicate with the Data Subject, at the latest, when the first communication takes place; and ✓ if disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
Right of access **Data subjects have the right to obtain:** ✓ **confirmation that their data is being Processed;** ✓ **access to their Personal Data; and** ✓ **other supplementary information – this largely corresponds to the information that should be provided in a Privacy Notice.**	Information must be provided **without delay** and at the latest within **one month of receipt**. Turley will be able to extend the period of compliance by a **further two months** where requests are complex or numerous. If so, Turley must inform the individual within one month and explain why. Where Turley Processes a **large quantity** of information about an individual, the UK GDPR permits Turley to ask the individual to **specify the information the request relates to**. Turley must provide a copy of the information **free of charge**. Turley can charge a **'reasonable fee':** ✓ when a request is manifestly **unfounded or excessive**, particularly if it is repetitive. Turley could also **refuse to respond** but, without undue delay and within one month, Turley would have to explain why and inform them of their right to complain and to a judicial remedy; or ✓ to comply with requests for **further copies** of the same information.
Right to rectification **Individuals are entitled to have Personal Data rectified if it is inaccurate or incomplete.**	Turley must respond within **one month** or, if the request is complex, this can be extended by **two months**. **If Turley is not taking any action**, Turley must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy. If Turley has disclosed the Personal Data to **third parties**, Turley must inform them of the rectification where possible and inform the Data Subject where appropriate.

Right to erasure **A Data Subject may request the erasure of Personal Data where:** **a) the Personal Data:** ✓ **is no longer necessary in relation to the purpose for which it was originally collected/Processed** ✓ **was unlawfully Processed** ✓ **has to be erased in order to comply with a legal obligation** ✓ **is Processed in relation to the offer of information society services to a child** **b) the individual:** ✓ **withdraws Consent** ✓ **objects to the Processing and there is no overriding legitimate interest for continuing the Processing**	Turley can **refuse to comply** with a request for erasure where the Personal Data is Processed: ✓ to exercise the right of freedom of expression and information; ✓ to comply with a legal obligation or for the performance of a public interest task or exercise of official authority; ✓ for public health purposes in the public interest; ✓ for archiving purposes in the public interest, scientific research historical research or statistical purposes; or ✓ for the exercise or defence of legal claims. If Turley has disclosed the Personal Data to **third parties**, Turley must inform them about the erasure of the Personal Data, unless it is impossible or involves disproportionate effort to do so.
Right to restrict Processing **Processing must be suppressed where:** ✓ **the individual contests the accuracy of the Personal Data;** ✓ **an individual has objected to the Processing (where it was necessary for performance of a public interest task or legitimate interests);** ✓ **Processing is unlawful and the individual requests restriction instead of erasure;** ✓ **Turley no longer needs the Personal Data but the individual requires the data to establish, exercise or defend a legal claim.**	Turley can continue to store the Personal Data, but **may only further Process it**: ✓ with the Data Subject's consent; ✓ to establish, exercise, or defend legal claims; ✓ to protect the rights of another individual or legal entity; or ✓ for important public interest reasons. Turley must inform individuals when Turley decide to **lift** a restriction on Processing. If Turley has disclosed the Personal Data to **third parties**, Turley must inform them about the restriction on the Processing of the Personal Data, unless it is impossible or involves disproportionate effort to do so.
Right to data portability **This includes the right to:** ✓ **receive a copy of the Personal Data, free of charge, from the Controller in a commonly used and machine-readable format and store it for further personal use on a private device;** ✓ **transmit the Personal Data to another Controller; and** ✓ **have Personal Data transmitted directly from one Controller to another where technically possible.**	The right to data portability only applies: ✓ to Personal Data that an **individual has provided** to a Controller; ✓ where the Processing is based on the individual's **consent or for the performance of a contract**; and ✓ when Processing is carried out by **automated means**. Turley must respond without undue delay and within **one month** or, if the request is complex or there are numerous requests, this can be extended by **two months**. Turley must **inform the individual of any extension** within one month of the receipt of the request and explain why it is necessary. **If Turley is not taking any action**, Turley must explain why to the individual, without undue delay and within one month, informing them of their right to complain to the supervisory authority and to a judicial remedy.

Right to object **Individuals have the right to object to:** ✓ **Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);** ✓ **direct marketing (including profiling); and** ✓ **Processing for purposes of scientific/historical research and statistics.**	If Processing for the performance of a legal task or legitimate interests, individuals must have an objection on "**grounds relating to his or her particular situation**". Turley must stop Processing the Personal Data unless: ✓ Turley can demonstrate **compelling legitimate grounds** for Processing, which override the interests, rights and freedoms of the individual; or ✓ the Processing is for the establishment, exercise or defence of **legal claims.** If Processing for the performance of a legal task or legitimate interests or for direct marketing purposes: ✓ Turley must inform individuals of their right to object **"at the point of first communication"** and in Turley's **Privacy Notice**. ✓ This must **be "explicitly brought to the attention** of the Data Subject and presented clearly and separately from any other information". If Processing for direct marketing purposes, there are no exemptions or grounds to refuse. If Turley receives an objection to Processing for direct marketing purposes: ✓ Turley must **stop Processing Personal Data for direct marketing** on receipt; and ✓ Turley must deal the objection **at any time** and free of charge. If Processing for research purposes, individuals must have "**grounds relating to his or her particular situation"** in order to object. Turley is **not required to comply with an objection** if Turley is conducting research where the Processing of Personal Data is **necessary for the performance of a public interest task**. If Turley's Processing activities fall into any of the specified categories and **are carried out online**, Turley must offer a way for individuals to object online.
Rights in relation to automated decision making and profiling **Individuals have the right not to be subject to a decision when:** ✓ **it is based on automated Processing; and** ✓ **it produces a legal effect or a similarly significant effect on the individual.**	The **right does not apply if** the decision: ✓ is necessary for entering into or performance of a contract between Turley and the individual; ✓ is authorised by law (eg for the purposes of fraud or tax evasion prevention); ✓ is based on explicit consent (Article 9(2)); or ✓ does not have a legal or similarly significant effect on the individual. Turley must ensure that individuals are able to: ✓ obtain human intervention; ✓ express their point of view; and obtain an explanation of the decision and challenge it.

Breach Notification Right **When a Personal Data Breach is likely to result in a high risk to a Data Subject's rights, a Controller must notify the Data Subject of the security breach without undue delay.**	The breach must be notified without undue delay.