**GDPR Policy – Paul David Process Ltd**

**1 Personal Data**

The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way we collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to any specific individual.

**2 Principles**

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

*“a) processed lawfully, fairly and in a transparent manner in relation to individuals;*

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

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

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

*e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and*

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

*Article 5(2) requires that:*

*“the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”*

**3 Compliance**

We review the purposes of our processing activities and select the most appropriate lawful basis (or bases) for each activity. We check that the processing is necessary for the relevant purpose and ensure we are satisfied that there is no other reasonable way to achieve that purpose. We document our decision on which lawful basis applies to help us demonstrate compliance. We include information about both the purposes of the processing and the lawful basis for the processing in any privacy notice issued. If/When we process special category data, we identify a condition for processing the special category data and document this. If/When we process criminal offence data, we also identify a condition for processing this data and have documented this.

**4 Documentation**

The GDPR requires that we clearly document our lawful basis to demonstrate our compliance in line with Articles 5(2) and 24. This has been done in Appendix 1 of this document. Appendix 1 will be reviewed and updated as and when appropriate but at least annually.

We will inform people upfront about our lawful basis for processing their personal data. We will include this information in all privacy notices.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever we process personal data:

(a) Consent: the individual has given clear consent for us to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone’s life.

(e) Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests.

**Consent**

Where we rely on consent to hold information; we check that consent is the most appropriate lawful basis for processing. We make the request for consent prominent and separate from our terms and conditions. We ask people to positively opt in. We don’t use pre-ticked boxes or any other type of default consent. We use clear, plain language that is easy to understand. We specify why we want the data and what we’re going to do with it. We give separate distinct (‘granular’) options to consent separately to different purposes and types of processing. We name our organisation and any third party controllers who will be relying on the consent. We tell individuals they can withdraw their consent. We ensure that individuals can refuse to consent without detriment. We avoid making consent a precondition of a service

**Contract**

We will hold information on this lawful basis if we need to process someone’s personal data:

* To fulfil our contractual obligations to them; or
* Because they have asked us to do something before entering into a contract (eg provide a quote).

We will not hold data under this basis that is not reasonably necessary to perform these tasks.

**Legal Obligation**

We will rely on this basis when we are obliged to process the personal data to comply with the law.

Article 6(3) requires that the legal obligation must be laid down by UK or EU law. Recital 41 confirms that this does not have to be an explicit statutory obligation, as long as the application of the law is foreseeable to those individuals subject to it. So it includes clear common law obligations.

We will reference the specific legal provision or point to an appropriate source of advice or guidance that sets it out clearly. For example, referring to the HMRC website or to industry guidance that explains generally applicable legal obligations.

**Vital Interest**

We will rely on vital interests as our lawful basis only if we need to process the personal data to protect someone’s life. If we can reasonably protect the person’s vital interests in another less intrusive way, this basis will not apply. We will not rely on vital interests for health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.

**Public Task**

We will rely on this lawful basis if we need to process personal data ‘in the exercise of official authority’. This covers public functions and powers that are set out in law; or to perform a specific task in the public interest that is set out in law. If we could reasonably perform our tasks or exercise our powers in a less intrusive way, this lawful basis will not apply.

**Legitimate Interests**

We check that ‘legitimate interests’ is the most appropriate basis. We protect the individual’s interests. We conduct a ‘legitimate interests assessment’ (LIA) and keep a record of it, to ensure that we can justify our decision. We identify the relevant legitimate interests. We check that the processing is necessary and there is no less intrusive way to achieve the same result. We carry out a balancing test and ensure individual’s interests do not override those legitimate interests. We only use individuals’ data in ways they would reasonably expect, unless we have a very good reason. We are not using people’s data in ways they would find intrusive or which could cause them harm, unless we have a very good reason. We consider safeguards to reduce the impact where possible. We consider whether we can offer an opt out. If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA. We keep our LIA under review and repeat it if circumstances change. We include information about our legitimate interests in our privacy information.

**Special Data/Criminal Offence Data**

Special category data is more sensitive, and so needs more protection. For example, information about an individual’s:

* race
* ethnic origin
* politics
* religion
* trade union membership
* genetics
* biometrics (where used for ID purposes)
* health
* sex life
* sexual orientation.

This type of data could create more significant risks to a person’s fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

We will only hold data where the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

We will process this data:

* Where it 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 Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
* Where it 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.
* Where it is for legitimate activities, with appropriate safeguards, and will not disclose it outside our organisation without the consent of the data subjects.
* Where it relates to personal data which are manifestly made public by the data subject.
* Where it is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
* Where it is necessary for reasons of substantial public interest, on the basis of Union or Member State law 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.
* Where it 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 Union or Member State law or pursuant to contract with a health professional.
* Where it 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 Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
* Where it 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 Union or Member State law 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.

**5 Individual Rights**

**The Right to be Informed**

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. We will provide individuals with information including: our purposes for processing their personal data, our retention periods for that personal data, and who it will be shared with. We call this ‘privacy information’. We will provide privacy information to individuals at the time we collect their personal data from them. If we obtain personal data from other sources, we will provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month. There are a few circumstances when we do not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.

When obtaining personal data from other sources, we do not need to provide individuals with privacy information if:

1. the individual already has the information;
2. providing the information to the individual would be impossible;
3. providing the information to the individual would involve a disproportionate effort;
4. providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing;
5. we are required by law to obtain or disclose the personal data; or
6. we are subject to an obligation of professional secrecy regulated by law that covers the personal data.

The information we provide to people will be concise, transparent, intelligible, easily accessible, and use clear and plain language.

We will regularly review, and where necessary, update our privacy information. We will bring any new uses of an individual’s personal data to their attention before we start processing it.

We will provide individuals with the following privacy information:

* The name and contact details of our organisation.
* The name and contact details of our representative (if applicable).
* The contact details of our data protection officer (if applicable).
* The purposes of the processing.
* The lawful basis for the processing.
* The legitimate interests for the processing (if applicable).
* The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).
* The recipients or categories of recipients of the personal data.
* The details of transfers of the personal data to any third countries or international organisations (if applicable).
* The retention periods for the personal data.
* The rights available to individuals in respect of the processing.
* The right to withdraw consent (if applicable).
* The right to lodge a complaint with a supervisory authority.
* The source of the personal data (if the personal data is not obtained from the individual it relates to).
* The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
* The details of the existence of automated decision-making, including profiling (if applicable).

**Right of Access**

Individuals have the right to access their personal data and supplementary information so that they are aware of and can verify the lawfulness of the processing. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

Under the GDPR, individuals 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 (see Article 15).

We will provide a copy of the information, free of charge, within one month of receipt.

We may extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, we will inform the individual within one month of the receipt of the request and explain why the extension is necessary. We also retain the right to charge a ‘reasonable fee’ when a request is manifestly unfounded or excessive, particularly if it is repetitive, and to charge a reasonable fee to comply with requests for further copies of the same information based on the administrative cost of providing the information. Where we are asked to process a large quantity of information about an individual we will ask the individual to specify the information the request relates to.

If the request is manifestly unfounded or excessive we may refuse to respond but will explain why. We will inform the person making the request of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

We will always verify the identity of the person making the request, using ‘reasonable means’.

If the request is made electronically, we may provide the information in a commonly used electronic format.

**Right to Rectification**

We will rectify, or complete information, or provide a supplementary statement, when required. We inform any recipients if we rectify any data we have shared with them.

**Right to Erasure**

We will respond to a request for erasure without undue delay and within one month of receipt. We can extend the time limit to respond to a request where the information is excessive. We inform any recipients if we erase any data we have shared with them. We have appropriate methods in place to erase information.

**Right to Restrict Processing**

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, we will store the personal data, but not use it. An individual can make a request for restriction verbally or in writing. We will respond within one calendar month.

**Right to Data Portability**

The right to data portability only applies to personal data 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.

Where possible we will respond to requests for transfer of data in a structured, commonly used and machine-readable form (such as CSV files) free of charge. If the individual requests it, we may transmit the data directly to another organisation **if this is technically feasible**. We will normally respond without undue delay, and within one month. This can be extended by two months where the request is complex, or we receive a number of requests. If an extension is necessary; we will inform the individual within one month of the receipt of the request and explain why. If the personal data concerns more than one individual; we must consider whether providing the information would prejudice the rights of any other individual. Where we decide not to take action in response to a request, we will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

**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 a person expresses their right to object to personal data being used for the performance of a legal task or my organisation’s legitimate interests it must be on “grounds relating to his or her particular situation”. We will stop processing the personal data unless:

* we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
* the processing is for the establishment, exercise or defence of legal claims.

We will inform individuals of their right to object “at the point of first communication” and in our privacy notice. This will be explicitly brought to the attention of the data subject and will be presented clearly and separately from any other information.

We will deal with an objection to processing for direct marketing at any time and free of charge. We will stop processing personal data for direct marketing purposes as soon as we receive an objection. There are no exemptions or grounds to refuse.

Where any processing activities are carried out online we will offer a way for individuals to object online.

**Rights related to automated decision making including profiling**

We do not currently undertake any automated decision-making services but will review this policy if we introduce such services in the future.

**6 Accountability and Governance**

**Contracts**

When entering into a contract we will ensure the processor only acts on the written instructions of the controller (unless required by law to act without such instructions). The processor will ensure that people processing the data

* are subject to a duty of confidence
* take appropriate measures to ensure the security of processing
* only engage a sub-processor with the prior consent of the data controller and a written contract
* assist the data controller in providing subject access and allowing data subjects to exercise their rights and obligations under the GDPR, to the security of processing, the notification of personal data breaches and data protection impact assessments
* delete or return all personal data to the controller as requested at the end of the contract; and
* submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

**Document Control**

The GDPR contains explicit provisions about documenting processing activities. We must maintain records on several things such as processing purposes, data sharing and retention. We may be required to make the records available to the ICO on request. Controllers and processors both have documentation obligations.

For small and medium-sized organisations, such as our own, documentation requirements are limited to certain types of processing activities but records must be kept in writing and can be maintained electronically. Records must be kept up to date and reflect our current processing activities. As we have fewer than 250 employees, we only need to document processing activities that:

* are not occasional; or
* could result in a risk to the rights and freedoms of individuals; or
* involve the processing of special categories of data or criminal conviction and offence data.

We will ensure the controller for the personal data we process documents all the applicable information under Article 30(1) of the GDPR.

We will ensure the processor for the personal data we process, documents all the applicable information under Article 30(2) of the GDPR.

Article 30 requires that we record

1. The name and contact details of our organisation (and where applicable, of other controllers, your representative and your data protection officer).
2. The purposes of our processing.
3. A description of the categories of individuals and categories of personal data.
4. The categories of recipients of personal data.
5. Details of your transfers to third countries including documenting the transfer mechanism safeguards in place.
6. Retention schedules.
7. A description of our technical and organisational security measures.

As part of our record of processing activities, it can be useful to document (or link to documentation of) other aspects of your compliance with the GDPR and the UK’s Data Protection Bill. Such documentation may include:

1. information required for privacy notices, such as:

* the lawful basis for the processing
* the legitimate interests for the processing
* individuals’ rights
* the existence of automated decision-making, including profiling
* the source of the personal data
* records of consent
* controller-processor contracts
* the location of personal data
* Data Protection Impact Assessment reports
* records of personal data breaches

1. information required for processing special category data or criminal conviction and offence data under the Data Protection Bill, covering:

* the condition for processing in the Data Protection Bill
* the lawful basis for the processing in the GDPR
* our retention and erasure policy document.

If we process special category or criminal conviction and offence data, we will document:

* the condition for processing we rely on in the Data Protection Bill;
* the lawful basis for our processing; and
* whether we retain and erase the personal data in accordance with our policy document.

**Data Protection Officer**

We do not need to appoint a Data Protection Officer as

* we are not a public authority
* our core activities do not require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking)
* our core activities do not consist of large scale processing of special categories of data or data relating to criminal convictions and offences

If you wish to contact us about your personal data please address your correspondence to The Directors

**7 Security**

Article 5(1)(f) of the GDPR concerns the ‘integrity and confidentiality’ of personal data. It says that personal data shall be:

*'Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'*

We refer to this as the GDPR’s ‘security principle’. It concerns the broad concept of information security.

*Article 32(1) states:*

*‘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’*

Poor information security leaves systems and services at risk and may cause real harm and distress to individuals.

We undertake an analysis of the risks presented by our processing, and use this to assess the appropriate level of security we need to put in place. When deciding what measures to implement, we take account of the state of the art and costs of implementation. We have an information security policy (or equivalent) and take steps to make sure the policy is implemented. Where necessary, we have additional policies and ensure that controls are in place to enforce them. We make sure that we regularly review our information security policies and measures and, where necessary, improve them. We have put in place basic technical controls and understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process. We will use encryption and/or pseudonymisation where it is appropriate to do so. We understand the requirements of confidentiality, integrity and availability for the personal data we process.

We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process. We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement. Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism. We ensure that any data processor we use also implements appropriate technical and organisational measures.

This means that you must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. You should remember that while information security is sometimes considered as cybersecurity (the protection of your networks and information systems from attack), it also covers other things like physical and organisational security measures.

Information security is important, not only because it is itself a legal requirement, but also because it can support good data governance. The ICO is also required to consider the technical and organisational measures that were in place when considering an administrative fine.

We will ensure that data can be accessed, altered, disclosed or deleted only by those you have authorised to do so (and that those people only act within the scope of the authority you give them); that the data we hold is accurate and complete in relation to why we are processing it; and the data remains accessible and usable, ie, if personal data is accidentally lost, altered or destroyed, we can recover it and therefore prevent any damage or distress to the individuals concerned.

Technical measures are sometimes thought of as the protection of personal data held in computers and networks. Whilst these are of obvious importance, many security incidents can be due to the theft or loss of equipment, the abandonment of old computers or hard-copy records being lost, stolen or incorrectly disposed of. Technical measures therefore include both physical and computer or IT security.

When considering physical security, we have looked at:

* the quality of doors and locks, and the protection of your premises by such means as alarms, security lighting or CCTV;
* how you control access to your premises, and how visitors are supervised;
* how you dispose of any paper and electronic waste; and
* how you keep IT equipment, particularly mobile devices, secure.
* In the IT context, technical measures may sometimes be referred to as ‘cybersecurity’. This is a complex technical area that is constantly evolving, with new threats and vulnerabilities always emerging. It may therefore be sensible to assume that your systems are vulnerable and take steps to protect them.

When considering cybersecurity, we have looked at factors such as:

* system security – the security of your network and information systems, including those which process personal data;
* data security – the security of the data you hold within your systems, eg ensuring appropriate access controls are in place and that data is held securely;
* online security – eg the security of your website and any other online service or application that you use; and
* device security – including policies on Bring-your-own-Device (BYOD) if you offer it.

**8 International Transfers**

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined. We do not transfer personal data outside of the UK.

**9 Personal Data Breaches**

We have in place a process to assess the likely risk to individuals as a result of a breach. We will contact the relevant supervisory authority for our processing activities and notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet. We will inform affected individuals, without undue delay, about a breach when it is likely to result in a high risk to their rights and freedoms. We will provide affected individuals with advice to help them protect themselves from its effects. We document all breaches, even if they don’t all need to be reported.