

GDPR STATEMENT

The **EU General Data Protection Regulation (GDPR)** is the most important change in data privacy regulation in 20 years. It replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy.

Organizations in non-compliance from 25th May 2018 may face heavy fines.

GDPR applies to the processing and holding of personal data of data subjects residing in the European Union, by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not.

Personal data can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

A **Data Controller** is the entity that determines the purposes, conditions and means of the processing of personal data. A **Data Processor** is an entity which processes personal data on behalf of the controller.

Whenever a Data Controller uses a Data Processor it needs to have a written contract in place. Under the GDPR a Data Processor can only act on the documented instructions of a Data Controller.

Our Clients are normally the **Data Controller**. Kent Payroll Bureaus Ltd is normally the **Data Processor**.

Information we hold. Where it came from. Who we share it with.

Information we hold is limited to personal data that is required to process payroll and pension. If we incidentally acquire any additional information it will be ignored.

The information we hold may come from the Data Controller (Client), HMRC, Pension Scheme Provider, or other authorised third parties such as Child Maintenance Service, Student Loans Company, County Court or similar .

The information we hold is only shared with parties as required for payroll and pension processing, e.g. Data Controller (Client), HMRC, Pension Scheme Provider, or other authorised third parties such as Child Maintenance Service, Student Loans Company, County Court or similar .

Our responsibilities as data processors include

- a duty to maintain records of all processing activities
- a duty to identify and document under what basis we are processing data
- a duty to inform our data controller if there is a breach.

Subject matter and duration of the processing

Personal Data which is necessary to render the services of payroll & pension processing, for the duration of our engagement, and beyond where required by authorised third parties such as HMRC, County Courts.

Nature and purpose of the processing

Processing the data may include, but not be limited to; collection, recording, extraction, disclosure by transmission, erasure, disclosure. The data is processed for the purpose of payroll & pension processing.

Type of personal data and categories of data subject

Personal data may include, but is not limited to; title, name, address, telephone, email, sex, marital status, previous surname, date of birth, nationality, ethnic origin, disability, national insurance number, job title, pay rates.

The obligations and rights of the controller

The Controller shall be solely responsible for assessing the admissibility of the processing requested and for the rights of affected parties. The Controller shall immediately notify the Processor if he finds any errors or irregularities when reviewing the results of the processing.

Terms

As processor we will;

- only act on the written instructions of the controller (unless required by law to act without such instructions);
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- not engage a sub-processor without 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 under the GDPR;
- assist the data controller in meeting its GDPR obligations in relation 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 we are both meeting our Article 28 obligations, and tell the controller immediately if we are asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Processors' responsibilities and liabilities checklist

In addition to the Article 28.3 contractual obligations set out in the controller and processor contracts checklist, as a processor we have the following direct responsibilities under the GDPR. As processor we must;

- only act on the written instructions of the controller (Article 29);
- not use a sub-processor without the prior written authorisation of the controller (Article 28.2);
- co-operate with supervisory authorities (such as the ICO) in accordance with Article 31;
- ensure the security of our processing in accordance with Article 32;
- keep records of our processing activities in accordance with Article 30.2;
- notify any personal data breaches to the controller in accordance with Article 33;
- employ a data protection officer if required in accordance with Article 37; and
- appoint (in writing) a representative within the European Union if required in accordance with Article 27.

As a processor;

- we may be subject to investigative and corrective powers of supervisory authorities (such as the ICO) under Article 58 of the GDPR;
- if we fail to meet our obligations, we may be subject to an administrative fine under Article 83 of the GDPR;
- if we fail to meet our GDPR obligations we may be subject to a penalty under Article 84 of the GDPR; and
- if we fail to meet our GDPR obligations we may have to pay compensation under Article 82 of the GDPR.

As a matter of good practice

- nothing within the contract relieves us of our own direct responsibilities and liabilities under the GDPR; and
- reflect any indemnity that has been agreed.

More information can be found on the GDPR Portal;

<https://www.eugdpr.org/>

Licensed & Regulated by

AAT under Licence Number 5927

Qualified by

The Chartered Institute of Payroll Professionals
Association of Accounting Technicians
Institute of Certified Bookkeepers

Registered Address

Kent Payroll Bureaus Ltd
Little Etchden, Etchden Road
Bethersden
Ashford, Kent
TN26 3DS

Registered in England & Wales Company Number 08261179
Vat Number GB 237 3002 41