

UK General Data Protection Regulation (UK GDPR)
as supplemented by **The Data Protection Act 2018 (DPA 2018)**

The **EU General Data Protection Regulation (EU-GDPR)** of 25th May 2018, was the most important change in data privacy regulation in 20 years. It replaced the UK's **Data Protection Act (DPA) 2018** and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy.

As a result of Brexit, from 1st January 2021 the UK stopped being part of the EU so EU-GDPR ceased to protect the rights and freedoms of UK Citizens regarding Personal Information. To prevent this, the UK Government published an update to the **DPA 2018**, called the '**Data Protection, Privacy and Electronic Communication**'.

The **DPA 2018** controls how personal information is used by organisations, businesses or the government.

Personal data only includes information relating to natural persons who can be identified, or who are identifiable, directly from the information in question, or who can be identified from that information in combination with other information. For example, a name, a photo, an email address, bank details, posts on social networking websites, medical information, a computer IP address or cookie identifier.

Everyone responsible for using personal data has to follow strict rules called '**data protection principles**'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

Under the Data Protection Act 2018, citizens have the right to find out what information the government and other organisations store about them. These include the right to:

- be informed about how their data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of their data
- data portability (allowing them to get and reuse their data for different services)
- object to how their data is processed in certain circumstances

They also have rights when an organisation is using their personal data for:

- automated decision-making processes (without human involvement)
- profiling, for example to predict behaviour or interests

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. 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 obligations, and tell the controller immediately if we are asked to do something infringing the UK GDPR or other data protection law.

Processors' responsibilities and liabilities checklist

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

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

As a processor;

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

As a matter of good practice

- nothing within the contract relieves us of our own direct responsibilities and liabilities under the Data Protection Act 2018; and
- reflect any indemnity that has been agreed.

More information can be found on the **Information Commissioner's Office (IC) Website;**
<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/>

Licensed & Regulated by

AAT under Licence Number 5927

Qualified by

The Chartered Institute of Payroll Professionals
Association of Accounting Technicians

Registered Address

Kent Payroll Bureaus Ltd
Little Etchden
Bethersden
Kent TN26 3DS

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