Checklists

Controller and processor contracts checklist

Our contracts include the following compulsory details:

☐ the subject matter and duration of the processing;

☐ the nature and purpose of the processing;

☐ the type of personal data and categories of data subject; and

☐ the obligations and rights of the controller.

Our contracts include the following compulsory terms:

☐ the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);

☐ the processor must ensure that people processing the data are subject to a duty of confidence;

☐ the processor must take appropriate measures to ensure the security of processing;

☐ the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;

☐ the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;

☐ the processor must 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;

☐ the processor must delete or return all personal data to the controller as requested at the end of the contract; and

☐ the processor must 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.

As a matter of good practice, our contracts:

☐ state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR; and

☐ reflect any indemnity that has been agreed.

Processors' responsibilities and liabilities checklist

In addition to the Article 28.3 contractual obligations set out in the controller and processor contracts checklist, a processor has the following direct responsibilities under the GDPR. The processor 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 its processing in accordance with Article 32;

☐ keep records of its 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.

A processor should also be aware that:

☐ it may be subject to investigative and corrective powers of supervisory authorities (such as the ICO) under Article 58 of the GDPR;

☐ if it fails to meet its obligations, it may be subject to an administrative fine under Article 83 of the GDPR;

☐ if it fails to meet its GDPR obligations it may be subject to a penalty under Article 84 of the GDPR; and

☐ if it fails to meet its GDPR obligations it may have to pay compensation under Article 82 of the GDPR.