ICO GDPR guidance:

Contracts and liabilities between controllers and processors

ico.
Information Commissioner's Office

Contents (for web navigation bar)

At a glance

- Whenever a controller uses a processor it needs to have a written contract in place.
- The contract is important so that both parties understand their responsibilities and liabilities.
- The GDPR sets out what needs to be included in the contract.
- In the future, standard contract clauses may be provided by the European Commission or the ICO, and may form part of certification schemes. However at the moment no standard clauses have been drafted.
- Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. In the future, using a processor which adheres to an approved code of conduct or certification scheme may help controllers to satisfy this requirement – though again, no such schemes are currently available.
- Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

About this guidance

These pages sit alongside our Overview of the GDPR and provide more detailed, practical guidance for UK organisations on contracts between controllers and processors under the GDPR.

Under the GDPR, when a controller uses a processor it needs to have a written contract (or other legal act) in place to evidence and govern their working relationship.

If you are a controller, this guidance will help you to understand what needs to be included in that contract and why. It will also help processors to understand their responsibilities and liability.

The guidance sets out how the ICO interprets the GDPR, and our general recommended approach to compliance and good practice.

However, as the GDPR is a regulation that applies consistently across the EU, our guidance will need to evolve to take account of future guidelines issued by relevant European authorities, as well as our experience of applying the law in practice from May 2018. We intend to keep this guidance under review and update it in light of relevant developments and stakeholders' feedback.

You can navigate back to the Overview at any time using the link on the left-hand side of this page. We also give links throughout to other relevant guidance and sources of further information.

Key GDPR provisions
See Articles 28, 29, 30, 31, 32, 33, 34, 35 and 36 and Recitals 81, 82 and 83. (external link)

Further reading

Overview of the GDPR

What's new?

In brief….

- The GDPR makes written contracts between controllers and processors a general requirement, rather than just a way of demonstrating compliance with the seventh data protection principle (appropriate security measures) under the DPA.
- These contracts must now include certain specific terms, as a minimum.
- These terms are designed to ensure that processing carried out by a processor meets all the requirements of the GDPR (not just those related to keeping personal data secure).
- The GDPR allows for standard contractual clauses from the EU Commission or a supervisory authority (such as the ICO) to be used in contracts between controllers and processors - though none have been drafted so far.
- The GDPR envisages that adherence by a processor to an approved code of conduct or certification scheme may be used to help controllers demonstrate that they have chosen a suitable processor. Standard contractual clauses may form part of such a code or scheme, though again, no schemes are currently available.
- The GDPR gives processors responsibilities and liabilities in their own right, and processors as well as controllers may now be liable to pay damages or be subject to fines or other penalties.

Is this a big change?

This depends on what your existing contracts say about processing.

If you currently employ a third party to process personal data on your behalf then you should already have a written contract in place, as you need one to comply with the seventh principle (security measures) of the Data Protection Act 1998 (DPA). Your existing contract should require your data processor to only

act upon your instructions and to take appropriate measures to keep the personal data secure.

Under the GDPR, the contract requirements are wider and are no longer confined to just ensuring the security of personal data. They are aimed at ensuring and demonstrating compliance with all the requirements of the GDPR. The GDPR sets out specific terms that must be included in your contract, as a minimum.

The contract must state details of the processing, and must set out the processor's obligations. This includes the standards the processor must meet when processing personal data and the permissions it needs from the controller in relation to the processing.

This is a significant change in what is required by law, but in practice you may already include many of the new contract requirements in your existing contracts, for commercial reasons or as good practice under the DPA.

The GDPR also allows you to use standard contractual clauses issued by the European Commission or a supervisory authority (such as the ICO). Such standard clauses can form part of a certification scheme or approved code of conduct. Again this is a significant change in the law, but, initially at least, it should make little difference in practice, as no standard clauses are currently available.

Similarly, the GDPR allows you to use adherence by a processor to an approved code of conduct or certification scheme. This will help you demonstrate that you have chosen a processor providing 'sufficient guarantees' that it will process the personal data in accordance with the GDPR. But again no such schemes have been approved so far so, initially at least, this should make little difference in practice.

What is very different under the GDPR, however, is that processors now have direct responsibilities and obligations under the GDPR, outside the terms of the contract. Processors can be held directly responsible for non-compliance with these obligations, or the contract terms, and may be subject to administrative fines or other sanctions and liable to pay compensation to data subjects.

Key GDPR provisions
See Articles 28, 82 and 83 and Recitals 81, 146 and 148. (external link)

What are the key changes to make in practice? What do we need to do?

Any contracts in place on 25 May 2018 will need to meet the new GDPR requirements.

You should therefore check your existing contracts to make sure they contain all the required elements. If they don't, you should get new contracts drafted and signed. You should review all template contracts you use.

It would also be prudent to make sure that your processor understands the reasons for the changes and the new obligations that the GDPR puts on it. Your processor should understand that it may be subject to an administrative fine or other sanction if it does not comply with its obligations.

Key GDPR provisions
See Articles 28 and 29 and Recital 81. (external link)

When is a contract needed?

In brief…

- Whenever a controller uses a processor (a third party who processes personal data on behalf of the controller) it needs to have a written contract in place.
- Similarly, if a processor employs another processor it needs to have a written contract in place.

What does the GDPR say about when a contract is needed?

The GDPR states at Article 28.3 that

> Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller ……

This means that you need a written contract every time you employ a processor to process personal data. This includes both:

- when you directly employ a processor; and
- when a processor, with your written authority, employs another processor.

Although the GDPR refers to a contract 'or other legal act', in practice, in the UK, contracts are likely to be the appropriate means of complying with Article 28.3.

Key GDPR provisions
See Articles 28.3, 28.4 and 28.9 and Recital 81. (external link)

What is the difference between a controller and a processor?

The GDPR says that:

- a controller is a natural or legal person or organisation which determines the purposes and means of processing personal data; and

- a processor is a natural or legal person or organisation which processes personal data on behalf of a controller.

If you are not sure whether you are a controller or a processor, please refer to our guidance Data controllers and data processors. Although it is based on the Data Protection Act 1998 (DPA), the parts of the guidance setting out how to determine who is the controller and who is the processor are still relevant under the GDPR.

Key provisions in the GDPR
Articles 4(2), 4(7) and 4(8) (external link).

Further reading
Data controllers and data processors (DPA guidance)

When are processors used?

In both the private and public sectors, it is common practice for a controller to engage a processor to process personal data on its behalf.

Examples

- A specialist private company provides software and data analysis to process the daily pupil attendance records of a state maintained school for an annual fee.
- A public body uses a private company to administer and carry out assessments of individuals in relation to certain state benefits.
- The readers of a monthly science magazine receive a hard copy delivered to their home. Their subscriptions and the mailings are handled by a company which is separate from the magazine publisher, and it does so at the publisher's request.
- A marketing company sends promotional vouchers to a hairdresser's customers on the hairdresser's behalf.

What is a sub-processor and when are they used?

A processor might decide to use another processor to process personal data on its behalf. For shorthand this is sometimes referred to as using a 'sub-processor', although this is not a term taken from the GDPR itself. Before employing a sub-processor, the original processor must inform you, as the controller, and obtain your written permission.

Example

The readers of a monthly science magazine receive a hard copy delivered to their home. The subscriptions are handled by a company which is separate from the magazine publisher. Rather than arranging the mailings itself, the subscription company uses a different company as sub-processor to administer the mailing list and arrange the mailings to subscribers.

Key GDPR provisions
See Articles 28.1, 28.2, 28.3 and 28.4 and Recital 81. (external link)

Why are contracts between controllers and processors important?

In brief ….

Contracts between controllers and processors:

- ensure that they both understand their obligations, responsibilities and liabilities;
- help them to comply with the GDPR;
- help controllers to demonstrate their compliance with the GDPR; and
- may increase data subjects' confidence in the handling of their personal data.

The GDPR imposes a legal obligation on both parties to formalise their working relationship. Aside from the legal requirements, this makes practical and commercial sense.

By having a contract in place with the required terms:

- you are ensuring that you are complying with the GDPR;
- you are protecting the personal data of customers, staff and others; and
- both parties are clear about their role in respect of the personal data that is being processed and there is evidence of this.

The contract should set out what the processor is expected to do with the data.

Data subjects may be reassured by the fact a formal contract exists between those handling their personal data, setting out their obligations, responsibilities and liabilities. It also indicates to other organisations the professionalism of your business and the standard of your services.

Key provisions in the GDPR
See Articles 28.1, 28.2, 28.3, 28.4, 28.9 and 28.10 and Recital 81. (external

link)

What needs to be included in the contract?

In brief…

- Contracts must set out:
    - 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.
- Contracts must also include as a minimum the following terms, requiring the processor to:
    - only act on the written instructions of the controller;
    - ensure that people processing the data are subject to a duty of confidence;
    - take appropriate measures to ensure the security of processing;
    - only engage sub-processors with the prior consent of the controller and under a written contract;
    - assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
    - assist the 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 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.

What details about the processing must the contract include?

Article 28.3 firstly states that the contract (or other legal act) must include the following details about the processing:

- the subject matter;
- how long it is to be carried out for;

- what processing is being done;
- its purpose;
- the type of personal data;
- the categories of data subjects; and
- the obligations and rights of the data controller.

You therefore need to be very clear from the outset about the extent of the processing that you are contracting out, and you can't use very general or 'catch all' contract terms.

This clarity should also help to protect against the possibility of changes being made to the scope of the processing over time without taking into account any additional risks this poses to the data subjects.

Recital 81 is clear that, in agreeing the contract or other legal act, the specific tasks and responsibilities of the processor and the risk to the rights and freedoms of the data subjects must be taken into account.

Minimum required terms

Article 28.3 then sets out some specific terms or clauses that you must include in your contract. These are the minimum required, but you and your processor may agree to supplement them with your own terms.

- Process only on the written instructions of the controller

Under Article 28.3(a) your contract must provide that:

  - the processor may only process personal data in accordance with your written instructions (including when making an international transfer of personal data) unless required to do so by law.

In this situation the processor needs to tell you what they are required to do by law, before they do it (unless the law also prevents you from being told for reasons of important public interest).

This contract term should make it clear that it is you, rather than the processor, who controls what happens to the personal data. The exception however means the contract doesn't prevent processors from complying with any other laws that they may be subject to.

- Duty of confidence

Under Article 28.3(b) your contract must provide that:

- your processor must obtain a commitment of confidentiality from anyone it allows to process the personal data, unless they are already under such a duty by law.

This covers the processor's employees as well as any temporary workers and agency workers.

This contract term should give data subjects important protection against non-compliant disclosures.

- Appropriate security measures

Under Article 28.3(c) your contract must provide that:

- the processor is subject to the same Article 32 requirements as you are to keep the personal data it is processing secure.

Under the GDPR you must obviously take measures to ensure the security of any personal data being processed; however the contract must also require your processor to do this. Article 32 of the GDPR lists the "appropriate technical and organisational measures" that you both must take to ensure the security of personal data processing, having taken account of the risks.

These include adopting security measures including encryption, pseudonymisation, resilience of processing systems and backing up personal data in order to be able to reinstate the system.

We will issue separate guidance on security matters under the GDPR in due course, but in the meantime our existing guidance under the DPA should still be relevant.

- Using sub-processors

Under Article 28.3(d) your contract must provide that:

- your processor should not employ another processor without your prior specific or general written authorisation;

- if another processor is employed under your prior general written authorisation, your processor should let you know of any changes it has made and give you a chance to object to them;

- if your processor employs another processor, then it must impose the contract terms that are required by Article 28.3 of the GDPR on the sub-processor; and

- if your processor employs another processor, then the original processor will still be liable to you for the compliance of the sub-processor.

This should mean that you remain in control of what happens to the personal data even if your original processor wishes to sub-contract out some or all of the processing. It also means that the original processor cannot absolve itself of responsibility by using a sub-processor.

- Data subjects' rights

Under Article 28.3(e) your contract must provide that:

  - your processor must assist you in meeting your obligations to data subjects under chapter III of the GDPR, by having appropriate technical and organisational measures.

This provision stems from Chapter III of the GDPR, which describes how the controller must enable data subjects to exercise their rights, such as subject access requests and requests for the rectification or erasure of personal data, and making objections to processing. We will issue guidance on this in due course.

There is a practical basis to including this in your contract: your processor will handle the personal data on a day to day basis, and their co-operation in helping data subjects to exercise their rights will therefore be essential.

- Assisting the controller

Under Article 28.3(f) your contract must provide that, taking into account the nature of the processing and the information available to the processor:

  - your processor must assist you in meeting your Article 32 obligation to keep personal data secure;

  - your processor must assist you in meeting your Article 33 obligation to notify personal data breaches to your supervisory authority;

  - your processor must assist you in meeting your Article 34 obligation to advise data subjects when there has been a personal data breach;

  - your processor must assist you in meeting your Article 35 obligation to carry out data protection impact assessments (DPIAs); and

  - your processor must assist you in meeting your Article 36 obligation to consult with your supervisory authority where your DPIA indicates there is an unmitigated high risk to the processing.

Again this requirement has a practical basis; your processor is handling daily the personal data that you will need to refer to in order to comply with your

duties on security, breaches, DPIAs and high risk processing under Articles 32-36 of the GDPR.

We will issue guidance on the specific requirements of each of these articles in due course.

However your processor's duty to assist you to comply is not infinite; it is limited by "taking into account the nature of processing and the information available to the processor".

- End of contract provisions

Under Article 28.3(g) your contract must provide that:

  - at the end of the contract your processor must, at your choice, either delete or return to you all the personal data it has been processing for you; and

  - an exception to this general rule applies if the processor is required to retain the personal data by law.

The contract must include this term in order to ensure the continuing protection of the personal data after the end of the contract. It reflects the fact that it is ultimately for you to decide what should happen to the personal data being processed, once processing is complete.

- Audits and inspections

Under Article 28.3(h) your contract must provide that:

  - your processor must provide you with all the information that is needed to show that that both of you have met the obligations of Article 28;

  - your processor must submit and contribute to audits and inspections that you carry out, or another auditor appointed by you carries out; and

  - your processor must tell you immediately if it thinks it has been given an instruction which doesn't comply with the GDPR, or related data protection law[1].

This is another practical provision, obliging both you and your processor to demonstrate compliance with the whole of Article 28. For instance, the processor could do this by providing you with the necessary information or

[1] We assume that there is a typographical error at paragraph (h) and that it should state "With regard to point (h) of the **third** subparagraph" – ie Article 28.3(h).

by submitting to an audit or inspection. In practice this means that your processor will need to keep records of the processing it carries out.

Key GDPR provisions
See Articles 28.3, 28.4, 28.5, 28.6, 28.7, 28.8, 28.9, 28.10, 29, 30, 32, 33, 34, 35 and 36 and Recitals 81 and 82-96. (external link)

Can standard contracts clauses be used?

In brief...

- The GDPR allows standard contractual clauses from the EU Commission or a Supervisory Authority (such as the ICO) to be used in contracts between controllers and processors. However, no standard clauses are currently available.
- The GDPR also allows these standard contractual clauses to form part of a code of conduct or certification mechanism to demonstrate compliant processing. However, no schemes are currently available.

The GDPR allows the EU Commission and supervisory authorities (such as the ICO) to issue standard clauses to include in contracts between controllers and processors. These clauses are not yet available, but in the future may provide a simple way for you to ensure that your contracts comply with the GDPR.

These clauses may also form part of a code of conduct, or certification scheme, although currently no schemes have been approved. Further guidance on these schemes will be provided in due course.

Key GDPR provisions
See Articles 28.5, 28.6, 28.7, 28.8, 40 and 42 and Recitals 77, 81, 98 and 100. (external link)

What responsibilities and liabilities do controllers have when using a processor?

In brief…

- Controllers must only use processors which are able to guarantee that they will meet the requirements of the GDPR and protect the rights of data subjects.
- Controllers must ensure that they put a contract in place which meets the requirements set out in this guidance.
- They must provide documented instructions for the processor to follow.
- Controllers remain directly liable for compliance with all aspects of the GDPR, and for demonstrating that compliance. If this isn't achieved then they may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

What responsibilities does a controller have when choosing a processor?

You have a responsibility to check that your processor is competent to process the personal data in accordance with all the requirements of the GDPR. Your assessment should take into account the nature of the processing and the risks to the data subjects. This is because Article 28.1 says that you must only use a processor that can provide "sufficient guarantees" in terms of its resources and expertise, to implement technical and organisational measures to comply with the GDPR and protect the rights of data subjects.

If you choose a processor which adheres to a code of conduct or a certification scheme that has been approved under Article 40 or 42 of the GDPR (as and when these become available), then this may help to demonstrate your compliance with Article 28.1. Ultimately, however, it is for you to satisfy yourself that the processor provides sufficient guarantees in the context of the processing.

Once you have chosen a suitable processor you must put in place a contract which meets all the requirements of Article 28.3, and you must provide it with documented instructions to follow.

What is the controller's liability when it uses a processor?

As a data controller you are ultimately responsible for ensuring that personal data is processed in accordance with the GDPR. This means that, regardless or your use of a processor, you may be subject to any of the corrective measures and sanctions set out in GDPR. These include orders to bring processing into compliance, claims for compensation from a data subject and administrative fines. Further guidance on sanctions and corrective measures under the GDPR will be issued in due course.

Unless you can prove that you were "not in any way responsible for the event giving rise to the damage", you will be fully liable for any damage caused by non-compliant processing, regardless of your use of a processor. This ensures that the data subject is properly compensated. You may however be able to claim back all or part of the amount of compensation from your processor, to the extent that it is liable.

Key GDPR provisions
See Articles 28, 29, 58, 82, 83 and 84 and Recitals 39, 81, 146, 148, 149, 150 and 152. (external link)

What responsibilities and liabilities do processors have in their own right?

In brief…

- A processor must only act on the documented instructions of a controller.
- If a processor determines the purpose and means of processing (rather than acting only on the instructions of the controller) then it will be considered to be a controller and will have the same liability as a controller.
- In addition to its contractual obligations to the controller, under the GDPR a processor also has the following direct responsibilities:
    - not to use a sub-processor without the prior written authorisation of the data controller;
    - to co-operate with supervisory authorities (such as the ICO);
    - to ensure the security of its processing;
    - to keep records of processing activities;
    - to notify any personal data breaches to the data controller;
    - to employ a data protection officer; and
    - to appoint (in writing) a representative within the European Union if needed.
- If a processor fails to meet any of these obligations, or acts outside or against the instructions of the controller, then it may be liable to pay damages in legal proceedings, or be subject to fines or other penalties or corrective measures.
- If a processor uses a sub-processor then it will, as the original processor, remain directly liable to the controller for the performance of the sub-processor's obligations.

How much autonomy does a processor have?

Although a processor may make its own day to day operational decisions, Article 29 provides that it should only process personal data in accordance with your instructions, unless it is required to do so by law. This is also a required contract term under Article 28.3(a).

If a processor acts without your instructions in such a way that it determines the purpose and means of processing then it will be considered to be a controller and will have the same liability as a controller.

What other responsibilities does a processor have in its own right?

Your processor also has some direct responsibilities and liabilities under the GDPR. When drawing up and negotiating a contract for data processing, it is good practice to make sure that your processor understands this.

You may also wish to explicitly cover this in your contract, although the GDPR doesn't require you to do so. For example you may want to include a clause to specify that nothing within the contract relieves your processor of its own direct responsibilities and liabilities under the GDPR – and to say what these are. Additionally the contract could specify the extent of any indemnity you have negotiated. In any case we would recommend that you and your processor obtain your own professional advice on this point.

Each of the processor's direct responsibilities under the GDPR is now considered in more detail below. Some, though not all, of these are also required contract terms.

- Using sub-processors

Article 28.2 provides that a processor should not engage another processor without your prior written authorisation. Your authorisation may be either specific or general. If your authorisation is general, the processor must tell you in advance of any changes it intends to make regarding the addition or replacement of other processors, so you have the opportunity to object. This is also a required contract term under Article 28.3(d).

- Co-operation with supervisory authorities

Article 31 provides that processors as well as controllers must, on request, co-operate with supervisory authorities, including the ICO in the UK.

- Security of processing

Article 32 provides that processors as well as controllers must implement technical and organisational measures to ensure the security of any personal data being processed. We will issue further guidance on the security

provisions of the GDPR in due course, but in the meantime our existing guidance under the DPA should still be relevant. This is also a required contract term under Article 28.3(c).

- Records of processing activities

Article 30(2) provides that processors must keep records of the processing activities they carry out on your behalf.

We will issue further guidance on the record-keeping provisions of the GDPR in due course.

- Notifying personal data breaches to the controller

Article 33 provides that processors must inform controllers of a personal data breach "without undue delay" after becoming aware of it.

We will issue further guidance on the personal data breach notification requirements of the GDPR in due course.

- Data protection officer

Article 37 provides that processors as well as controllers need to designate a data protection officer in certain circumstances, and to provide necessary resources to them and ensure their independence.

We will provide further guidance on the data protection officer provisions of the GDPR in due course.

- Appointing a representative within the European Union

Article 27 provides that processors as well as controllers must appoint a representative within the EU, in writing, in certain circumstances.

We will issue further guidance on the requirement to appoint a representative in due course.

Can a processor be held liable for non-compliance?

Under contract law a processor may be directly liable to you for any failure to meet the terms of your agreed contract. This will of course depend upon the exact terms of your contract.

It will be subject to the relevant investigative and corrective powers of a supervisory authority (such as the ICO) under Article 58 of the GDPR and

may also be subject to administrative fines or other penalties under Articles 83 and 84.

A processor can also be held liable under Article 82 to pay compensation for the damage caused by processing where:

- it has failed to comply with GDPR provisions specifically relating to processors, or
- where it has acted without the lawful instructions of the controller, or against those instructions.

It will not be liable if it can prove it is not "in any way responsible for the event giving rise to the damage". Under Article 82.5 it may be able to claim back from you part of the compensation it paid, for your share of liability.

We will provide more guidance on investigative and corrective powers, penalties and damages in due course.

All this provides a very strong reason for you to make sure that your processor is aware of the consequences and penalties which it may be subject to if it fails to comply with the GDPR. The GDPR has real 'teeth' in terms of enforcement, which could have serious operational and financial implications for both controllers and processors.

Who is liable if a sub-processor is used?

Where a processor uses a sub-processor to carry out processing on its behalf, it must put in place a contract (or other legal act). This should impose on the sub-processor the same legal obligations the processor itself owes to the controller. The sub-processor has the same direct responsibilities and liabilities under the GDPR as the original processor has. If a sub-processor is used and someone makes a claim for compensation then there are potentially three liable parties: you as controller, the original processor, and the sub-processor. Under Article 82.5 each of you may be able to claim against the others for their share of the liability.

Key GDPR provisions
See Articles 3, 5, 27, 28, 29, 30, 31, 32, 33.2, 37, 38, 82, 83 and 84 and Recitals 22, 23, 24, 39, 80, 81, 85, 87, 88, 91, 97, 146, 148, 149, 150 and 152. (external link)

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.