

About this detailed guidance	2
What are 'controllers' and 'processors'?	4
How do you determine whether you are a controller or processor?	9
What does it mean if you are a controller?	14
What does it mean if you are a processor?	16
What does it mean if you are joint controllers?	19

About this detailed guidance

This guidance discusses controllers and processors in detail. Read it if you have detailed questions not answered in the Guide, or if you need a deeper understanding. DPOs and those with specific data protection responsibilities in larger organisations are likely to find it useful.

If you haven't yet read controllers and processors [in brief](#) in the Guide to Data Protection, you should read that first. It sets out the key points you need to know, along with practical checklists to help you comply.

This guidance will help you decide whether you are acting as a controller, processor or joint controller when processing personal data. We know this exercise can be difficult, so we have included examples to help you. The guidance also explains the roles and responsibilities of each, and outlines the governance issues that are relevant to them.

Contents

What are 'controllers' and 'processors'?

[What does the UK GDPR say about controllers and processors?](#)

[What is a controller?](#)

[What is a joint controller?](#)

[What is a processor?](#)

[What is a sub-processor?](#)

How do you determine whether you are a controller or processor?

[Why is it important to distinguish between controllers and processors?](#)

[How do you determine whether you are a controller or processor?](#)

[How does this apply in practice?](#)

[Can you be both a controller and a processor of personal data?](#)

What does it mean if you are a controller?

[What are your responsibilities as a controller?](#)

[Can you be held liable for non-compliance?](#)

What does it mean if you are a processor?

[What are your responsibilities as a processor?](#)

[Can a processor be held liable for non-compliance?](#)

[Can you sub-contract to another processor?](#)

[How does using a sub-processor affect liability for non-compliance?](#)

What does it mean if you are joint controllers?

[What are the responsibilities of joint controllers?](#)

[Can a joint controller be held liable for non-compliance?](#)

What are ‘controllers’ and ‘processors’?

In detail

- [What does the UK GDPR say about controllers and processors?](#)
- [What is a controller?](#)
- [What is a joint controller?](#)
- [What is a processor?](#)
- [What is a sub-processor?](#)

What does the UK GDPR say about controllers and processors?

The UK GDPR draws a distinction between a ‘controller’ and a ‘processor’ in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. The UK GDPR defines these terms:



‘**controller**’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

‘**processor**’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

If you are a controller, you are responsible for complying with the UK GDPR – you must be able to demonstrate compliance with the data protection principles, and take appropriate technical and organisational measures to ensure your processing is carried out in line with the UK GDPR.

If you are a processor, you have more limited compliance responsibilities.

Further Reading

 [Relevant provisions in the UK GDPR - See Articles 4\(7\), 4\(8\), 5\(1\), 5\(2\) and 28](#) 

External link

What is a controller?

The UK GDPR defines a controller as:



the natural or legal person, public authority, agency or other body which, alone or jointly with others,

determines the purposes and means of the processing of personal data.

Controllers make decisions about processing activities. They exercise overall control of the personal data being processed and are ultimately in charge of and responsible for the processing.

Some controllers may be under a statutory obligation to process personal data. Section 6(2) of the Data Protection Act 2018 says that anyone who is under such an obligation and only processes data to comply with it will be a controller.

A controller can be a company or other legal entity (such as an incorporated partnership, incorporated association or public authority), or an individual (such as a sole trader, partner in an unincorporated partnership, or self-employed professional, eg a barrister).

However, an individual processing personal data for the purposes of a purely personal or household activity is not subject to the UK GDPR.

Further Reading

 [Relevant provisions in the UK GDPR - See Article 2\(2\)\(c\)](#) 

External link

Example

A GP surgery uses an automated system in its waiting room to notify patients when to proceed to a GP consulting room. The system consists of a digital screen that displays the waiting patient's name and the relevant consulting room number, and also a speaker for visually impaired patients that announces the same information.

The GP surgery will be the controller for the personal data processed in connection with the waiting room notification system because it is determining the purposes and means of the processing.

Example

A firm uses an accountant to do its books. When acting for his client, the accountant is a controller in relation to the personal data in the accounts. This is because accountants and similar providers of professional services work under a range of professional obligations that oblige them to take responsibility for the personal data they process. For example, if the accountant detects malpractice while doing the firm's accounts he may, depending on its nature, be required under his monitoring obligations to report the malpractice to the police or other authorities. In doing so, an accountant would

not be acting on the client's instructions but in line with his own professional obligations and therefore as a controller in his own right.

If specialist service providers are processing data in line with their own professional obligations, they will always be acting as the controller. In this context, they cannot agree to hand over or share controller obligations with the client.

Some organisations don't have a separate legal personality of their own – for example, unincorporated associations such as sports clubs or voluntary groups. In this case you should review the document which sets up and governs the management of that organisation. This document should set out which individual(s) manage the organisation on behalf of its members and are likely to act as the controller or joint controllers, and how contracts may be entered into on behalf of the organisation.

For convenience you may identify the organisation as a whole as the controller (eg you may use the club or group name in your privacy information for individuals). But for legal purposes the controller will actually be the relevant members who make the decisions about the processing by the organisation.

What is a joint controller?

Controllers can determine the purposes and means of processing alone, or jointly with others – as a joint controller. Article 26(1) of the UK GDPR states that:



Where two or more controllers jointly determine the purposes and means of processing, they shall be **joint controllers**.

Joint controllers decide the purposes and means of processing together – they have the same or shared purposes. Controllers will not be joint controllers if they are processing the same data for different purposes.

Further Reading

[Relevant provisions in the UK GDPR - See Article 26](#)

External link

What is a processor?

The UK GDPR defines a processor as:



'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Processors act on behalf of the relevant controller and under their authority. In doing so, they serve the controller's interests rather than their own.

Although a processor may make its own day-to-day operational decisions, Article 29 says it should only process personal data in line with a controller's instructions, unless it is required to do otherwise by law.

If a processor acts without the controller's instructions in such a way that it determines the purpose and means of processing, including to comply with a statutory obligation, it will be a controller in respect of that processing and will have the same liability as a controller.

A processor can be a company or other legal entity (such as an incorporated partnership, incorporated association or public authority), or an individual, for example a consultant.

Example

A gym engages a local printing company to produce invitations to a special event the gym is hosting. The gym gives the printing company the names and addresses of its members from its member database, which the printer uses to address the invitations and envelopes. The gym then sends out the invitations.

The gym is the controller of the personal data processed in connection with the invitations. The gym determines the purposes for which the personal data is being processed (to send individually addressed invitations to the event) and the means of the processing (mail merging the personal data using the data subjects' address details). The printing company is a processor processing the personal data only on the gym's instructions.

Employees of the controller are not processors. As long as they are acting within the scope of their duties as an employee, they are acting as an agent of the controller itself. They are part of the controller, not a separate party contracted to process data on the controller's behalf.

What is a sub-processor?

A processor might wish to sub-contract all or some of the processing to another processor. For shorthand this is sometimes referred to as using a 'sub-processor', although this term is not taken from the UK GDPR itself.

Further Reading

 [Relevant provisions in the UK GDPR - See Article 28\(4\) !\[\]\(64f7c7e956682d89489e8b2ffcb346b7_img.jpg\)](#)

External link

How do you determine whether you are a controller or processor?

In detail

- [Why is it important to distinguish between controllers and processors?](#)
- [How do you determine whether you are a controller or processor?](#)
- [How does this apply in practice?](#)
- [Can you be both a controller and a processor of personal data?](#)

Why is it important to distinguish between controllers and processors?

The nature of your UK GDPR obligations will depend on whether you are a controller, joint controller or processor. Therefore, it is very important that you carefully consider your role and responsibilities in respect of your data processing activities, so you understand:

- your UK GDPR obligations and how to meet them;
- your responsibilities to individuals and supervisory authorities (including the ICO) and the penalties associated with non-compliance, such as fines and other enforcement powers; and
- how you can work with other organisations to ensure you process personal data responsibly and respect individuals' rights.

Controllers (including joint controllers) have more obligations under the UK GDPR than processors do, because they decide what personal data is collected and why, and exercise ultimate control over the data. UK controllers must also pay a data protection fee unless they are exempt.

Processors have fewer obligations, but must be careful to only process personal data in line with the relevant controller's instructions.

How do you determine whether you are a controller or processor?

It is important to remember that an organisation is not by its nature either a controller or a processor. Instead you need to consider the personal data and the processing activity that is taking place, and consider who is determining the purposes and the manner of that specific processing.

You need to ask which organisation decides:

- to collect personal data in the first place;
- the lawful basis for doing so;
- what types of personal data to collect;
- the purpose or purposes the data are to be used for;
- which individuals to collect data about;
- whether to disclose the data, and if so, to whom;

- what to tell individuals about the processing;
- how to respond to requests made in line with individuals' rights; and
- how long to retain the data or whether to make non-routine amendments to the data.

These are decisions that determine the purposes and means of the processing. Therefore, if you make any of these decisions, it is likely that you are a controller.

However, within the terms of its contract with the controller, a processor may decide:

- what IT systems or other methods to use to collect personal data;
- how to store the personal data;
- the details of the security measures to protect the personal data;
- how it will transfer the personal data from one organisation to another;
- how it will retrieve personal data about certain individuals;
- how it will ensure it adheres to a retention schedule; and
- how it will delete or dispose of the data.

These lists are not exhaustive, but illustrate the differences between the controller's and the processor's roles. In certain circumstances, and where allowed for in the contract, a processor may have the freedom to use its technical knowledge to decide how to carry out certain activities on the controller's behalf. However, it cannot take any of the overarching decisions, such as what types of personal data to collect or what the personal data will be used for. Such decisions must only be taken by the controller.

How does this apply in practice?

The definition of a processor can be difficult to apply in the complexity of modern business relationships. In practice, there is a scale of responsibility in how organisations work together to process personal data. The key is to determine each party's degree of independence in determining how and in what manner the data is processed as well as the degree of control over it.

At one extreme, one party (the client) will determine what personal data is to be processed and provide detailed processing instructions that the other party (the service provider) must follow. The service provider is tightly constrained in what it can do with the data and has no say at all over how it is processed. In this relationship the client is clearly the controller and the service provider is the processor.

However, it is far more common for a data controller to allow its processor discretion over how the processing takes place using its own expertise.

Example

A bank hires an IT services firm to store archived data on its behalf – having ensured that the IT firm has given sufficient guarantees about the security of its systems and processes. The bank will still control how and why the data is used and determine its retention period. In reality the IT services firm will use a great deal of its own technical expertise and professional judgement to decide how best to store the data in a safe and accessible way.

However, despite this freedom to take technical decisions, the IT firm is still not a data controller in respect of the bank's data – it is a processor. This is because the bank retains exclusive control over the purpose for which the data is processed, if not exclusively over the manner in which the processing takes place.

Example

A private company provides software to process the daily pupil attendance records of a state-maintained school. Using the software, the company gives attendance reports to the school.

The company's sole purpose in processing the attendance data is to provide this service to the school. The school sets the purpose – to assess attendance. The company has no need to retain the data after it has produced the report. It does not determine the purposes of the processing, it merely provides the processing service. This company is likely to be a processor.

Example

A bank contracts a market-research company to carry out some research. The bank's brief specifies its budget and that it requires a satisfaction survey of its main retail services based on the views of a sample of its customers across the UK. The bank leaves it to the research company to determine sample sizes, interview methods and presentation of results.

The research company is processing personal data on the bank's behalf, but it is also determining the information that is collected (what to ask the bank's customers) and the manner in which the processing (the survey) will be carried out. It has the freedom to decide such matters as which customers to select for interview, what form the interview should take, what information to collect from customers and how to present the results. This means the market-research company is a joint controller with the bank regarding the processing of personal data to carry out the survey, even though the bank retains overall control of the data because it commissions the research and determines the purpose the data will be used for.

Example

A hospital is sending envelopes containing patient data to another health provider and contracts a delivery service to deliver them.

The delivery service is not processing the personal data contained in those envelopes. Although it is in physical possession of the envelopes, it has no idea what the envelopes contain and may not open them to access the content. For data protection purposes, the delivery service does not 'process' any personal data contained within those envelopes.

The hospital that chooses to use the delivery service is the controller responsible for the data contained in the envelopes. If the delivery service loses or misdirects an envelope containing highly sensitive personal data, for data protection purposes the controller that sent it is responsible for that loss. So the sender should think carefully about the type of service that is most appropriate in the circumstances.

Example

An online retailer contracts a mail delivery service to deliver orders to customers. The customers can use a website to check the status of their order and track its delivery.

The retailer will be the controller for any personal data inside the package. The delivery service will not be a controller or a processor for any personal data contained inside the package, as it has no control over or access to that data.

However, the delivery company will be processing some personal data (eg the name and address of the customer) in order to deliver the package and provide the tracking service. Whether it is a controller or a processor for the tracking element of the service will depend on who makes the decisions. If the retailer makes the final decision on the tracking service to be provided and the delivery service merely follows the retailer's instructions, then the retailer will be the controller and the delivery service is likely to be a processor. But if the delivery company independently decides on the tracking service provided to individuals without the retailer's sign-off, it will be a controller.

Can you be both a controller and a processor of personal data?

Yes. If you are a processor that provides services to other controllers, you are very likely to be a controller for some personal data and a processor for other personal data. For example, you will have your own employees so you will be a controller regarding your employees' personal data. However, you cannot be both a controller and a processor for the same processing activity.

In some cases, you could be a controller and a processor of the same personal data – but only if you are processing it for different purposes. You may be processing some personal data as a processor for the controller's purposes and only on its instruction, but also process that same personal data for your own separate purposes.

In particular, if you are a processor, you should remember that as soon as you process personal data outside your controller's instructions, you will be acting as a controller in your own right for that element of your processing.

If you are acting as both a controller and processor, you must ensure your systems and procedures distinguish between the personal data you are processing in your capacity as controller and what you process as a processor on another controller's behalf. If some of the data is the same, your systems must be able to distinguish between these two capacities, and allow you to apply different processes and measures to each. If you cannot do this, you are likely to be considered a joint controller rather than a processor for the data you process on your client's behalf.

What does it mean if you are a controller?

In detail

- [What are your responsibilities as a controller?](#)
- [Can you be held liable for non-compliance?](#)

What are your responsibilities as a controller?

If you are a controller, you are responsible for ensuring your processing – including any processing carried out by a processor on your behalf – complies with the UK GDPR. Your UK GDPR responsibilities include the following:

- **Compliance with the data protection principles:** you must comply with the data protection principles listed in Article 5 of the UK GDPR. For more information please read our guidance on the [principles](#).
- **Individuals' rights:** you must ensure that individuals can exercise their rights regarding their personal data, including the rights of access, rectification, erasure, restriction, data portability, objection and those related to automated decision-making. For more information please read our guidance on [individuals' rights](#).
- **Security:** you must implement appropriate technical and organisational security measures to ensure the security of personal data. For more information please read our guidance on [security](#).
- **Choosing an appropriate processor:** you can only use a processor that provides sufficient guarantees that they will implement appropriate technical and organisational measures to ensure their processing meets UK GDPR requirements. This means you are responsible for assessing that your processor is competent to process the personal data in line with the UK GDPR's requirements. This assessment should take into account the nature of the processing and the risks to the data subjects.
- **Processor contracts:** you must enter into a binding contract or other legal act with your processors, which must contain a number of compulsory provisions as specified in Article 28(3). For more information please read our guidance on [contracts](#).
- **Notification of personal data breaches:** you are responsible for notifying personal data breaches to the ICO and, where necessary, other supervisory authorities in the EU, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. You are also responsible for notifying affected individuals (if the breach is likely to result in a high risk to their rights and freedoms). For more information please read our guidance on [personal data breaches](#).
- **Accountability obligations:** you must comply with the UK GDPR accountability obligations, such as maintaining records, carrying out data protection impact assessments and appointing a data protection officer. For more information please read our guidance on [accountability and governance](#).
- **International transfers:** you must comply with the UK GDPR's restrictions on transfers of personal data outside of the UK. For more information please read our guidance on [international transfers](#).
- **Co-operation with supervisory authorities:** you must cooperate with supervisory authorities (such as the ICO) and help them perform their duties.
- **Data protection fee:** you must pay the ICO a data protection fee unless you are exempt. For more information please see our guidance on [the data protection fee](#).

Can you be held liable for non-compliance?

Yes. You are ultimately accountable for your own compliance and the compliance of your processors.



An individual can also bring claims directly against a controller if the processing breaches the UK GDPR, in particular if the processing causes the individual damage.

You will be liable for any damage (and any associated claim for compensation payable to an individual) if your processing activities infringe the UK GDPR.

However, you are not liable for damage resulting from a breach of the UK GDPR if you can prove you were not in any way responsible for the event giving rise to the damage.

If you are not the only party involved in the processing (for example, a joint controller or processor is also involved), the individual making the claim for compensation can claim against any of you. If you have to pay full compensation for damage suffered by individuals, you may be able to claim back all or part of the amount of compensation from other controllers or processors involved in the processing, to the extent that they are at fault.

Further Reading

 [Relevant provisions in the UK GDPR - See Chapters 1 to 5 in particular Articles 4\(7\), 5\(2\), 13-14, 24-28, 30-37, 44, 46-49 and 82 and Recitals 58-61, 73-74, 78-79, 80-89, 97, 101, 108-110 and 146](#) 

External link

What does it mean if you are a processor?

In detail

- [What are your responsibilities as a processor?](#)
- [Can a processor be held liable for non-compliance?](#)
- [Can you sub-contract to another processor?](#)
- [How does using a sub-processor affect liability for non-compliance?](#)

What are your responsibilities as a processor?

Processors have less autonomy and independence over the data they process, but they do have several direct legal obligations under the UK GDPR and are subject to regulation by supervisory authorities. If you are a processor, you have the following obligations.

- **Controller's instructions:** you can only process the personal data on instructions from a controller (unless otherwise required by law). If you act outside your instructions or process for your own purposes, you will step outside your role as a processor and become a controller for that processing.
- **Processor contracts:** you must enter into a binding contract with the controller. This must contain a number of compulsory provisions, and you must comply with your obligations as a processor under the contract. For more information please read our guidance on [contracts](#).
- **Sub-processors:** you must not engage another processor (ie a sub-processor) without the controller's prior specific or general written authorisation. If authorisation is given, you must put in place a contract with the sub-processor with terms that offer an equivalent level of protection for the personal data as those in the contract between you and the controller.
- **Security:** you must implement appropriate technical and organisational measures to ensure the security of personal data, including protecting against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access. For more information please read our guidance on [security](#).
- **Notification of personal data breaches:** if you become aware of a personal data breach, you must notify the relevant controller without undue delay. Most controllers will expect to be notified immediately, and may contractually require this, as they only have a limited time in which to notify the supervisory authority (such as the ICO). You must also assist the controller in complying with its obligations regarding personal data breaches. For more information please read our guidance on [personal data breaches](#).
- **Notification of potential data protection infringements:** you must notify the controller immediately if any of their instructions would lead to a breach of the UK GDPR or local data protection laws.
- **Accountability obligations:** you must comply with certain UK GDPR accountability obligations, such as maintaining records and appointing a data protection officer. For more information please read our guidance on [accountability and governance](#).
- **International transfers:** the UK GDPR's prohibition on transferring personal data applies equally to processors as it does to controllers. This means you must ensure that any transfer outside the UK is authorised by the controller and complies with the UK GDPR's transfer provisions. For more information please read our guidance on [international transfers](#).
- **Co-operation with supervisory authorities:** you are also obliged to cooperate with supervisory

authorities (such as the ICO) to help them perform their duties.

Can a processor be held liable for non-compliance?

Yes. You will be subject to the relevant investigative and corrective powers of a supervisory authority (such as the ICO) and may be subject to administrative fines or other penalties.

You may also be contractually liable to the controller for any failure to meet the terms of your agreed contract. This will of course depend on the exact terms of that contract.

An individual can also bring a claim directly against you in court. You can be held liable under Article 82 to pay compensation for any damage caused by processing (including non-material damage such as distress). You will only be liable for the damage if:

- you have failed to comply with UK GDPR provisions specifically relating to processors; or
- you have acted without the controller's lawful instructions or against those instructions.

You will not be liable if you can prove you are not in any way responsible for the event giving rise to the damage.

If you are required to pay compensation but are not wholly responsible for the damage, you may be able to claim back from the controller, the share of the compensation for which they were liable. Both parties should seek professional legal advice on this.

Further Reading

 [Relevant provisions in the UK GDPR – See Articles 3\(1\), 4\(8\), 28-33, 37, 44, 46-49 and 82 and Recitals 22, 81-82, 91, 101, 108-110 and 146](#) 

External link

Further reading – ICO guidance

[Contracts and liabilities between controllers and processors](#)

Can you sub-contract to another processor?

If you wish to use a sub-processor, you must obtain the controller's written authorisation. The authorisation can be specific or general. Specific authorisation means the controller must approve the particular sub-processor for the particular processing operation in question. General authorisation means:

- the controller pre-approves a list of potential sub-processors; or
- the controller approves a list of criteria that you can use to select and appoint a sub-processor.

If you have general authorisation, you must inform the controller if you wish to make any changes to the list of possible sub-processors or criteria for choosing a sub-processor, and give the controller a chance to

object.

You must send the controller any proposed changes in writing, setting out the date by which the controller should raise any objections. The controller should also respond in writing and explain the reasons for any objections. Remember you can only act on the controller's instructions.

If you have written authorisation, you may appoint the sub-processor but must put in place a contract with the sub-processor. The terms of the contract that relate to Article 28(3) must offer an equivalent level of protection for the personal data as those in the contract between you and the controller.

The fact that you may sub-contract some or all of the processing activities you have been engaged to perform does not make you a controller in your own right, as overall control of the processing remains with the original controller. However, you will be liable to the controller for the sub-processor's compliance.

How does using a sub-processor affect liability for non-compliance?

If you are a sub-processor, you will be liable for any damage caused by your processing only if you have not complied with the UK GDPR obligations imposed on processors or you have acted contrary to the controller's lawful instructions, relayed by the processor, regarding the processing.

If you are a processor and use a sub-processor to carry out processing on your behalf, you will be fully liable to the controller for the sub-processor's compliance. This means that, under Article 82(5), if a sub-processor is at fault, the controller may claim back compensation from you for the failings of the sub-processor. You may then claim compensation back from the sub-processor.

A sub-processor may also be contractually liable to the processor for any failure to meet the terms of their agreed contract. This will of course depend on the exact terms of that contract.

Processors and sub-processors should seek their own legal advice on issues of liability and on the contracts made between controllers and processors and processors and sub-processors.

Further Reading

 [Relevant provisions in the UK GDPR - See Articles 28\(2\) and 28\(4\)](#) 

External link

Further reading – ICO guidance

[Contracts and liabilities between controllers and processors](#)

What does it mean if you are joint controllers?

In detail

- [What are the responsibilities of joint controllers?](#)
- [Can a joint controller be held liable for non-compliance?](#)

What are the responsibilities of joint controllers?

- **Obligations of controllers:** You need to decide with your fellow joint controllers who will carry out which controller obligation under the UK GDPR. However, regardless of those arrangements, each controller remains responsible for complying with all the obligations of controllers under the UK GDPR.
- **Transparent arrangement:** Joint controllers are not required to have a contract, but you must have a transparent arrangement that sets out your agreed roles and responsibilities for complying with the UK GDPR. The main points of this arrangement should be made available to individuals. We recommend that you include this in your privacy information.
- **Individuals' rights:** In particular, you must decide (and be transparent about) how you will comply with transparency obligations and individuals' rights. You may choose to specify a central point of contact for individuals. However, individuals must remain able to exercise their rights against each controller.

Can a joint controller be held liable for non-compliance?

Yes. Individuals can seek compensation from joint controllers in exactly the same way as from any sole controller. Each joint controller will be liable for the entire damage caused by the processing, unless it can prove it is not in any way responsible for the event giving rise to the damage. The arrangement made between controllers is irrelevant for these purposes.

If as a joint controller you have had to pay compensation to an individual but were not wholly responsible for the damage, you may be able to claim back from another controller or processor the share of the compensation for which they were liable.

In addition, joint controllers are each fully accountable to supervisory authorities (such as the ICO) for failure to comply with their responsibilities.

Example

A luxury car company teams up with a designer fashion brand to host a co-branded promotional event. The companies decide to run a prize draw at the event. They invite attendees to participate in the prize draw by entering their name and address into their prize draw system at the event. After the event, the companies post out the prizes to the winners. They do not use the personal data for any other purposes.

The companies will be joint controllers of the personal data processed in connection with the prize

draw, because they both decided the purposes and means of the processing.

Example

A property management company maintains student halls of residence for the landlord, the university. The company enters tenancy agreements with the students on the university's behalf and chases any rent arrears. It collects the rent and passes it to the university after taking a commission.

The company is a joint controller of the tenancy-related information, including regarding rental payments. It decides what information it needs from the residents to set up and manage the tenancies but will share this data with the university.

Further Reading

 [Relevant provisions in the UK GDPR - See Articles 26, 82 and 83 and Recitals 79 and 146](#) 

External link