

Commercial Data Storage Policy

Introduction and scope

- The Company obtains, keeps and uses personal information (also referred to as data) about job applicants and about current and former staff for a number of specific lawful purposes as set out in the Company's data protection privacy notices.
- For the purposes of this policy, staff include: employees, workers, consultants, contractors, volunteers and apprentices.
- This policy is non-contractual and the Company may amend it at any time. The Company will also review, and if necessary update, this policy in accordance with our data protection obligations.
- This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our workforce. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

Professional Codes and Standards as published by the Building Safety Regulator (BSR):

All clients / stakeholders should be aware that OWL BCS have an obligation to issue information (including sensitive information) to relevant bodies / individuals / regulatory bodies when required to do so by legislation (e.g. Building Act 1984) / governing requirements (e.g. RBI Code of Conduct).

OWL BCS is fully committed to adherence to Section 5 of the RBI Code of Conduct & Section 5 of the RBCA Professional Conduct Rules.

Definitions

criminal records information data breach	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures; means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
data subject personal information	means the individual to whom the personal information relates; (sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;

processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
sensitive personal information	(sometimes known as ‘special categories of personal data’ or ‘sensitive personal data’) means personal information about an individual’s race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual’s health, sex life or sexual orientation.

Data protection principles

- The Company will comply with the following data protection principles when processing personal information:
- we will process personal information lawfully, fairly and in a transparent manner;
- we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;
- we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;
- we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;
- we will keep personal information for no longer than is necessary for the purposes for which the information is processed; and
- we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Basis for processing personal information

- in relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

- review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:
- that the data subject has consented to the processing;
- that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- that the processing is necessary for compliance with a legal obligation to which the Company is subject;
- that the processing is necessary for the protection of the vital interests of the data subject or another natural person; or
- that the processing is necessary for the purposes of legitimate interests of the Company or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.
- except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);
- document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
- include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);
- where sensitive personal information is processed, also identify a lawful special condition for
- processing that information and document it; and
- where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

Sensitive personal information

- The Company may from time to time need to process sensitive personal information. We will only process sensitive personal information if:
 - we have a lawful basis for doing so as set out in paragraph above; and
 - one of the special conditions for processing sensitive personal information applies, e.g
 - the data subject has given explicit consent;
 - the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject;
 - the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

- processing relates to personal data which are manifestly made public by the data subject;
 - the processing is necessary for the establishment, exercise or defence of legal claims; or
 - the processing is necessary for reasons of substantial public interest.
- Before processing any sensitive personal information, staff must notify Cathy Brode, QMS Consultant of the proposed processing so that they may assess whether the processing complies with the criteria noted above.
- Sensitive personal information will not be processed until the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.
- The Company will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.

Data protection impact assessments (DPIAs)

- Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the Company is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:
 - whether the processing is necessary and proportionate in relation to its purpose;
 - the risks to individuals; and
 - what measures can be put in place to address those risks and protect personal information.
- During the course of any DPIA, the employer will, where appropriate, seek the views of employees (this may be a representative group) and any other relevant stakeholders.

Documentation and records

- We will keep written records of processing activities
- As part of our record of processing activities we document, or link to documentation, on:
 - information required for privacy notices;
 - records of consent;
 - controller-processor contracts;
 - the location of personal information;
 - DPIAs; and
 - records of data breaches.

- We may document our processing activities in electronic form so we can add, remove and amend information easily.

Individual rights

- You (in common with other data subjects) have the following rights in relation to your personal information:
- to be informed about how, why and on what basis that information is processed—see the Company’s data protection privacy notices;
- to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request—see section Subject access requests below;
- to have data corrected if it is inaccurate or incomplete;
- to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as ‘the right to be forgotten’);
- to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information but you require the data to establish, exercise or defend a legal claim; and
- to restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation’s legitimate grounds override your interests).
- If you wish to exercise any of the rights i, please contact Brian Gerhardt, Managing Director.

Subject access requests

- Data subjects have the right to request access to their personal data processed by us. Such requests are called subject access requests (SARs). When a data subject makes an SAR, we will usually take the following steps:
 - log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);
 - confirm the identity of the data subject who is the subject of the personal data. For example, we may request additional information from the data subject to confirm their identity;
 - search databases, systems, applications and other places where the personal data which are the subject of the request may be held; and

- confirm to the data subject whether or not personal data of the data subject making the SAR are being processed.
- If personal data of the data subject are being processed, we shall provide the data subject with the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing or by other (including electronic) means

The purposes of the processing;

- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients overseas;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
 - the existence of the right to request rectification or erasure of personal data or
 - restriction of processing of personal data or to object to such processing;
 - the right to lodge a complaint with the Information Commissioner's Office (ICO);
 - where the personal data are not collected from the data subject, any available information as to their source;
 - the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and
 - where personal data are transferred outside the EU, details of the appropriate safeguards to protect the personal data
- We shall also, unless there is an exemption, provide the data subject with a copy of the personal data processed by us in a commonly used electronic form (unless the data subject either did not make the request by electronic means or has specifically requested not to be provided with the copy in electronic form) within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.
- Before providing the personal data to the data subject making the SAR, we shall review the personal data requested to see if they contain the personal data of other data subjects.
If they do, we may redact the personal data of those other data subjects prior to providing

the data subject with their personal data, unless those other data subjects have consented to the disclosure of their personal data.

- If the SAR is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing the personal data or refuse to act on the request.
- If we are not going to respond to the SAR we shall inform the data subject of the reason(s) for not taking action and of the possibility of lodging a complaint with the ICO.

Individual obligations

- You may have access to the personal information of other members of staff, suppliers and customers or clients of the Company in the course of your employment or engagement. If so, the Company expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out in paragraph above.
- If you have access to personal information, you must:
 - only access the personal information that you have authority to access, and only for
 - authorised purposes;
 - only allow other Company staff to access personal information if they have appropriate authorisation;
 - only allow individuals who are not Company staff to access personal information if you
 - have specific authority to do so from Name;
 - keep personal information secure;
 - not remove personal information, or devices containing personal information (or which can be used to access it), from the Company's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and
 - not store personal information on local drives or on personal devices that are used for work purposes.
 - You should contact Name if you are concerned or suspect that any breaches of this policy have taken place (or is taking place or likely to take place).

Information security

- Information may be held at our offices and third party agencies, service providers, representatives and agents and in cloud based IT services.
- The Company will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:
- making sure that, where possible, personal information is pseudonymised or encrypted;
- ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- Where the Company uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by Name.

Retention of personal (and sensitive personal) information

- Personal information (and sensitive personal information) will be retained in accordance with Schedule 1.
- Personal information (and sensitive personal information) that is no longer required
- will be deleted permanently from our information systems and any hard copies will be destroyed securely.

Data breaches

- A data breach may take many different forms, for example:
 - loss or theft of data or equipment on which personal information is stored;

- unauthorised access to or use of personal information either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- blagging' offences, where information is obtained by deceiving the organisation which holds it.

The Company will:

- make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
- notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

Consequences of failing to comply

- The Company takes compliance with this policy very seriously. Failure to comply with the policy puts individuals whose personal information is being processed at risk, carries significant civil and criminal sanctions for the individual and the Company and may, in some circumstances, amount to a criminal offence by the individual.
- Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.
- If you have any questions or concerns about anything in this policy, do not hesitate to contact Brian Gerhardt, Managing Director.

Data sharing covered by the code

There is no formal definition of data sharing within the legislation, although the scope of this code is defined by section 121 of the DPA 2018 as “the disclosure of personal data by transmission, dissemination or otherwise making it available”. This includes:

- providing personal data to a third party, by whatever means;
- receiving personal data as a joint participant in a data sharing arrangement;
- the two-way transmission of personal data; and
- providing a third party with access to personal data on or via your IT systems.

For the purposes of this code, data sharing does not include providing data access to employees or contractors, or with processors such as third-party IT processors. Please read the paragraphs later in this section on sharing data with processors.

The following examples illustrate a range of data sharing types within the scope of the code:

- a one-way or reciprocal exchange of data between organisations;
- an organisation providing another organisation with access to personal data on its IT system for a specific research purpose;
- several organisations pooling information and making it available to each other or to a third party or parties;
- data sharing on a routine, systematic basis for an established purpose;
- one-off, exceptional or ad hoc data sharing; and
- one-off data sharing in an urgent or emergency situation.

Examples of real-life data sharing activities

- a bank disclosed personal data about its employees to an anti-fraud body;
- a primary school passed details about a child showing signs of harm to the police and social services;
- the police and Border Force exchanged information about individuals thought to be involved in serious crime;
- a supermarket gave information about a customer’s purchases to the police following an allegation of shoplifting;
- a secondary school provided information about its pupils to a research company for research purposes; and
- a multi-agency network group regularly exchanged information about individuals for safeguarding or social care purposes.

The code only applies to sharing personal data. Neither the UK GDPR, the DPA 2018, nor this code, applies to sharing information that does not constitute personal data. Some sharing doesn't involve personal data; for example, if an organisation is sharing information that cannot identify anyone (anonymous information; please refer to the ICO website for forthcoming guidance on anonymisation).

The position is different for pseudonymised data. Data which has undergone pseudonymisation is defined in the UK GDPR as data that can no longer be attributed to a data subject without the use of additional information. If you have pseudonymised the data according to the definition of the UK GDPR, such that the additional information could be used to re-identify a data subject within that data, then you must treat the pseudonymised data as personal data.

It is common to consider data sharing as falling into two main types of scenario:

- data sharing on a frequent and/or regular basis, also known as routine or 'systematic' data sharing, where the same data sets are regularly shared between the same organisations for an established purpose; and
- exceptional, one-off decisions to share data for a purpose that is ad hoc, unexpected or due to an urgent situation or an emergency.

Different approaches apply to these two scenarios, and the code reflects this. Most of the code concentrates on routine data sharing.

Routine data sharing

This is data sharing done on a regular basis in a routine, pre-planned way. It generally involves sharing data between organisations for an established purpose - perhaps with standardised data structures and values - at regular, scheduled intervals.

For example, a group of organisations might make an arrangement to share or pool their data for specific purposes, again on a frequent and/or regular basis.

If you are carrying out this type of data sharing, you should establish rules and agree procedures in advance.

Ad hoc or one-off data sharing

It is good practice to formalise your data sharing through a data sharing agreement. However in some instances you may decide, or be asked, to share data in ad hoc situations that are not covered by any routine arrangement or agreement. It is still possible to share data in this situation, but you should carefully assess the risks every time. We recommend that you make plans to cover such contingencies. Sometimes you may have to make a decision quickly about data sharing in conditions of real urgency, or even in an emergency situation. You should not be put off from data sharing in a scenario like this; in an urgent situation you should assess the risk and do what is necessary and proportionate. Please see the section later in this code on [Data sharing in an urgent situation or in an emergency](#).

Data pooling

Data pooling is a form of data sharing where organisations decide together to pool information they hold and make it available to each other, or to different organisations, for a specific purpose or purposes. The organisations should consider whether they are separate or joint controllers.

If the organisations are joint controllers, under Article 26 of the UK GDPR they must enter into a formal, transparent arrangement setting out agreed roles and responsibilities for complying with the

UK GDPR. For more details, you should refer to the guidance on controllers and processors on the ICO website.

Data sharing and reuse of data by competent authorities for non-law enforcement purposes

[Share\(Opens Share panel\)](#)

At a glance

- Personal data processed by competent authorities for law enforcement purposes under Part 3 of the DPA 2018 may be shared with another organisation or reused internally for non-law enforcement processing under the UK GDPR / Part 2 of the DPA 2018, provided that the processing is “authorised by law”.
- As a competent authority, you need to determine what the purpose of your proposed sharing or reuse is for and whether this is “authorised by law”. This might be provided by, for example, statute, common law, royal prerogative, or statutory codes.
- As the further processing of the personal data is no longer for law enforcement purposes, you need to have a lawful basis under Article 6 of the UK GDPR.
- As the personal data you want to share or reuse is likely to include criminal offence data, you need to meet the requirements of Article 10. This means you need either a condition for processing, or official authority for the processing. This is in addition to identifying a lawful basis under Article 6.
- If this includes special category data you need to identify a condition for processing under Article 9 as well as a lawful basis under Article 6.

Checklist

- We consider the purpose for further processing personal data (either sharing it or reusing it internally) for non-law enforcement purposes before processing in this way, and whether it is necessary and proportionate to do so. This new purpose must not be incompatible with the original law enforcement purpose.
- We determine whether the proposed sharing or reuse of data is “authorised by law”.
- We identify a lawful basis for processing under Article 6 of the UK GDPR before sharing or reusing personal data for non-law enforcement purposes.
- Before sharing or reusing criminal offence data for a non-law enforcement purpose, we check we have met the requirements of Article 10 of the UK GDPR. This means we either identify our official authority for the processing or identify a relevant condition in Schedule 1 of the DPA 2018. This is in addition to having a lawful basis under Article 6.
- We identify a condition for processing under Article 9 of the UK GDPR and any relevant condition in Schedule 1 of the DPA 2018 before sharing or reusing special category data. This is in addition to having a lawful basis under Article 6.
- We only process the minimum necessary amount of relevant and adequate personal data.

- We share or reuse the personal data in compliance with our other data protection duties and obligations.

What are the lawful bases for processing?

The lawful bases for processing are set out in **Article 6 of the UK GDPR**. At least one of these must apply whenever you process personal data:

(a) Consent:

the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract:

the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation:

the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests:

the processing is necessary to protect someone's life.

(e) Public task:

the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests:

the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

For more detail on each lawful basis, read the specific page of this guide.

Further Reading

<https://www.legislation.gov.uk/eur/2016/679/contents>

Article 7 Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Why is consent important?

The UK GDPR sets a high standard for consent, which must be unambiguous and involve a clear affirmative action (an opt-in).

It specifically bans pre-ticked opt-in boxes. It also requires distinct ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

You must keep clear records to demonstrate consent.

The UK GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.

Public authorities, employers and other organisations in a position of power may find it more difficult to show valid freely given consent.

You need to review existing consents and your consent mechanisms to check they meet the UK GDPR standard. If they do, there is no need to obtain fresh consent.

Consent is one lawful basis for processing, and explicit consent can also legitimise use of special category data. Consent may also be relevant where the individual has exercised their right to restriction, and explicit consent can legitimise automated decision-making and overseas transfers of data.

Genuine consent should put individuals in control, build trust and engagement, and enhance your reputation.

Relying on inappropriate or invalid consent could destroy trust and harm your reputation – and may leave you open to large fines.

When is consent appropriate?

Consent is one lawful basis for processing, but there are alternatives. Consent is not inherently better or more important than these alternatives. If consent is difficult, you should consider using an alternative.

Consent is appropriate if you can offer people real choice and control over how you use their data, and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair.

If you make consent a precondition of a service, it is unlikely to be the most appropriate lawful basis.

Public authorities, employers and other organisations in a position of power over individuals should avoid relying on consent unless they are confident they can demonstrate it is freely given.

What is valid consent?

Consent must be freely given; this means giving people genuine ongoing choice and control over how you use their data.

Consent should be obvious and require a positive action to opt in. Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly.

Consent must specifically cover the controller's name, the purposes of the processing and the types of processing activity.

Explicit consent must be expressly confirmed in words, rather than by any other positive action.

There is no set time limit for consent. How long it lasts will depend on the context. You should review and refresh consent as appropriate.

How should we obtain, record and manage consent?

Make your consent request prominent, concise, separate from other terms and conditions, and easy to understand. Include:

- the name of your organisation;
- the name of any third party controllers who will rely on the consent;
- why you want the data;
- what you will do with it; and
- that individuals can withdraw consent at any time.

You must ask people to actively opt in. Don't use pre-ticked boxes, opt-out boxes or other default settings. Wherever possible, give separate ('granular') options to consent to different purposes and different types of processing.

Keep records to evidence consent – who consented, when, how, and what they were told.

Make it easy for people to withdraw consent at any time they choose. Consider using preference-management tools.

Keep consents under review and refresh them if anything changes. Build regular consent reviews into your business processes.

Article 28 UK GDPR & Section 60 of the Data Protection Act 2018

Section 60 Processing under the authority of the controller or processor

A processor, and any person acting under the authority of a controller or processor, who has access to personal data may not process the data except—

- (a) on instructions from the controller, or
- (b) to comply with a legal obligation.

Article 28 Processor

Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under **[F1domestic law]**, that is binding on the processor with regard to the controller and that sets 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 subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

- (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by **[F2domestic law]**; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

- (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- (c) takes all measures required pursuant to Article 32;
- (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
- (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
- (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;
- (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless **[F3domestic law]** requires storage of the personal data;
- (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or **[F4other domestic law relating to data protection]**.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under **[F5domestic law]**, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data

protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in [F6 paragraph 8] of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

F77.....

8. [F8 The Commissioner] may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article F9... .

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Further Reading

Relevant provisions in the UK GDPR - See

<https://www.legislation.gov.uk/eur/2016/679/contents>

Data sharing request form template

For use by the organisation making the request for data sharing

Name of organisation

Name and position of person requesting data

If requester is not the data protection officer (DPO) or equivalent, have they been consulted and their views considered?

Date of request

Description of data requested

☐ Joint ☐ Separate

Data controller relationship:

Will we have a data sharing agreement in place?

☐ Yes ☐ No

Purpose of sharing

Does processing involve any special category data ☐ Yes ☐ No
(or sensitive processing under part 3 DPA 2018)?

Are there any specific arrangements for retention / deletion of data?

Are there any circumstances in the proposed sharing that might result in a risk to individuals?

Date(s) provision of data is required