# Data sharing induction pack
# Grosvenor Hart Homes

GROSVENOR

GROSVENOR

# Contents

# 1. Introduction to your role as a data controller

Data protection is relevant to everyone since it involves individuals and their rights and responsibilities. The law in the UK is governed by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

Data protection legislation aims to give individuals control over their personal data. This ensures that individuals are at the core of everything an organisation does. By complying with data protection requirements, it shows that individuals can trust you with their personal data.

You are sharing personal data with Grosvenor Hart Homes (GHH) and/or we are sharing personal data with you. Specific details are in the information-sharing charter and agreement. Since we are in a sharing relationship, you have the role of 'data controller'. A data controller is the main decision-maker – they have overall control over the purposes and means of processing personal data.

As you are in a personal data sharing relationship, we have created this induction pack to assist you in this role, it covers the following:

- What we expect of your organisation
- What you need to do to meet the requirements of data sharing
- What support we can provide
- Guidance to help you in this role, including key data protection guidance, GDPR principles, a list of lawful processing conditions and useful links from the Information Commissioner's Office.

# 2. What we expect of your organisation

1. You have appointed someone who is responsible for data protection, confidentiality, and information security.
2. You pay the fee to the Information Commissioner's Office (ICO) (see 7.3.10 in the 'Data protection key guidance' below) if you currently do not pay it.
3. You review how you manage personal information and take any required action to improve security (see 7.3.3 in the 'Data protection key guidance' below).
4. You read guidance on the ICO website and take required actions (see useful links from the Information Commissioner's Office on page 13).
5. You and any your personnel how to quickly respond to and report information security breaches involving personal data (see 7.3.5 in the 'Data protection key guidance' below).
6. You implement policies and/or procedures for how your personnel appropriately and lawfully handle personal data and share these with us upon request.
7. You provide clear information about how you use personal data through a privacy notice (see 7.3.6 in the 'Data protection key guidance' below) and share this with us upon request.
8. You train all your personnel on the use, management, and handling of personal data (see Do you know what to include in your data protection training? | ICO).
9. You securely destroy information held electronically and/or on paper when it is no longer needed (see 7.3.3.1 and 7.3.3.2 in the 'Data protection key guidance' below).

10. You review the data processors used in your organisation and take necessary actions (see 7.3.8 in the 'Data protection key guidance' below).
11. You create a record of processing activities (see 7.3.11 in the 'Data protection key guidance' below).

# 3. What you need to do to meet the requirements of data sharing:

1. Return or destroy all relevant personal data provided to you by us in connection with the information sharing agreement.
2. Ensure your staff keep personal data confidential.
3. Report data breaches to us by:
    - Telephone: 01244 684609
    - Email: data.protectionFO@grosvenor.com
4. If you receive a request from someone about their personal data and you have their data, assist us in handling their request properly according to the rules.
5. Provide copies of information on how you are processing personal data in relation to the information sharing agreement.

# 4. Support from Grosvenor Hart Homes

We appreciate that meeting data protection requirements can be daunting, even after you've read the information in this pack and looked at the Information Commissioner's Office website. Therefore, if you have any questions or need any assistance in ensuring you meet the requirements of a data controller, please don't hesitate to contact us:

- Telephone: 01244 563777
- Email: hello@grosvenorhart.com

# 5. Guidance to help you in this role

This packs includes the following information to help you:

- Data protection key guidance
- GDPR principles
- List of lawful processing conditions
- Useful links from the Information Commissioner's Office

# 6. Indemnity

GHH has made every attempt to ensure the accuracy and reliability of this document. However, this document is provided "as is" without warranty of any kind. GHH does not accept any responsibility or liability for the accuracy, content, completeness, legality, or reliability of this document.

No warranties, promises and/or representations of any kind, expressed or implied, are given as to the nature, standard, accuracy or otherwise of this document nor to the suitability or otherwise of the document for your particular circumstances.

GHH shall not be liable for any loss or damage of whatever nature (direct, indirect, consequential, or other) whether arising in contract, tort or otherwise, which may arise as a result of your use of (or inability to use) this document.

By providing this document to you, GHH are not giving legal or financial advice.

# 7. Data protection key guidance

## 7.1 What is personal data?

Information is considered personal data if both are true:

1. It relates to a living individual.
2. It is about an individual (or their household or device).

An individual can be identified from this information alone or by combining it with other information held by the organisation or others. Identification can be through 'real world' identifiers like name and address, or 'digital' identifiers like email, IP address, browser cookie, serial numbers, coordinates, employee ID, or facial recognition data. Other examples include:

- Date of birth
- Passport number
- Bank account details

It also includes personal opinions about people. So, if you write something unpleasant about someone in a work context, they have the right to see it.

Some personal data is classified as 'special category data' and needs extra care due to potential risks. This includes information about health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, sex life/sexual orientation, or criminal convictions. It also includes biometrics used for identification, like fingerprints or facial recognition.

## 7.2 What is processing

The GDPR and DPA regulate how you handle personal data. Examples of what you might do include:

- Storing customers' personal data in paper files, emails, etc
- Collecting personal data from job applicants during interviews
- Updating personal data for contacts in other organisations
- Recording CCTV footage
- Sharing personal data of tenants, customers, etc.
- Keeping customers' details secure from those who don't need access

## 7.3 GDPR requirements

### 7.3.1 Data protection principles

There are six principles, including an accountability principle, which requires organisations to show they comply with these principles. For more details, see 'GDPR principles' on page 12.

### 7.3.2 Accountability requirement

You need to make compliance a core part of your organisation and be ready to prove it if asked. This means you'll need to keep more detailed records related to data protection, which is unavoidable.

You also need to show that you've included technical and organisational measures in your data processing activities. This approach is called privacy by design and default, meaning privacy should be a fundamental part of your processing activities.

### 7.3.3 Considerations for managing information

#### 7.3.3.1 Working Electronically

- Where you save files: Ensure files are stored securely and only accessible to those who need them.
- How you share files: Make sure files are sent to the correct recipients, especially if they have similar names.
- How long you keep files: Determine the appropriate retention period for electronic files.
- Please see Practical methods for destroying documents that are no longer needed | ICO for more information.

#### 7.3.3.2 Working on Paper

- Storing paper: Keep paper documents in a safe and secure place.
- Method of transfer: Ensure you send the correct personal data without mixing it with others. Use special or hand delivery if tracking is needed.
- Confidential disposal: Use a confidential waste company or a crosscut shredder to dispose of personal data. Please see Practical methods for destroying documents that are no longer needed | ICO for more information.
- How long you keep paper: Determine the appropriate retention period for paper documents.

#### 7.3.3.3 Work Environment

- Office security: Ensure your office or workspace is secure.
- Computer screen: Position your screen to prevent others from seeing it.
- Left on desks: Do not leave personal data out at the end of the day or when finished. Consider who might access it.

#### 7.3.3.4 Confidential Conversations

- Private discussions: Avoid discussing sensitive information in public places like cafes or on trains.

Please see How secure is your personal data? | ICO for more information.

### 7.3.4 Lawfulness of processing

You need a valid reason to process personal data, and no single reason is better than another. Most reasons require that processing is necessary. If your purpose changes, you might still be able to use the original reason if the new purpose is similar.

For special category data, you need both a general reason and an extra condition for processing.

Check the 'List of lawful processing conditions' on page 14 for more details.

If you use consent as your reason, it must be separate from other agreements and clearly presented. People can withdraw consent at any time. You can't make services dependent on consent, especially if there's an imbalance of power. For marketing via email or text, you need valid prior consent from the recipient.

### 7.3.5 Data breach response

You must report any breaches of our personal data to us immediately by calling XXXXX or emailing xxxx

When a personal data breach happens, you need to assess the risk to people's rights and freedoms. If there's likely to be a risk, you must notify the Information Commissioner's Office (ICO). If it's unlikely, you don't need to report it. This must be done within 72 hours of becoming aware of the breach, if possible.

If the breach is likely to have a high risk of negatively affecting individuals' rights and freedoms, you must also inform those individuals without delay.

Ensure you have strong procedures for detecting, investigating, and reporting breaches internally. This helps decide if you need to notify the ICO and the affected individuals.

You must keep a record of all personal data breaches, even if you don't need to notify the ICO.

See 72 hours - how to respond to a personal data breach | ICO for further information.

### 7.3.6 Collecting personal data

Consider if you collect personal data through:

- Online forms
- Paper forms
- Over the telephone

Under GDPR, we must provide clear information about how we use personal data. Not providing this information breaches GDPR principles and individual rights. We should give enough information upfront and tell people where to find more details.

A privacy notice is a statement that explains how your business collects, uses, and protects personal data. It's important because it helps build trust with your customers by showing that you respect their privacy and comply with the law. You provide your privacy notice on your website (if you have one) and at the point of data collection, ensuring it's easy to find and understand.

Please see the following additional assistance and guidance:

- Are you transparent about how you use peoples data? | ICO
- Create your own privacy notice | ICO

### 7.3.7 Rights of individuals

Individuals have the following rights regarding their personal data:

- To access their own personal data
- To receive it in a portable format
- To have it erased
- To have it corrected if inaccurate
- To have its use restricted
- To object to its use, especially for marketing and profiling
- To object to automated decisions made about them

The following rules apply:

- No charge can be made to an individual unless the request is clearly unfounded or excessive due to its repetitive nature.
- Organisations must respond promptly, within one month. This can be extended by two months if the request is complex or if there are multiple requests from the same individual.

If we receive a request for personal data, we may need to contact you to access any personal data you are processing for us.

If an individual asks you about the personal data you hold on them as part of your work for us, you must notify us immediately by emailing: data.protectionFO@grosvenor.com

Please see How to deal with a request for information: a step-by-step guide | ICO for more information.

### 7.3.8 Using data processors

You may also use a data processor or data processors for your own purposes. Examples include:

- Using a company for payroll
- Hiring a printer to send invitations
- Using an external website provider that collects personal information

If you use a data processor, you must have a contract that includes data protection obligations. This ensures the data processor meets GDPR requirements with proper technical and organisational measures. This applies whether you're processing our data or your own.

The contract should cover:

- The subject of the processing
- The duration of the processing
- The nature and purpose of the processing
- The type of personal data involved
- The categories of data subjects

- Your obligations and rights

The contract must state that:

- The processor acts only on your instructions, unless required by law
- The processor ensures data handlers are bound by confidentiality
- The processor takes measures to secure the data
- The processor only uses sub-processors with your approval and under a written contract
- The processor helps you respond to individuals' rights requests
- The processor assists you with GDPR obligations, including security, breach notifications, and impact assessments
- The processor deletes or returns all personal data at the end of the contract, unless legally required to keep it
- The processor allows audits and inspections
- The processor must delete or return all personal data to you (at your choice) at the end of the contract, and the processor must also delete existing personal data unless the law requires its storage
- The processor must submit to audits and inspections

### 7.3.9 Fees regime

Every organisation, including sole traders, that processes personal data must pay a data protection fee to the Information Commissioner's Office (ICO), unless exempt. You don't need to pay a fee if you process personal data only for:

- Staff administration
- Advertising, marketing, and public relations
- Accounts and records
- Not-for-profit purposes
- Personal, family, or household affairs
- Maintaining a public register
- Judicial functions
- Processing personal information without an automated system like a computer

The ICO publishes some of this information on the register of controllers.

For more information, visit: Data protection fee | ICO

There are three tiers of fees:

- **Tier 1 – Micro organisations:** Turnover up to £632,000 or no more than ten staff. Fee: £40 (£35 if paid by direct debit)
- **Tier 2 – SMEs:** Turnover up to £36 million or no more than 250 staff. Fee: £60

- **Tier 3 – Large organisations:** Those not meeting Tier 1 or 2 criteria. Fee: £2,900

#### 7.3.10 Record of processing activities

You need to record the following for each processing activity:

- Purposes of processing
- Description of categories of individuals and personal data
- Categories of recipients of personal data
- Details of transfers to third countries, including safeguards
- Retention and disposal periods
- Description of technical and organisational security measures

For organisations with:

- **250 or more employees:** Document all processing activities
- **Less than 250 employees:** Document activities that are not occasional, could risk individuals' rights and freedoms, or involve special categories of data or criminal data

For a template, visit: How do we document our processing activities? | ICO

#### 7.3.11 Data Protection Impact Assessments (DPIA)

DPIAs are mandatory under GDPR to assess potential risks to personal data. They are needed for new initiatives or changes that might impact personal data, such as:

- Implementing a new IT system
- Installing fingerprint technology for access controls
- Collecting new types of personal data

### 7.4 Offences, remedies, and fines

#### 7.4.1 Unlawful obtaining

If an employee knowingly or recklessly obtains, discloses, or keeps personal data without the organisation's consent, they can be personally fined in the magistrate's court. The fine amount is not fixed and is not a recordable offence.

#### 7.4.2 Alteration

If you receive a request for personal data and then destroy any of it, you can be fined. For example, if a manager writes something negative about a candidate on an interview note, keeps it within the team, and then shreds it when the candidate asks to see all interview notes, the manager can be fined.

#### 7.4.3 Directors' imprisonment

Directors can be prosecuted (fined or imprisoned) if an organisation commits an offence with their consent, participation, or neglect.

### 7.4.4. Organisations fined

Fines have increased significantly. They can be imposed instead of, or alongside, other measures ordered by the ICO. Each case is assessed individually.

7.4.4.1 Fines of up to €10 million or 2% of the total annual worldwide turnover (whichever is higher) can be imposed for issues such as:

- Implementing technical and organisational measures for data protection by design and default
- Engaging data processors
- Maintaining written records of processing activities
- Keeping records of personal data being processed
- Co-operating with the ICO
- Reporting breaches as required by GDPR
- Conducting data protection impact assessments
- Appointing a Data Protection Officer (DPO)

7.4.4.1 Fines of up to €20 million or 4% of the total annual worldwide turnover (whichever is higher) can be imposed for issues such as:

- Data protection principles
- Individuals' rights
- Transferring personal data outside the EEA (including using IT systems with servers outside the EEA)
- Specific UK legal requirements
- Not complying with the ICO's instructions

# 8. GDPR principles

These are outlined in Article 5 of the GDPR.

| **Principle** | **What this means in practice** |
|---|---|
| 1. Processed lawfully, fairly and in a transparent manner in relation to individuals | 2. A legal basis for processing personal data must be identified and documented.<br>3. Individuals are provided with the following information:<br>a. Why their personal data is collected and used.<br>b. The risks, rules, safeguards, and rights related to the processing of their personal data, and how to exercise their rights. |

| | |
|---|---|
| | c. The legal basis for processing their personal data.<br>4. This information is provided in an easily accessible and understandable manner.<br>5. We do not use personal data in ways that have unjustified adverse effects on individuals.<br>6. We ensure that we do not do anything unlawful with personal data. |
| 2. Personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes | 1. Be clear from the start about why we are collecting personal data and what we will do with it.<br>2. To decide if a new use of personal data is compatible with the original purpose (if not based on consent), consider:<br>a. The context in which the data was collected.<br>b. The nature of the personal data.<br>c. The possible consequences of the new processing.<br>d. The safeguards in place. |
| 3. Personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. | 1. Collect only the personal data you need for the specified purposes.<br>2. Do not keep more personal data than necessary for that purpose. |
| 4. Personal data is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. | 1. Accurately record personal data provided by the individual or another source.<br>2. Take reasonable steps to ensure the data's accuracy.<br>3. If someone challenges the data's accuracy, make this clear to those accessing it.<br>4. Erase or correct inaccurate data if needed. |
| 5. Personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research | 1. Keep personal data only for specific time periods.<br>2. Securely destroy personal data when its retention period ends. |

| | | |
|---|---|---|
| | purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals. | |
| 6. | Personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. | Ensure you have appropriate security measures to prevent personal data from being accidentally or deliberately compromised. |

# 9. Lawful basis for processing personal data

Process personal data fairly and lawfully.

- Ensure at least one condition in Article 6 is met.
- For special category data, ensure at least one condition in Article 9 is also met.

## 9.1 Article 6 Conditions

1. Consent: The individual has given consent for specific purposes. Obtaining consent is harder under GDPR and should be avoided if possible.
2. Child Consent: For online services, a child under 16 needs parental authorisation.
3. Vital Interests: Processing is necessary to protect someone's vital interests, typically in medical emergencies.
4. Legal Obligation: Processing is necessary to comply with a legal obligation under, even if the law is not statutory.
5. Performance of a Contract: Processing is necessary to perform a contract with the individual or to take steps at their request before entering a contract.
6. Public Functions: Processing is necessary for tasks carried out in the public interest or in the exercise of official authority as defined in law.
7. Legitimate Interests: Processing is necessary for the legitimate interests of the controller or a third party, unless overridden by the individual's rights, especially if the data subject is a child.

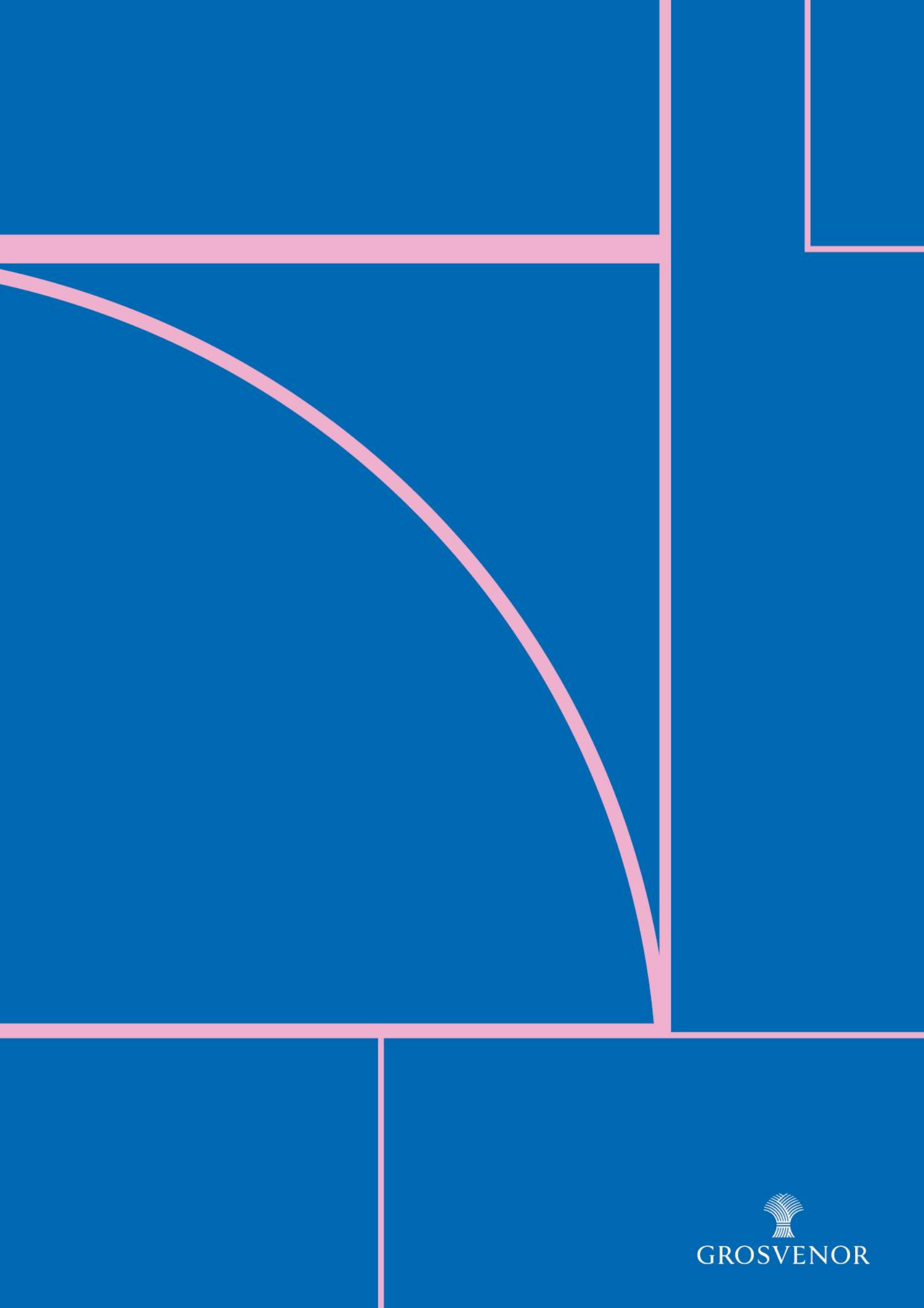
## 9.2 Article 9 conditions

1. Explicit Consent: The individual has given explicit consent.
2. Vital Interests: Processing is necessary to protect someone's vital interests, typically in medical emergencies.

3. Legal Obligation Related to Employment: Processing is necessary for legal obligations in employment and social security law, such as a collective agreement.
4. Not-for-Profit Bodies: Processing is done for legitimate activities of a not-for-profit body and only involves members or related persons. Personal data is not shared outside the body without consent.
5. Public Information: Processing involves personal data that the individual has made public.
6. Legal Claims: Processing is necessary for legal claims or when courts are acting in their judicial capacity.
7. Substantial Public Interest: Processing is necessary for substantial public interest.
8. Healthcare: Processing is necessary for healthcare purposes and includes suitable safeguards.
9. Public Health: Processing is necessary for public health purposes and includes suitable safeguards.
10. Archive: Processing is necessary for archiving, scientific or historical research, or statistical purposes.

# 10. Useful links from the Information Commissioner's Office

- Information Commissioner's Office (ICO) website: https://ico.org.uk/
- How well do you comply with data protection law: an assessment for small business owners and sole traders | ICO
- Advice for small organisations | ICO
- UK GDPR guidance and resources | ICO


GROSVENOR