Data sharing induction pack

GROSVENOR

Contents

Introduction to your role as a data controller

Welcome!

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

Data protection legalisation aims to empower individuals and give them control over their personal data. It has the benefit of ensuring that individuals are put in the heart of everything that an organisation does. By meeting data protection requirements, it has the benefit of demonstrating that individuals can trust you with their personal data.

You are sharing personal data with the 4th Duke of Westminster's 1964 Settlement and/or we are sharing personal data with you. Specific information is 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 exercise overall control over the purposes and means of the processing of personal data.

As you are in a personal data sharing relationship, we have created this induction pack to help you in this role.

What you need to meet the requirements of data sharing

The key requirements are outlined below:

- Report data breaches (see 1.3.5 in data protection key guidance section) to us by:
  - Telephone on 01244 684400; and
  - Email to Data.protectionFIO@grosvenor.com
- Assist us in complying with data subject rights (see 1.3.6 in data protection key guidance section)
- Upon request:
  - Return or destroy all relevant personal data provided to you by us in connection with the information sharing agreement.
  - Provide copies of information on how you are processing the personal data in relation with the information sharing agreement.

Guidance to help you in this role

This packs includes the following information to help you:

- Confidentiality requirements
- Data protection checklist
- Data protection key guidance
- GDPR principles
- List of lawful processing conditions
- Role of Data Protection Officer
- Useful links from the Information Commissioner's Office

Support from Grosvenor

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 Alex Hodge, Information Governance Manager:

- 01244 684609
- Data.protectionFIO@grosvenor.com

Data protection checklist

The following is a checklist of actions to ensure you are meeting your data protection requirements.

- Review how you manage information and take any required action to improve security (see 1.3.3 in the 'Data protection key guidance' below)
- Review what data processors are used in your organisation and take required actions (see 1.3.7 in the 'Data protection key guidance' below)
- Pay the fee to the Information Commissioner's Office (ICO) (see 1.3.9 in the 'Data protection key guidance' below)
- Create record of processing activities using template on ICO website (see 1.3.10 in the 'Data protection key guidance' below)
- Read guidance on ICO website for small businesses (if applicable) and take required actions (see useful links from the Information Commissioner's Office on page 19)

Confidentiality requirements

You may also have a confidentiality agreement with us which sets out specific information. This could be because you provide services to us. As such you may have come to know and/or become aware of information of a confidential and/or private nature about the Grosvenor Family Office and Rural Estates and/or Grosvenor Family.

If you do have a confidentiality agreement with us, the following are key requirements that you need to follow. 'You' in this contract means, you, your organisation, and the following:

- Employees, including all those that are permanently employed or on a fixed term contract
- Sub-contractors and/or subsidiary companies

1. You will not at any time directly or indirectly, disclose, divulge, or make unauthorised use of any Confidential Information.
2. You will keep any Confidential Information provided to you as part of your role strictly confidential and accordingly you must not disclose it to any other person outside of your employment at Grosvenor.
3. You will not take any photographs, other than where strictly required in connection with the work for which you have been contracted.
4. You will not post or share images, statuses, comments and/or content on any form of social media which is part of your day-to-day work for the Grosvenor Estate and/or is related to the Grosvenor Family in any way.
5. You will not remove any information from the work environment without prior written authorisation.
6. You will be very careful when discussing Confidential Information, where you may be overheard by those who have no right to access the Confidential Information.
7. You will only access Information that you have a right to see as part of the role you are carrying out for us.
8. You will only share Confidential Information with other people and organisations where it is necessary to do so as part of your role.
9. You will not allow anyone to gain unauthorised access to a restricted area by tailgating, which is to avoid or bypass security measures by following you or another person through a door or gate, without consent.

You must immediately inform the Grosvenor Family Office and Rural Estates if you become aware of the possession, use or knowledge of Confidential Information by any person not authorised to possess, use, or have knowledge of it. to us by:

- Telephone on 01244 684400; and
- Email to Data.protectionFIO@grosvenor.com

Data protection key guidance

1.1 What is personal data?

Information will be defined as personal data if the following are both true:

1. The information relates to a living individual.
2. If the information is in anyway about an individual (or their household or device)

The individual can be identified from the information alone or by using other information held by the organisation or others

An individual can be identified from 'real world' identifiers such as name and address but also from 'digital' identifiers such as email, IP address, browser cookie, serial numbers, longitude and latitude coordinates, employee ID or facial recognition information. Other examples of identifiers are:

- Date of birth
- Passport number
- Bank account details

It also includes personal opinions on people too! So, if you wrote something not very pleasant about someone else in a work capacity then they have the right to see it.

There is also some personal data that is classified as '**special category data**'. This personal data needs to be managed even more sensitively due to potential risks and includes health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, sex life/sexual orientation or criminal convictions. It also includes biometrics (where used for ID purposes) such as fingerprint or face recognition.

1.2 What is processing

The GDPR and DPA regulate the 'processing' of personal data. Examples of processing you could carry out could include:

- Holding customers' personal data within paper files, emails, etc.
- Obtaining personal data about job applicants during a job interview
- Altering the personal data relating to the names of people in other organisations that you need to contact
- Recording of CCTV images
- Disclosing personal data to you of tenants, customers, etc.
- Keeping secure the details of customers from those that don't need to see them

1.3 GDPR requirements

1.3.1 Data protection principles

There are six principles including a new accountability principle which makes organisations responsible for demonstrating compliance with the principles. Please see 'GDPR principles' on page 12 for more information.

1.3.2 Accountability requirement

You must embed compliance into the fabric of your organisation and demonstrate compliance if challenged. The impact of this is that your record keeping associated with data protection will increase. Unfortunately, this is something that is unavoidable.

You will also have to demonstrate that you have considered and integrated technical and organisational measures into your processing activities. This is known as privacy by design and default – there must be a presumption of privacy in your processing activities.

1.3.3 Considerations for managing information

1.3.3.1 Working electronically

If you are working electronically you need to consider the following:

- **Where you save files**

  Is it only held where it can be accessed by others and only by those that need to see it?

- **How do you share it?**

  Is it being sent to the right people, especially with people with the same or similar surnames?

- **How long do you keep it?**

1.3.3.2 Working on paper

If you are working on paper, you need to consider the following:

- Storing paper

  Is it kept in a safe and secure place?

- Method of transfer

  Are you sending the correct personal data, without other people's personal data mixed with it?

  If you are sending externally do you need to send it by special delivery (if you need to track it) or hand delivery?

- **Confidential disposal**

  Are you using a confidential waste company or a crosscut shredder to get rid of any personal data?

- **How long do you keep it?**

1.3.3.3 Work environment

- **Office**

  Is your office or other place where you work secure?

- **Computer screen**

  Is your screen positioned in a way to stop people seeing what is on it?

- **Left on desks**

Do you leave personal data out at the end of the day or when you have finished with it? Think who else could get access to it.

1.3.3.4 Confidential conversations

There are certain things that you may not want to discuss in front of others. This also includes when you are out and about, such as in cafes, on trains, etc.

1.3.4 Lawfulness of processing

You must have a valid lawful basis to process personal data and no single basis is 'better' or more important than the others. Most lawful bases require that processing is 'necessary'. If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose.

If you are processing special category data, you need to identify both a lawful basis for general processing and an additional condition for processing.

See the 'List of lawful processing conditions' on page 14 for more information on the different processing 'conditions.

If you are using consent as a lawful basis it must now be separable from other written agreements and clearly presented, since individuals have the right to withdraw consent at any time. The supply of services cannot be made conditional on consent, and so avoid relying on consent where there is a clear imbalance between the individual and the organisation. Marketing via email and text message may not be sent to a recipient unless that recipient has given valid prior consent to receiving such communications.

1.3.5 Data breach response

You must report all breaches of any of our personal data to us immediately by calling the Eaton Estate Office on 01244 684600 and emailing Data.protectionFIO@grosvenor.com.

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then you must notify the Information Commissioner's Office. If it's unlikely then you don't have to report it. You must do this within 72 hours of becoming aware of the breach, where feasible.

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

You should ensure you have robust breach detection, investigation, and internal reporting procedures in place. This will facilitate decision-making about whether you need to notify the relevant supervisory authority and the affected individuals.

You must also keep a record of any personal data breaches, regardless of whether you are required to notify the Information Commissioner's Office.

1.3.6 Rights of individuals

The following are the rights individuals have with their personal data:

- To access their own personal data
- To have it provided to them in a portable format
- To have it erased

- To have it rectified if inaccurate
- To have it restricted
- To object to the way it is used, especially around marketing and profiling
- To object to it being used to make automatic decisions about them

The following apply:

- No charge can be issued to an individual, unless they are manifestly unfounded or excessive, due to their repetitive character; and
- Organisations must respond without undue delay, and within one month. This can be extended by two months where the request is complex, or organisations receive several requests from the individual requirements.

An individual may ask you what personal data you hold on them, as part of the data sharing. If this is the case, you must notify us straight away by emailing Data.protectionFIO@grosvenor.com.

1.3.7 Using data processors

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

- If you use a company to carry out your payroll
- If you use a printer to send out invitations to individuals
- If you use an external website provider and the website collects personal information when someone visits the website

If you do use a data processor, you must put a 'contract' in place imposing data protection obligations on that data processor. This should include that the data processor will provide enough guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the GDPR's requirements. This is also the same if you are going to use a processor for your own purposes and where you are not processing our personal data. The following states what to include in the 'contract':

- The subject matter 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 subject
- Your obligations and rights

The contract or other legal act includes terms or clauses stating that:

- The processor must only act on your documented instructions, unless required by law to act without such instructions
- The processor must ensure that people processing the data are subject to a duty of confidence
- The processor must take appropriate measures to ensure the security of processing

- The processor must only engage a sub-processor with your prior authorisation and under a written contract
- The processor must take appropriate measures to help the controller respond to requests from individuals to exercise their rights
- Considering the nature of processing and the information available, the processor must assist you in meeting your GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments
- The processor must delete or return all personal data to 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

1.3.8 Fees regime

Every organisation, including sole traders, who processes personal data needs to pay a data protection fee to the Information Commissioner's Office (ICO), unless they are exempt. Organisations don't need to pay a fee if you are processing personal data only for one (or more) of the following purposes:

- 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 such as a computer

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

For more information please click on this link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-fee/

There are three tiers of fees that you need to pay the ICO unless you are exempt from paying the fee:

- Tier 1 – Micro organisations. Maximum turnover of £632,000 or no more than ten members of staff. Fee: £40 (or £35 if paid by direct debit)
- Tier 2 – SMEs. Maximum turnover of £36million or no more than 250 members of staff. Fee: £60
- Tier 3 – Large organisations. Those not meeting the criteria of Tiers 1 or 2. Fee: £2,900

This is a link to the ICO website about the fees regime: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-fee/

1.3.9 Record of processing activities

The following is what needs to be recorded for each processing activity:

- Purposes of your processing
- Description of the categories of individuals and categories of personal data
- Categories of recipients of personal data
- Details of your transfers to third countries including documenting the transfer mechanism safeguards in place
- Retention and disposal periods
- Description of your technical and organisational security measures

For the record of processing activities there are two tiers depending upon the number of employees:

- 250 or more employees, you must document all your processing activities
- Less than 250 employees, you only need to document processing activities that:
- are not occasional; or
- could result in a risk to the rights and freedoms of individuals; or
- involve the processing of special categories of data or criminal conviction and offence data

This is a link to the record of processing activities template on the ICO website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

1.3.10 Collecting personal data

Think about if you collect personal data from people, via any of the following:

- Online forms
- Paper forms
- Over the telephone

Under GDPR we need to provide more information about what we do with an individual's personal data, but we need to do so in an understandable way. There are issues in not providing the information, breaching both a fundamental principle of GDPR and not complying with a specific individual right. It doesn't mean that we give them the detail up front if we give them enough information and tell them where they can find out more.

1.3.11 Data Protection Impact Assessments (DPIA)

These are mandatory under GDPR and they are a structured way of assessing potential risks to personal data. They need to be carried out for any new initiative or changes to an existing way of working that might impact on personal data.

These are the following examples of when a DPIA would be required:

- Before implementing a new IT system.
- Before installing fingerprint technology for access controls; or
- Before collecting any new type of new personal data.

1.3.12 Data Protection Officer (DPO)

It is mandatory for certain organisations to designate a DPO:

- As a core activity, individuals are monitored regularly, systematically and on a large scale and/or
- Process special categories of personal data on a large scale.

See the 'Role of Data Protection Officer' on page 17 for more information.

1.4 Offences, remedies, and fines

1.4.1 Action against the data processor

An individual can also bring a claim directly against a data processor in court. A data processor can be held liable to pay compensation for any damage caused by data processing. A data processor will only be liable for the damage if:

- it has failed to comply with GDPR provisions specifically relating to processors; or
- it has acted without the data controller's lawful instructions, or against those instructions.

The data processor will not be liable if it can prove it is not responsible for the event giving rise to the damage.

If a data processor is required to pay compensation, but is not wholly responsible for the damage, it may be able to claim back from the data controller, the share of the compensation for which they are responsible.

1.4.2 Unlawful obtaining

If an employee knowingly or recklessly obtains, discloses, or retains personal data without the consent of the organisation, action can be taken against them personally. They could then have to pay a fine in the magistrate's court. The fine is not fixed at any amount and is not a recordable offence.

1.4.3 Alteration

In addition, if you get a request for personal data about an individual and then destroy any of the personal data, then you can be fined for this as well.

An example is when a Manager writes something horrible about a candidate on their paper job interview note. The interview note is kept in the team and not sent to HR. The employee asks to see all interview notes. The manager shreds the note and is discovered doing so.

1.4.4 Directors imprisonment

Directors, etc. can be prosecuted (either fined or imprisoned) if an organisation commits an offence and it is proved that the offence was committed with their consent, participation, or neglect.

1.4.5 Organisations fined

Fines have increased dramatically. They are to be imposed instead of, or in addition to, measures that may be ordered by the ICO. They are imposed on a case by case basis.

1.4.5.1 10m Euro or 2% of the undertaking's total annual worldwide turnover in the preceding financial year, whatever is higher.

These fines would be imposed if there were specific issues with the following:

- Implementing technical and organisational measures to ensure data protection by design and default
- In relation to the engagement of data processors
- Maintaining written records of processing activities
- Records of what personal data you are processing
- Co-operating with the ICO
- Reporting breaches when required by the GDPR
- Conduct of data protection impact assessments or
- Appointment of the DPO role

1.4.5.2 20m Euro or 4% of the undertaking's total annual worldwide turnover in the preceding financial year, whatever is higher.

These fines would be imposed if there were specific issues with the following:

- Data protection principles.
- Individuals rights.
- Transfer of personal data outside the EEA (EU plus Iceland, Liechtenstein, and Norway). This also includes when we use IT systems and their servers are held outside of the EEA;
- Specific UK legal requirements; or
- Not doing what the Information Commissioner's Office tells you.

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	1. There needs to be a legal basis identified for the processing of personal data and this is documented. 2. The following information is provided to individuals: a. Why personal data is collected and used. b. The risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights. c. The legal basis for processing the personal data. 3. The information is provided to them is easily accessible manner and is easy to understand. 4. We do not use personal data in ways that have unjustified adverse effects on the individuals concerned. 5. You make sure 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 considered to be incompatible with the initial purposes	1. You are clear from the outset about why we are collecting personal data and what we intend to do with it. 2. The following is considered to assess whether a new processing purpose is compatible with the purpose for which the personal data was initially collected, if not based on consent: a. the context in which personal data has been collected b. the nature of the personal data c. the possible consequences of the proposed processing; and d. the existence of safeguards
3: Personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.	1. You only collect personal data needed for the purposes you have specified. 2. You do not hold more personal data than you need 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. You accurately record personal data provided by the individual concerned, or by another individual or organisation. 2. You have taken reasonable steps in the circumstances to ensure the accuracy of the personal data.

	3. If an individual has challenged the accuracy of the personal data, this is clear to those accessing it. 4. If required inaccurate personal data is erased or rectified.
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 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.	1. You keep personal data for specific time periods. 2. You securely destroy personal data when it has come to the end of its retention period.
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.	1. You must have appropriate security to prevent the personal data we hold being accidentally or deliberately compromised

Lawful basis for processing personal data

Principle 1

Personal data shall be processed fairly and lawfully and **shall not** be processed **unless**:

a) at least **one of the conditions in Article 6** is met and
b) in the case of **sensitive personal data**, at least **one of the conditions in Article 9** is also met

Article 6 Conditions	**Article 9 Sensitive Personal Data Processing Conditions** Members States can introduce additional conditions in relation to health, genetic or biometric data.
Consent The individual has given consent to the processing for one or more specific purposes. Consent will be much harder to obtain under this new regulation and should be avoided. Consent from a child (aged under 16) in relation to online services requires authorisation by a parent.	**Explicit consent** The individual has given explicit consent. However, Union or Member State law may limit the circumstances in which consent is available.
Vital interests The processing is necessary in order to protect the vital interests of the individual or of another natural person. This is typically limited to processing needed for medical emergencies.	**Vital interests** The processing is necessary in order to protect the vital interests of the individual or of another natural person. This is typically limited to processing needed for medical emergencies.
Legal Obligation The processing is necessary for compliance with a legal obligation under Union or Member State law will satisfy this condition. However, that law need not be statutory.	**Legal obligation related to employment** The processing is necessary for a legal obligation in the field of employment and social security law for a collective agreement.
Necessary for performance of a contract The processing is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual prior to entering a contract.	See the rest below
Public Functions The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Those functions must arise under Member State or EU law.	
Legitimate Interests The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where	

Article 6 Conditions	Article 9 Sensitive Personal Data Processing Conditions Members States can introduce additional conditions in relation to health, genetic or biometric data.
such interests are overridden by the interests or fundamental right and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.	
	Not for profit bodies The processing is carried out during the legitimate activities of a not-for-profit body and only relates to members or related persons and the personal data is not disclosed outside that body without consent.
	Public information The processing relates to personal data which is manifestly made public by the data subject.
	Legal claims The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
	Substantial public interest The processing is necessary for reasons of substantial public interest, based on Union or Member State law.
	Healthcare Processing is necessary for healthcare purposes and is subject to suitable safeguards.
	Public Health Processing is necessary for healthcare purposes and is subject to suitable safeguards.
	Archive The processing is necessary for archiving, scientific or historical research purposes or statistical purposes and is based on Union or Member State law.

Role of Data Protection Officer

1.1 Which organisations are required to appoint a Data Protection Office (DPO)? (Article 37(1))

Under GDPR it is mandatory for certain organisations to designate a DPO. This will be the case for all public authorities (irrespective of what personal data they process), and for other organisations that - as a core activity - monitor individuals systematically and on a large scale, or that process special categories of personal data on a large scale.

1.2 What does the notion of 'core activities' mean? (Article 37(1)(b) and (c))

'Core activities' can be considered as the key operations necessary to achieve the organisation's goals. However, 'core activities' should not be interpreted as excluding activities where the processing of data forms an inseparable part of the organisation's activity.

1.3 What does the notion of 'large scale' mean? (Article 37(1)(b) and (c))

The GDPR does not define what constitutes large-scale. It is recommended that the following factors be considered when determining whether the processing is carried out on a large scale:

- The number of data subjects concerned - either as a specific number or as a proportion of the relevant population
- The volume of data and/or the range of different data items being processed
- The duration, or permanence, of the data processing activity
- The geographical extent of the processing activity

1.4 What does the notion of 'regular and systematic monitoring' mean? (Article 37(1)(b))

The notion of regular and systematic monitoring of data subjects is not defined in the GDPR. The

'Regular' has been interpreted as meaning one or more of the following:

- Ongoing or occurring at intervals for a particular period
- Recurring or repeated at fixed times
- Constantly or periodically taking place

'systematic' has been interpreted as meaning one or more of the following:

- Occurring according to a system
- Pre-arranged, organised or methodical
- Taking place as part of a general plan for data collection
- Carried out as part of a strategy

1.5 Can organisations appoint a DPO jointly? If so, under what conditions? (Articles 37(2) and (3))

The GDPR provides that a group of undertakings may designate a single DPO if he or she is 'easily accessible from each establishment'. The notion of accessibility refers to the tasks of the DPO as a contact point with respect to data subjects, the ICO and internally within the organisation.

1.6 What are the professional qualities that the DPO should have (Article 37(5))?

The GDPR requires that the DPO 'shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred

to in Article 39'. The necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed. The necessary skills and expertise include:

- expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR.
- understanding of the processing operations carried out;
- understanding of information technologies and data security;
- knowledge of the business sector and the organisation; and
- ability to promote a data protection culture within the organisation.

1.7 What are the resources that should be provided to the DPO to carry out her/his tasks?

Article 38(2) of the GDPR requires the organisation to support its DPO by 'providing resources necessary to carry out [their] tasks and access to personal data and processing operations, and to maintain his or her expert knowledge'. Depending on the nature of the processing operations and the activities and size of the organisation, the following resources should be provided to the DPO:

- Active support of the DPO's function by senior management
- Enough time for DPOs to fulfil their duties
- Adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate
- Official communication of the designation of the DPO to all staff
- Access to other services within the organisation so that DPOs can receive essential support, input or information from those other services
- Continuous training

1.8 What are the safeguards to enable the DPO to perform her/his tasks in an independent manner (Article 38(3))?

Several safeguards exist in order to enable the DPO to act in an independent manner:

- No instructions by the controllers or the processors regarding the exercise of the DPO's tasks;
- No dismissal or penalty by the controller for the performance of the DPO's tasks; and
- No conflict of interest with possible other tasks and duties.

Useful links from the Information Commissioner's Office

- Information Commissioner's Office (ICO) website: https://ico.org.uk/
- Registering as a data controller with the ICO: https://ico.org.uk/for-organisations/register/
- ICO guidance for micro-businesses: https://ico.org.uk/for-organisations/making-data-protection-your-business/
- ICO guidance for small businesses: https://ico.org.uk/for-organisations/business/
- ICO getting ready for GDPR resources: https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/
- ICO GDPR resources: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- Record of processing activities: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

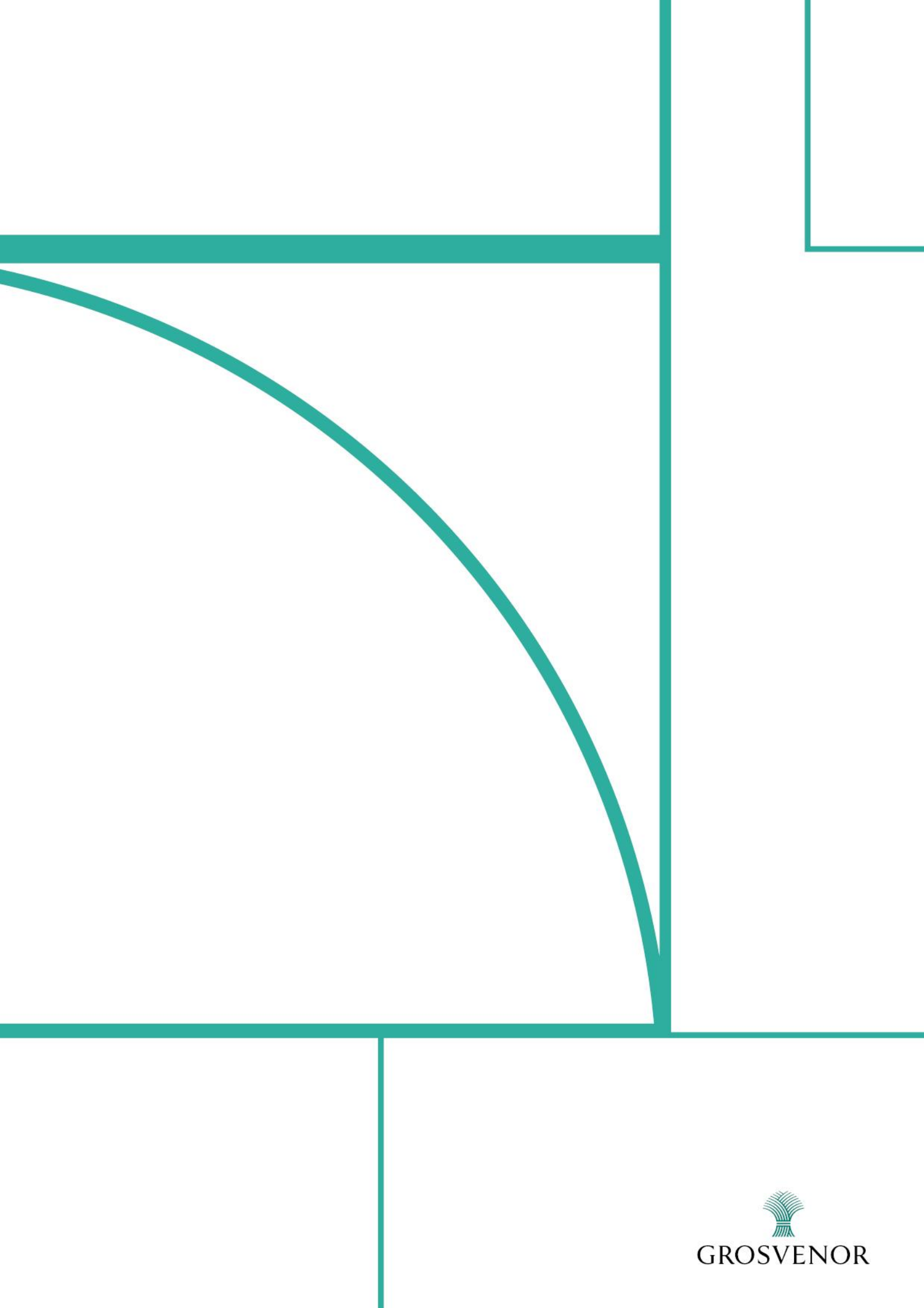
Appendix A

Document control

Author(s) name(s) and job title(s):	Alex Hodge, Information Governance Manager
Version number:	v2-0
Date approved:	N/A
Approved by:	N/A
Date of next review:	N/A

Document history

Version number	Summary of change	Author(s)	Date
v1-0		Alex Hodge	2020-06-15
v2-0	Updated document following change in branding, including adding the confidentiality requirements section	Alex Hodge	2022-02-11



GROSVENOR