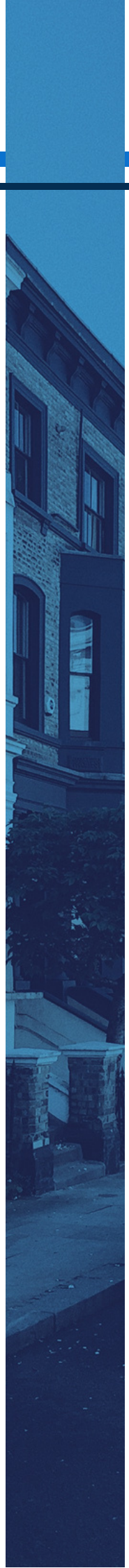
ARTHUR

MANAGING PRIVACY AND DATA PROTECTION SAFELY

FOR LETTING AGENTS

https://www.arthuronline.co.uk

Contents



Contents

Introduction

Since the revamped Data Protection Act (2018), data, privacy and protection became a letting agent's burden to bear.

The General Data Protection Regulation (GDPR) was introduced to prevent data exploitation. Issues such as identity theft and computer hacking are amongst the biggest fears. 4 in 10 businesses reported a cyber-security attack or breach between March 2020 to 21 – and real estate cooperations were among the unlucky.

There are many data risks when storing data. Using spreadsheets or third-party companies that share data globally without consent – which is not GDPR compliant – can result in prosecution. Hence why many letting agents opt for cloud-based software to store, process and protect data.

This eBook covers the ins and outs of GDPR, data privacy and data protection for letting agents. By the end, you'll understand your roles and responsibilities to stay compliant. We'll also share insight into the benefits of cloud-based software so your jobs are free from strife.

Section 1:

What is GDPR and Why is it Important?

What is GDPR and Why is it Important?

When news struck that the Data Protection Act (1998) would change with Brexit, uncertainty befell letting agents. The updated Data Protection Act 2018 outlines the terms for GDPR which applies to anyone that controls and processes data.

- Data Controller: the organisation responsible for the way data is handled and processed.

- Data Processor: the organisation that processes personal data for the data controller (excluding employees).

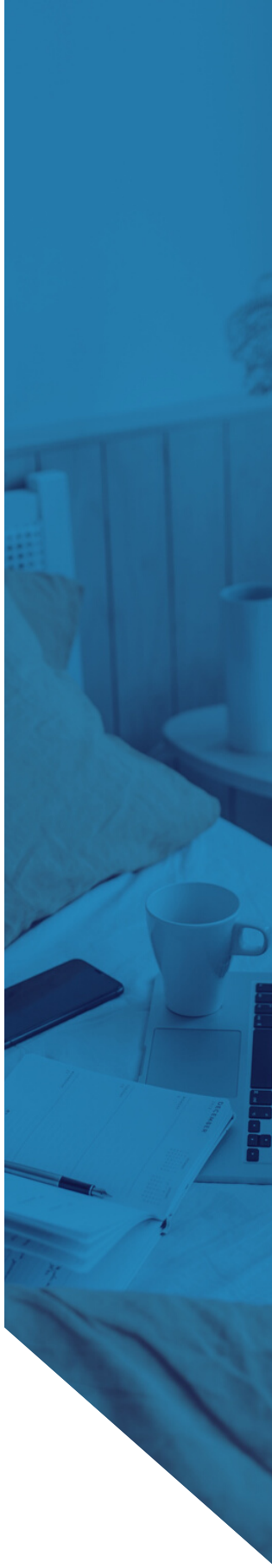
In the majority of cases, letting agents will be both the data controller and the data processor. Unless you outsource processing to a third party, then pay close attention to how they handle data (we'll cover this later). In any case, you are the sole owner of the data.

Types of Personal Data

Letting agents are entrusted with handling personal information. This includes (but is not limited to), an individual's name, phone number, email address, and resident address. This data can come from a tenant booking a viewing online, or securing bank details for rent during a tenancy.

You also work with several private organisations such as contractors and landlords. This requires you to get signed consent from each individual before controlling or processing information.

Personal information even extends to one's online footprint, which includes cookies and IP addresses. Even if someone voluntarily opts in to receiving marketing emails from you via a webform, you must have a personalised Privacy Notice that determines where data will be stored and who it will be shared with.

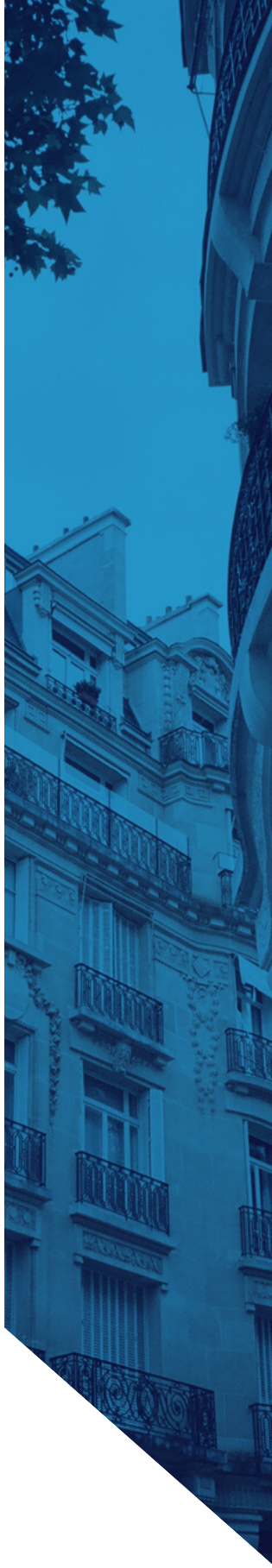


Data Protection Principles

Anyone responsible for gathering or storing data must abide by the protocol. You are trusted to follow these principles to maintain utmost integrity. Information must be:

1. Used fairly, lawfully and transparently: communicate how data will be used and who it will be shared with.
2. Used for specified and explicit purposes: such as storing tenancy information for deposits.
3. Used in a way that is relevant and for what is necessary: for instance, taking simple contact details from prospective tenants for viewings.
4. Accurate and kept updated: all information stored must be updated if/when necessary, such as a tenant's new occupation.
5. Deleted when no longer necessary: deleting prospective tenant information after a few months when they have likely found residence.

Handled securely: protected against "unlawful or unauthorised processing", loss or damage.

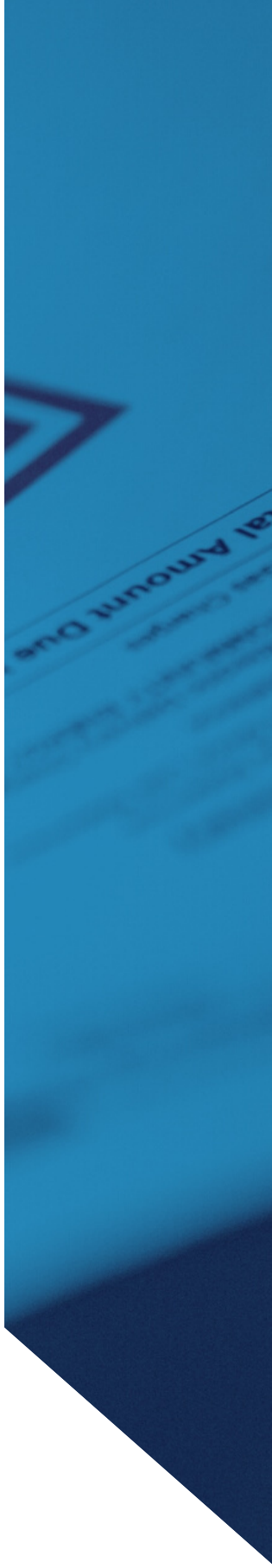


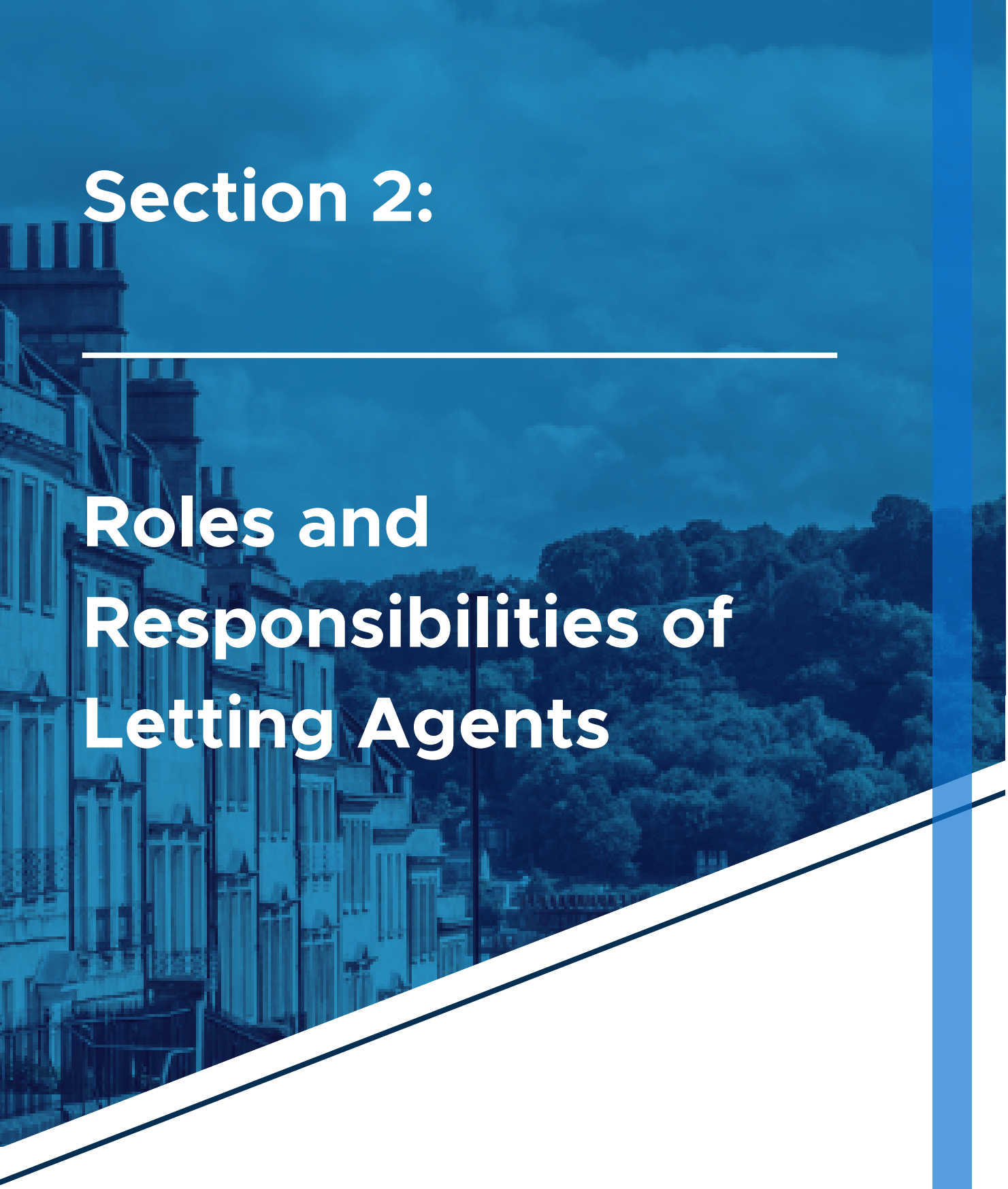
Fines and Penalties

“Unlawful or unauthorised processing” refers to not gaining consent from an individual. Terms must be unambiguous and outline exactly how their data will be used. Failure to do so results in penalties.

Not following GDPR law means you could be subject to fines of up to 20 million euros (4% of the total annual worldwide turnover in the previous financial year).

The minimum penalty includes fines up to 10 million euros (2% of the total annual worldwide turnover). In these cases, an inspection is carried out by data protection authorities when an unsatisfied client or employee complains.





Section 2:

Roles and Responsibilities of Letting Agents

Roles and Responsibilities of Letting Agents

The British Landlord Association (BLA) survey found that 9 in 10 agencies were fully compliant with data regulations.

To maintain compliance and transparency, you must follow and understand your responsibilities as a data controller or processor. This includes privacy notices and registering with the ICO.

Privacy Notice

Recall the rights of individuals: a critical principle of GDPR is the right to inform persons by using a Privacy Notice. This should include:

1. Who you are;
2. What you plan to do with the information i.e. store for tenancy deposits;
3. Where and/or who it will be shared with i.e. HMRC Tax Revenue regarding deposits and rent.

Personalising the Privacy Notice to your agency with appropriate branding and terms of use is important. This notice should be clear on any platform or strategy used to gather data. For instance, when a prospective tenant signs up for marketing emails for new properties; or when a tenant books a property viewing. This should also be logged on your CRM.

Create a Data Protection Policy

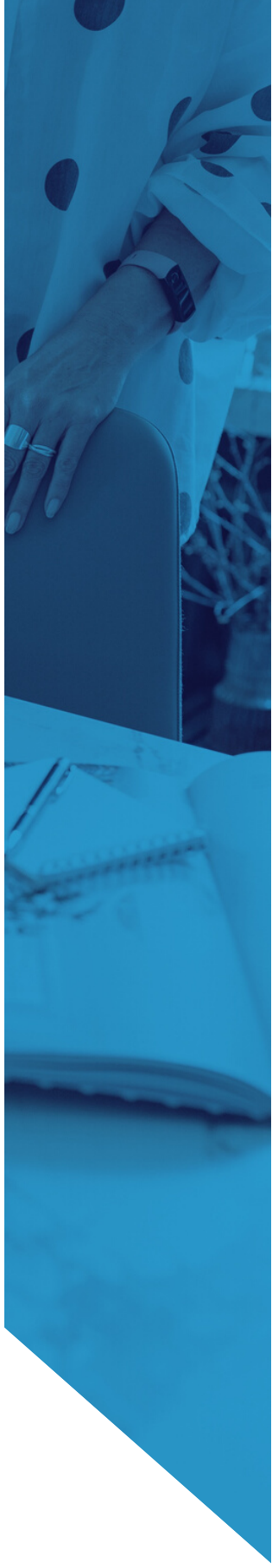
A Data Protection Policy outlines the terms by which your organisation and staff handle data. These guidelines will help you stay compliant as well as encourage team members to understand their responsibilities.

Be direct and transparent on how an individual's data is stored. Follow GDPR good practice to respect and protect individuals who submit and process data.

Register for ICO

All letting agents should register with the ICO (Information Commissioner's Office) if intending to collect and store data on an electronic device.

You will need to pay a fee based on your maximum turnover in the financial year. Generally, you will fall under 'Tier 1' – which includes selling or letting properties with less than 10 members of staff. This fee is approximately £40 per year for any data handling.



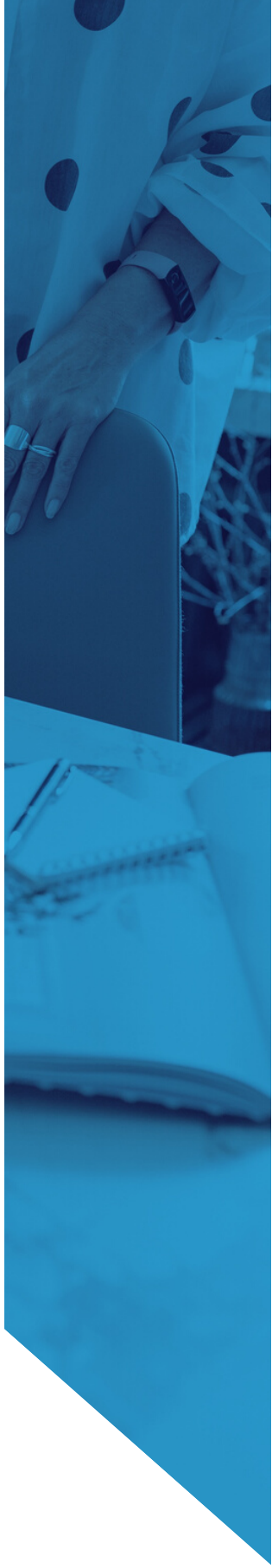
Processing Personal Information

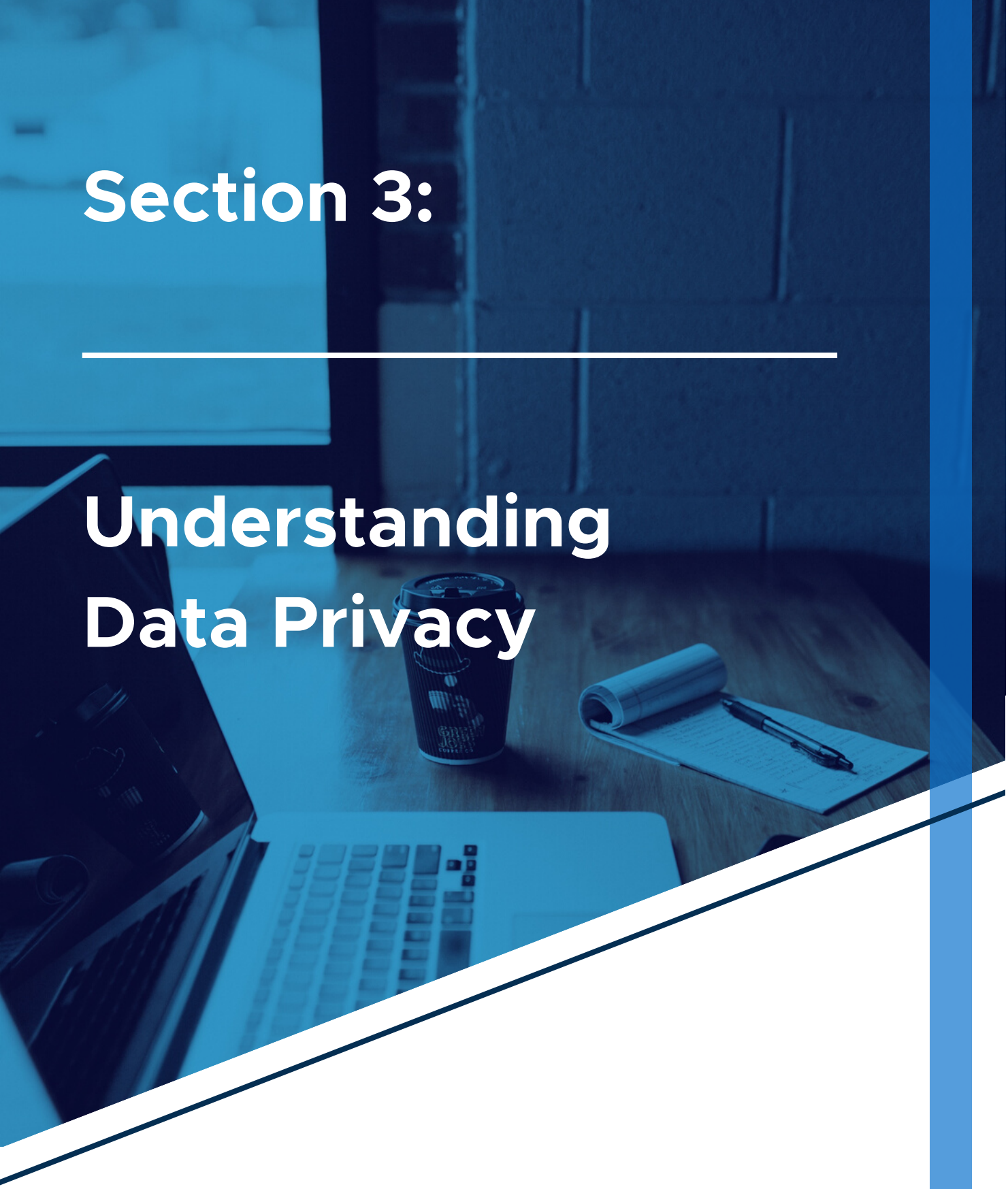
When processing personal data, you should categorise the types of individuals you will deal with. Once you have this list, consider the minimum information you'll need.

For example: existing tenants, contractors and landlords versus prospective tenants and landlords.

For an existing tenant, you'll need contact information (name, phone number, email address), as well as financial information (direct debit or bank details for rent). For a prospective landlord or tenant, basic information like a name and contact number will suffice. Only gather what is necessary to keep in line with data processing.

With regards to ex-tenants, contractors and landlords, all recorded information must be deleted. Conducting a data audit once a year will ensure you're following these guidelines and checking data validity.





Section 3:

Understanding Data Privacy

Understanding Data Privacy

The PRS accounts for 4.5 million homes, representing 19% of housing in England. This means letting agents handle almost one-fifth of personal data. There are several risks involved when processing data; it's your prerogative to manage risks and expectations for data privacy.

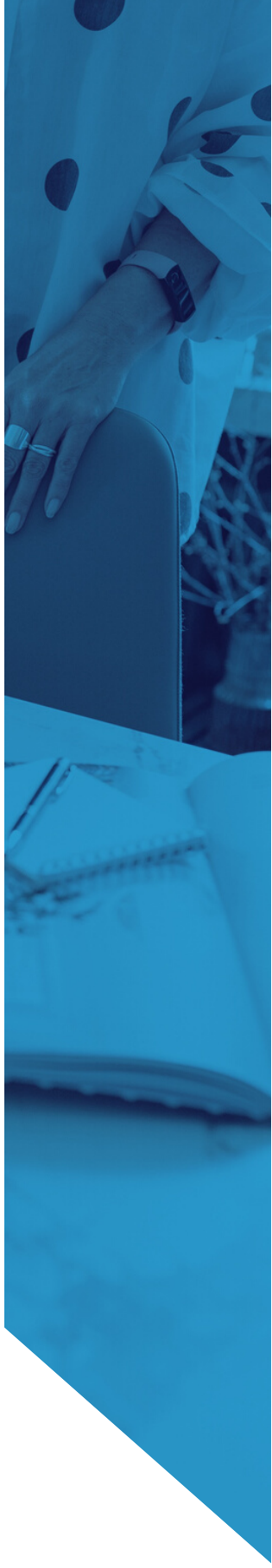
Individual Rights

Article 15 of GDPR outlines an individual's rights. They are authorised to:

- Request access to their data and enquire into how it is being used;
- Request data deletion;
- Transfer data to another provider;
- Be informed about how their data is being gathered and give consent;
- Ensure their data is updated;
- Restrict how data is processed;
- Object against companies using their data for marketing;
- Be informed about any data breach or data loss within 72 hours.

Essentially, you must communicate your data policy honestly and respect an individual's rights. Consent is not a one-off request; a person can ask you to stop using their data or opt-out of marketing, as is outlined in their rights.

At any time, individuals can request access to a copy of their data. You have one month from the date of request to comply. These requests are generally free of charge; although you may charge a fee depending on the amount of data to be gathered, considering also the length of time or effort to process.



Data Risks

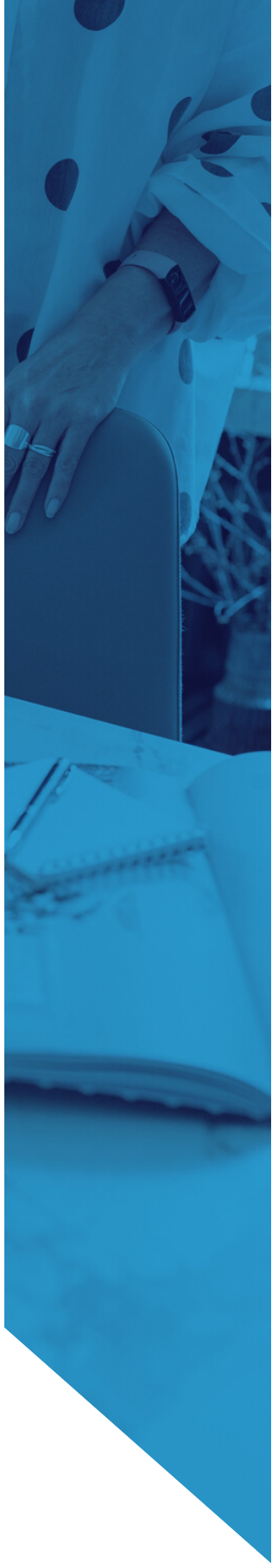
Several challenges come with running a GDPR-compliant agency. Controlling data via spreadsheets or old-school paper filing systems goes against regulations. Moreover, it's much more difficult for you to update information at the request of stakeholders. So how do you store this data and ensure it's protected?

Processing data via Google Sheets or using third-party cloud software comes with an array of risks. For instance, legitimate providers, including Google and Microsoft Office, have multiple drives or servers that hold data. Yet they've experienced the worst cloud server crashes in IT history, which meant the credibility of cloud providers took a hit.

Furthermore, some third-party cloud-based systems have servers based in foreign countries, like the United States. According to the EU GDPR rules, all data must be solely processed within the EU jurisdiction and not transferred globally. This prevents the risk of data falling into the wrong hands.

If in some cases data is transferred outside the EU, necessary safeguards must be put in place and conser provided by individuals. We recommend exporting c file copies regularly for extra security.

Even password-protected computers where yc data risk being hacked. It's important to encrypt y software and all credentials on your database. Hence why investing in a trusted cloud-based server which is GDPR-compliant will minimise these risks, giving you more control and peace of mind.



Data Loss or Breaches

Imagine a situation where your servers crash. Albeit rare, it can happen and leaves you in a pickle. What happens to the data? What if there's a loss? In most cases, this can be resolved quickly as servers will have a backup drive.

A data breach occurs when an employee shares data; or a cybercriminal enters your computer or website and extracts confidential information. Data breaches are commonly caused by:

- Weak passwords: a hacker's dream as it's easy to break into software.
- Malware or spam mail: clicking phishing links that look credible and grant access to cyberhackers. Once entering information (usually financial details) the criminal can use/share data and commit identity fraud.
- Corrupt employees: those who have access to data may share it either for profit or power. Oftentimes, employees may not even be authorised to process data, yet may mishandle it.
- User error: accidents or mistakes, like shari data with the wrong person.

Cyberhackers and employees alike can infiltrate your system and extract data. It's in your best interests to mitigate these risks. Enter cloud-based software; it increases your compliance and quality of service to stakeholders.

Section 4:

Protecting Cloud-Computing Data

Protecting Cloud-Computing Data

Cloud-computing is a revolutionary tool and is considered the modern architecture of IT. You might use Apple cloud data, enabling you to store unlimited photos and download episodes on your device. When you stop paying for this, you lose access to the data. But you can export and print files beforehand. The same goes for cloud-based software.

However, the more complex the system, the more complex the failure. Failure results in data loss and the inability to access accounts, services, projects and critical data for many hours. Take into account that whenever there's bad weather, a cloud failure strikes.

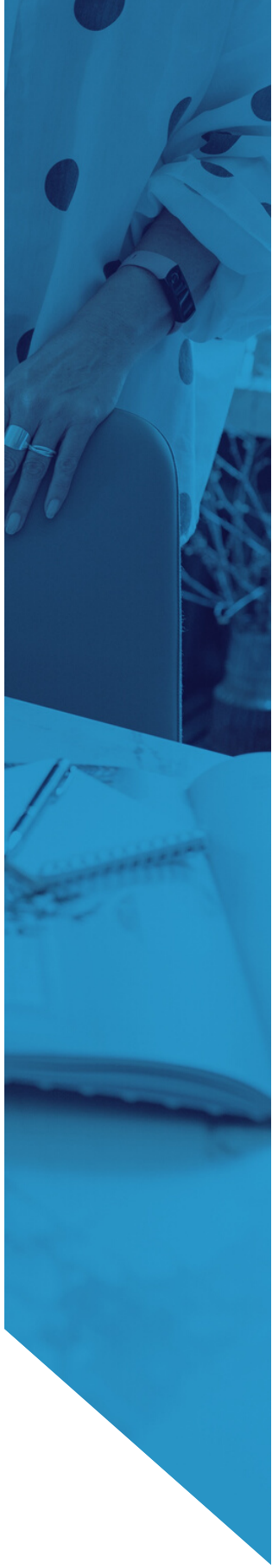
Despite this, trusted tools that provide cloud-based property management software (PMS) help mitigate these risks and optimise your process to stay safe and efficient.

What Does Cloud-Based PMS Do?

PMS enables you to manage properties from anywhere at any time, whilst staying GDPR-compliant. It's an all-in-one system designed to give you full control, integrated with tools like Xero and Signable to streamline data processing and contract agreements. This allows you to manage more properties with less resources in half the time. Some features include:

1. Obtain consent with a Privacy Notice;
2. Upload documents such as certificates and tenancy agreements to properties;
3. Share signable files, such as a welcome pack or contract;
4. Inbuilt CRM to track customer contact information (GDPR compliant).

All of this can be easily stored and tracked via a dashboard that gives you a birdseye view of properties. You can manually add personal information (when lawfully obtained), or delete personal data to limit prolonged storage.



Why Use Cloud-Based Software?

Cloud-based software is a saving grace for letting agents. It can massively improve existing IT measures, taking a weight off your shoulders. So you won't have to worry about hiring executive IT staff or a data protection officer. This means you avoid forking out a pirate's ransom to keep data safe.

Note that Arthur's cloud-based system is fully encrypted and stores information in trustworthy and responsible locations, within the EEA (European Economic Area). We undergo the necessary steps to ensure your data is kept secure as we do our own. Our infrastructure is highly secure and robust, and we have a dedicated support team to walk you through data handling.

When choosing cloud software, opt for Service Level Agreements (SLAs) operating at 99.99% availability, which means an average yearly downtime of 53 minutes. If servers crash, there's a redundancy in cloud storage. Simply put, when one server fails, another pops up in its place to preserve and back-date data. Downtime is inevitable; in our case it's minimal. Regardless, ensure that any SAAS solution addresses its uptime openly.

Conclusion

Now you should be a GDPR pro and understand legal requirements when handling data. Using a nifty tool like Arthur, you can standardise processes and improve data safety in-house, meaning you can concentrate on scaling your portfolio and managing stakeholder expectations efficiently.

Book a demo to see how faff-free software could work for your agency, to manage data safely and effectively.

ARTHUR

Email:

https://www.arthuronline.co.uk/

Phone:

+44(0)207 112 4860

Website:

sales@arthuronline.co.uk