urban.co.uk

GDPR: The Great Data Puzzle Revealed

What do the changes mean for landlords?

How has data handling changed?

General Data Protection Regulation (GDPR) – the biggest change to data handling that UK organisations have seen since the introduction of the current Data Protection Act - was introduced on May 25th, and impacts all of us.

Although a EU regulation, the rules will not change when the UK exits Europe – the regulations are **'Brexit-Proof'**

Many of the principles of GDPR are the same of the DPA. The regulation's principles aim to ensure that an individual has:

- **The right to be informed:** Allowing individuals to know that their data is being stored
- **The right of access:** Allowing individuals to access their data is so that verify the lawfulness of the processing
- **The right to rectification:** Allowing individuals to change/amend their data if it is incorrect/incomplete
- **The right to erasure:** 'The right to be forgotten' Total wipe out of their data from your systems
- **The right to restrict processing:** Allowing individuals to put a block on their data being used at all
- **The right to data portability:** To obtain and reuse their own data for their own purposes across different services
- **The right to object:** Can say no to their data being used for marketing or processing
- **The right not to be subject to automated decision-making including profiling:** Can say no to their data being subject to analysis without 'human intervention'

What if I don't comply?

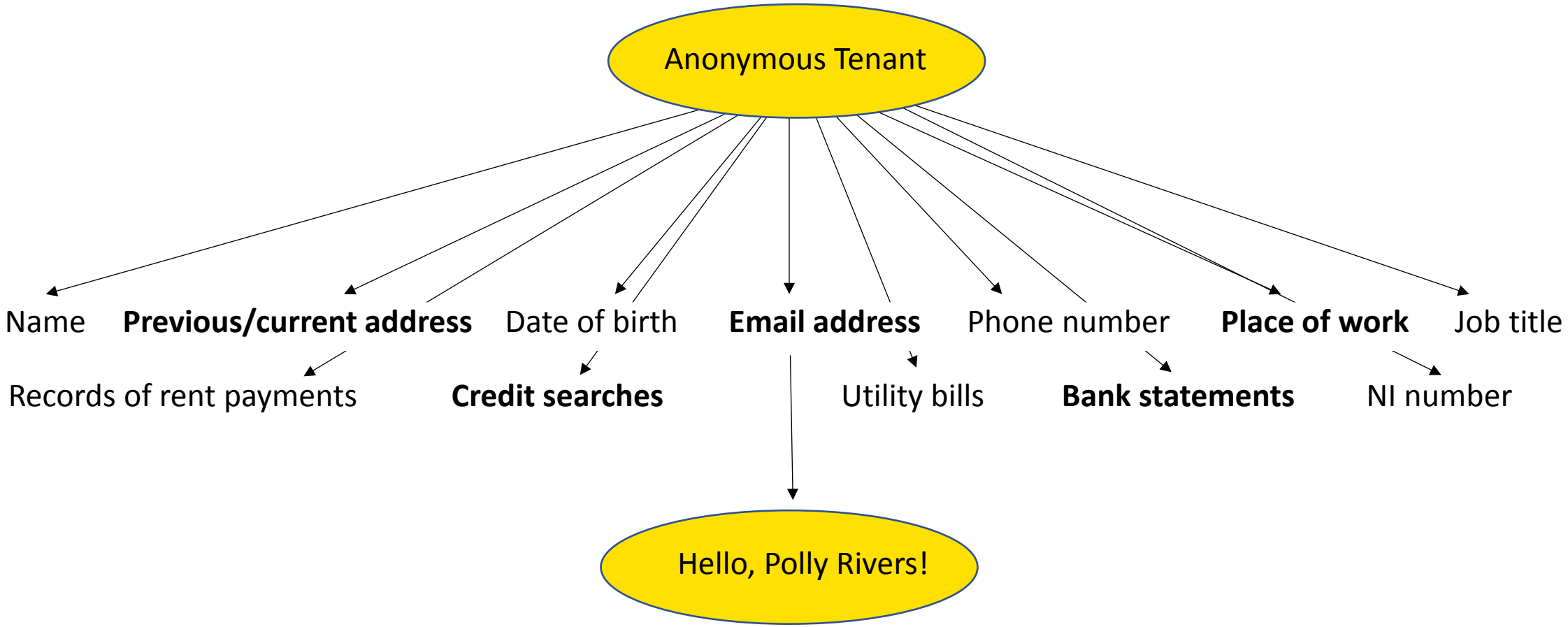
The GDPR has introduced larger penalties for data breaches than were in place for breaching the Data Protection Act (£500,000 maximum), with fines of up to **4% of annual worldwide turnover or €20 million** being possible.

Whilst it is unlikely that an individual landlord would ever be handed a €20 million fine (the largest ever fine levied under the DPA was £400,000), penalties will be handed out by the Information Commissioners Office (ICO) who the have a DUTY to impose a penalty – this is not being taken lightly.

If your tenant is subject to a data breach and it is considered that your mishandling of their data has played a part, they are also able to pursue you for damages. Depending on the impact the breach has had on them, these costs could be significant.

What exactly qualifies as data?

Anything that could identify your tenant.



How has it changed things for me?

A **data controller** is an individual (or an organisation) who decides how personal data is processed.

Data protection obligations primarily fall upon the **data controller** – it's your job to keep your tenant's data safe. Initially, as a **data controller,** you decide:

- **To collect the personal data in the first place**
- **The legal basis for data collection**
- **Which items of personal data to collect (what you need to know!)**
- **What you're planning on using the personal data for**
- **Whose data you need**
- **Whether to pass the data onto a Processor, which Processor, and whether they have an data handling process**
- **How long you will keep the data** – this could change depending on whether you have a formal legal contract in place with the individual or not. Keeping data for 6 years is acceptable after the end of a formal legal contract (such as a tenancy agreement), but if there is no formal contract in place, it should be deleted immediately.
- **Whether to make any amendments to the data**

How has it changed things for me?

As a data controller, you also have to keep an eye on any **Data Processors** that you engage with.

A **Data Processor** is any of the organisations you ask to handle data on your behalf– your referencing agency or your agent, for example. Under GDPR they have responsibilities for:

- **Appropriate collection of data**
- **Appropriate editing of data**
- **Retaining/storing in line with GDPR guidelines**
- **Disclosing (or sharing) data in line with GDPR guidelines (how secure: password protected, cloud systems etc)**
- **The correct deletion/erasing/destroying of data**
- **The proper viewing (e.g. looking at someone's personal data, which could include their image, on screen or on paper) of data in line with GDPR guidelines**
- **Appropriate archiving of data**

As a **Data Controller** it is your responsibility to ensure that any **Data Processor** that you engage with is managing your tenant's data correctly, and complying with the guidelines.

Legal bases for processing

One of the most important elements of GDPR is understanding the legal bases for processing.

There are six legal bases for processing. As a landlord, the process you follow to let your property will touch upon some of these more than others. It is important to identify the ones you will be reliant upon, clearly making note of them in your privacy policy, and ensuring than your tenant is aware of them.

It is very bad practice to switch from one legal basis to another part way through processing, so it is important to identify the correct basis at the start of proceedings.

You should decide the best bases for your business – every process is different and therefore your plan may be different to the landlord sat next to you!

Six methods for processing

Consent

Consent to collect and process an individual's data must be properly documented, and easily withdrawn: either provided by a statement or by a clear affirmative action (such as a clear Yes/No tick box). **Silence or inactivity DOESN'T MEAN CONSENT.**

You can gain consent a number of ways:

- **Signing a consent statement on a paper form**
- **Ticking an opt-in box on paper or electronically**
- **Clicking an opt-in button or link online**
- **Selecting from equally prominent yes/no options**
- **Responding to an email requesting consent (Building a paper trail via email is a great idea wherever possible!)**
- **Answering yes to a clear oral consent request**
- **Dropping a business card into a box**

Consent cannot be considered a 'safe option'. Remember that it can be withdrawn, and therefore may not be the most appropriate basis for processing.

Six methods for processing

If you are relying on consent and are asking your tenants to sign a consent form, or sending them and email requesting a positive response, you must make sure include clear details on the followings:

- **Your name/the name of your organisation and the names of any third parties who will rely on the consent – consent for categories of third-party organisations (referencing/maintenance etc) isn't enough**
- **Why you want their data**
- **What you will do with their data**
- **How they can withdraw their consent for it to be processed (passed on)**

Six methods for processing

Contract

The ICO website states that this basis can be relied upon to process someone's personal data to **fulfil your contractual obligations** to them or because they have asked you to do something before entering into a contract.

The processing must be necessary to deliver your side of the contract with this particular person. If you could carry out proceedings without processing their personal data, this basis will not apply. If the processing is only necessary to maintain your business model generally, this lawful basis will not apply.

Legal obligation

The ICO website states that this basis can be relied upon if you are reliant on processing the data in order to comply with **common law or statutory obligation**. However, this does not apply to contractual obligations.

The processing must be necessary. If you can reasonably comply without processing the personal data, this basis does not apply. You should document your decision to rely on this lawful basis, and be able to either identify the specific legal provision or an appropriate source of advice or guidance that clearly sets out your obligation, and ensure that you can justify your reasoning.

Six methods for processing

Legitimate Interest

The ICO website states that this is the most flexible basis for processing, but not always the most appropriate. If you choose to rely on legitimate interest, you are taking on **extra responsibility** for considering and protecting people's rights and interests.

Legitimate interest is likely to be most appropriate where you use people's data in ways they would reasonably expect, and which have a minimal privacy impact, or where there is a compelling justification for the processing.

There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to:

- identify a legitimate interest;
- show that the processing is necessary to achieve it; and
- balance it against the individual's interests, rights and freedoms.

You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.

Keep a record of your **legitimate interests assessment (LIA)** to help you demonstrate compliance if required and make sure to include details of your legitimate interests in your privacy notice.

Six methods for processing

Vital interests

The ICO website states that this basis can be relied upon to if you need to process the personal data to **protect someone's life**, and you must be able to justify your reasons for this choice

Public Task

The ICO website states that this basis can be relied upon to if you need to process personal data:

- 'in the exercise of official authority'. This covers public functions and powers that are set out in law; or
- to perform a specific task in the public interest that is set out in law.

Your underlying task, function or power must have a clear basis in law, and if you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply. It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest. **This is unlikely to apply to may individual landlords**.

Information you already hold

Auditing the data that you already hold is a great idea. An information audit will help you get your files prepared, an give you an overview. You should understand:

- **What personal data do you hold?**
- **Where did it come from?**
- **Who have you shared it with?**
- **Is it all still accurate?**
- **How you would delete that data if required?**

If you do not have consent to use your existing tenant's data, you should gain their consent in line with the consent process. You should serve your existing (and new) tenants with a **Privacy Notice**, which will give them details about how their data is used, stored and deleted, and how to contact you with regards to opting out of processing.

Privacy notices

A Privacy Notice only needs to be a simple document, laying out clear, easily understandable facts surrounding your data management process. You should include:

- **Type of data that is being collected** – name, date of birth etc
- **Who is collecting it**
- **Legal basis for collecting data**
- **Who has access to it** – You, any third party data processors (refer to their Privacy Policy)
- **What will be the effect of sharing to these organisations have this on the individuals concerned?**
- **How is it collected** – email/digital form/in person etc
- **Why is it being collected** – are there different types of potential processing?
- **How will it be used** – what are you planning to do with it?
- **How it WON'T be used** – what will you NOT do with it
- **How data will be stored/protected** – Cloud storage, how long will you store it etc
- **How you would manage a data breach**
- **The potential consequences of choosing to not provide data** (not being able to issue a tenancy agreement, for example)
- **Provide a clear way to contact you to stop processing of their data completely, or stop aspects of processing**

It's useful to issue a privacy notice separately to your tenancy agreement (rather than including it), if you have to make any changes, you can reissue without having to change the entire agreement.

Data breaches

One of the requirements of GDPR is to make sure you have the correct procedures in place to detect, report and investigate a personal data breach.

You must notify the 'relevant supervisory authority' of any data breach that could result in a risk of rights and freedom of individuals, including discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. In addition, you would also have to notify the person who's data had been breached.

Anyone handling data is required to be registered with the Information Commissioner's Office (ICO), and one of the benefits of registration is that the ICO offer support and advice.

An annual registration of the ICO is £40 - https://ico.org.uk/for-organisations/register/

THIS IS REALLY IMPORTANT!

Getting ready checklist

- **Create a privacy policy (and consent form if required)**
- **Review your process on how you ask for customer data**
- **Create a process for the secure storage, and deletion of data**
- **Audit the data you already hold** – make sure everything is current, correct and consenting!
- **Contact Data Processors that you regularly transact with** (agents, property managers, referencing agencies, maintenance companies etc), gather their full contact details and ask about their GDPR data management policy
- **Register with the ICO!** This is really important!

urban.co.uk

Any questions?

e: p.rivers@urban.co.uk
t: 0800 689 9955
w: www.urban.co.uk

(I am consenting to you having my data!)