# Data protection for RTM and RMC companies

*How to handle residents' personal information lawfully, from the ICO fee and subject access requests to CCTV, breaches and retention.*

A resident-run company holds personal information about leaseholders and others: names, addresses, contact details, payment history, correspondence and sometimes more sensitive matters. The UK GDPR and the Data Protection Act 2018 apply to it, even though it is small and run by volunteers.

## The basics

- **Know what you hold.** List the personal data you keep, where it lives and who has access.
- **Have a lawful reason.** For most building administration, the reason will be performing the leases and the company's legitimate interests. Occasionally you will need consent.
- **Tell people.** A short privacy notice should explain what you collect, why, who sees it, how long you keep it and their rights. Our privacy notice template is a starting point.
- **Collect only what you need.** Do not keep personal details just in case.
- **Keep it accurate and up to date.**

## Do we need to pay the ICO data protection fee?

Many small resident companies are exempt, but the exemptions are narrow. In particular, using CCTV for crime prevention generally means the fee is payable.

The Information Commissioner's Office has a short fee self-assessment. It takes a few minutes, so do it once and keep a note of the answer. Fees change, so we do not quote them here: check the current amount with the ICO.

## Keeping it secure

- Use strong passwords, and keep systems up to date.
- Limit access to the directors and advisers who need it.
- Do not circulate the whole resident list by email. Use blind copy or a communication tool.
- Keep paper records locked away.
- Make sure contractors and the agent treat the data properly, and have a written agreement with any that process it for you.

## If something goes wrong

A personal data breach that risks people's rights must be reported to the ICO within 72 hours of becoming aware of it. Whether a breach is reportable depends on the facts, so decide quickly and write down your reasoning either way. Three examples:

- **The resident list is emailed with open CCs.** Every recipient can see everyone else's details. This may be reportable if the list showed more than names and email addresses, such as phone numbers or arrears. If it showed only names and email addresses, it may be low risk, but it depends on the facts.

- **A director's laptop is stolen.** Likely to be reportable if it held resident records and was not encrypted or protected by a strong password. If it was encrypted and locked, the risk may be low.
- **A contractor is given the wrong key list.** It depends on what the list showed. Names, flat numbers and access codes could put residents at risk, which points towards reporting and telling them. A list of key numbers alone may not.

In each case, tell the affected residents what happened if they could be harmed, and take advice quickly. Do not wait until you are sure. The 72 hours run from when you become aware of the breach, not from when you finish investigating it.

Keep a record of every breach, including the ones you decide not to report: what happened, what was involved, who might be affected, what you decided and why. If the ICO asks later, that note is your answer. The fastest way to find out is to ask the director who sent the email or lost the laptop, so make it easy to own up.

## Residents' rights

People may ask what you hold, ask for corrections, object to certain uses and, in some cases, ask for deletion. A request for a copy of their own data is called a subject access request.

- A subject access request must be answered within one month.
- This can be extended by up to two further months for complex or numerous requests, and you must tell the requester within the first month.
- You can't normally charge a fee.

Agree in advance who handles these requests and where they are logged. When one arrives, note the date it was received, which starts the clock, and check that the person asking is who they say they are. Gather what you hold, take out other people's personal data, and send the reply securely. Keep a copy of what you sent.

## How long to keep it

Keep records for as long as they are needed, and for the periods the law sets for company and financial records. Agree a retention schedule and review it each year, so that old data is deleted.

| RECORD | KEEP FOR | WHY |
|---|---|---|
| **Company accounting records** | At least 3 years (private company, CA 2006 s388); 6 years in practice for HMRC | Companies Act and tax |
| **Service charge accounts, invoices and receipts** | 6 years after the year end | Leaseholder challenges and limitation |
| **Register of members** | Current entries indefinitely; former members 10 years after they cease (CA 2006 s121) | Companies Act |
| **Minutes of meetings** | At least 10 years (CA 2006 s248, s355) | Companies Act |
| **CCTV footage** | Around 30 days unless needed for an incident | Proportionality |

Review the schedule every year. Shred paper records when their time is up, and delete digital copies from laptops, email and shared drives as well as the main system. A record that nobody remembers is the one most likely to be lost.

## Managing agents and contractors

If a managing agent, accountant or contractor handles residents' details for you, have a written agreement that says what they may do with them. When an agent leaves, ask for the data to be handed over and the copies deleted. Our guide to taking over from your agent covers what to ask for.

## CCTV and door entry

Cameras and entry systems capture images and movements. You need a clear purpose, signs, controls on who can view the footage and a limit on how long it is kept. Think carefully before installing cameras that cover people's homes. If the cameras are for crime prevention, the ICO fee above will usually be payable.

## Company registers

The register of members and directors' details are held for legal reasons, and some of it is available to the public or to members. Be clear what can be disclosed and to whom. Our guide to company secretarial duties covers the registers, and the guide to leaseholders' rights to information covers who may inspect them.

## Template download

A one-page privacy notice for a resident company, with placeholders in square brackets for you to fill in.

**Download the privacy notice template (Word)**

> Keep it proportionate. Good housekeeping, a short notice and sensible security meet most of what is needed. If something goes wrong, tell the right people quickly and take advice.

## Frequently asked questions

### Does a residents' management company need to register with the ICO?

Many small resident companies are exempt from the data protection fee, but the exemptions are narrow. In particular, using CCTV for crime prevention generally means the fee is payable. Use the ICO's fee self-assessment to check your own position, and keep a note of the result.

### Can directors share leaseholders' contact details with each other?

Directors who need residents' details to run the building can normally have them, because that is why the details were collected. They should not be shared more widely or used for other purposes. Do not circulate the whole list by email, and say in your privacy notice who sees the data.

### Can we install CCTV in communal areas?

Possibly, if you have a clear purpose such as crime prevention. You need signs, limits on who can view the footage and a short retention period, around 30 days unless needed for an incident. Cameras that cover people's doors or windows are hard to justify, and the ICO fee will usually be payable.

### Who is the data controller: the RTM company or the managing agent?

The company is normally the controller of the resident data it holds, because it decides why and how the data is used. A managing agent usually acts on the company's behalf as a processor,

and the arrangement should be in a written agreement. If an agent also uses the data for its own purposes, it may be a controller too, so ask.

---

General information, not advice on your circumstances. Leasehold law is detailed and changes: check the current position and take advice before acting. Leasehold Clarity is provided by Leasehold Clarity Limited (company no. 16963931), with management and professional services from Murphy Thompson Moore LLP (LLP No. OC314041).