SMARTSPACE
SOFTWARE

The GDPR and visitor management:

What the law requires, and how to ensure your compliance

A guide for business space managers

A SmartSpace smart building guide

Contents

Part 1

An overview of the GDPR and visitor management – why you need to read and share this guide

The moment your visitors step foot inside your offices or building, their safety, security and privacy become your responsibility.

This guide focuses on one fundamental aspect of those responsibilities: specifically, the legal responsibilities of organisations with offices in the UK and the EU in relation to data privacy and the General Data Privacy Regulations (GDPR).

How the GDPR affects your visitor management

Enacted in the UK in 2018, the GDPR enforces a whole new level of rigour on any business that collects, stores and in any way utilises data relating to an individual.

Why this matters to your front desk

There remains a general misconception that the GDPR only applies to data collected online.

The fact is the GDPR applies to ALL personal data, including visitors' information collected from offices and other workplaces.

Eye-opener #1

If your organisation uses a paper visitors' book method to track visitors coming in and out of the building, chances are you will not be meeting the data privacy standards of the GDPR.

In fact, you could be violating laws and regulations that come with hefty fines and penalties for non-compliance.

The truth is...

...whatever form of visitor management systems or processes you have (or are planning to put in place), you need to be aware of the implications of the GDPR. These implications affect how you collect, store and use your visitor data – from the point they check in to a parking space in your carpark or sign in at your front desk or reception.

The penalties for non-compliance

The GDPR empowers supervisory authorities to assess fines that are “effective, proportionate and dissuasive.” In the UK, the supervisory authority is the Information Commissioners Office.

There are two tiers of maximum fines, depending on whether the data controller or processor committed any previous violations and the nature of violation. The higher fine threshold is 4% of an undertaking’s worldwide annual turnover or 20 million euros, whichever is higher.

The lower fine threshold fine is 2% of an undertaking’s worldwide annual turnover or 10 million euros, whichever is higher.

It’s important to remember these are maximum fines. The ICO is empowered to consider a range of mitigating factors in the case of an upheld GDPR violation. The surest mitigating tactic of them all is to ensure compliance.

In the next section of this guide, we explain what you need to know to take steps to achieve that compliance.

(A quick disclaimer before we proceed. This guide is intended to provide practical insight and guidance into GDPR compliance, and not a substitute for professional legal advice.)

Part 2

A closer look at the GDPR and how your visitor management could be violating the law

The GDPR is platform-agnostic. This means if you're collecting personal information, you're under the regulation of the GDPR, regardless of how you are capturing it.

Whether you're using a paper or digital visitors' book, you are collecting personal data. Therefore, your processes and system need to enable full GDPR compliance.

The first step is to understand the provisions under the GDPR and how they affect your visitor management process.

Here we will cover the six key provisions that affect how you collect and manage your visitor data.

Provision 1.

Clear Consent

According to the GDPR, when collecting data, "consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication."

So what does that actually mean in the context of your visitor management?

Consent and legitimate business interest

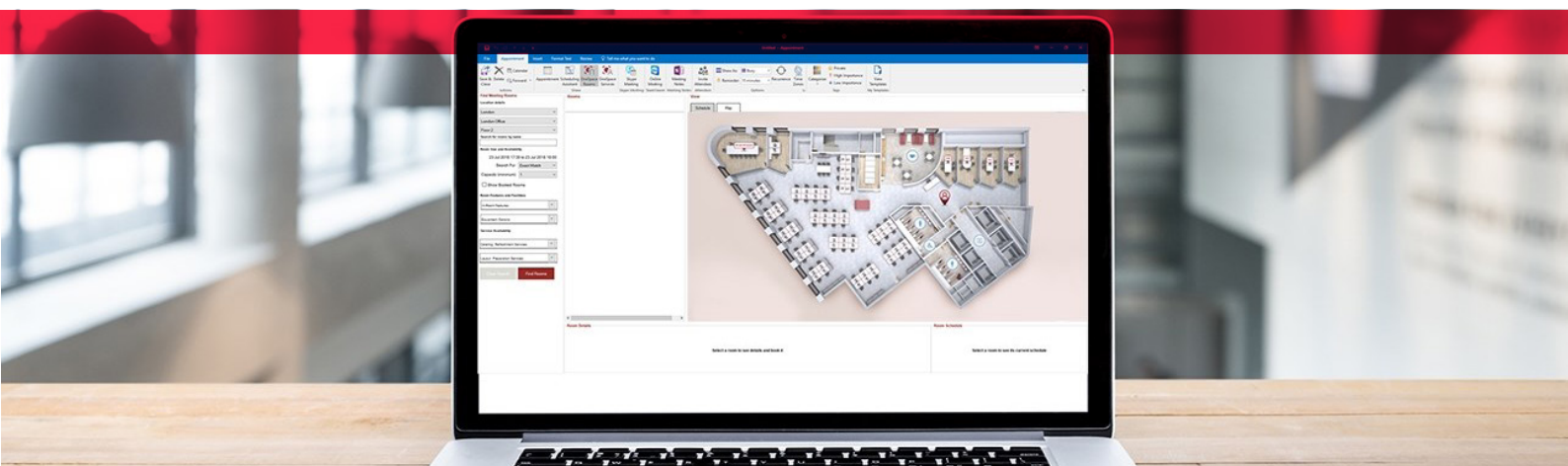
There's a common misconception around GDPR that specific consent to collect and use an individual's personal data is always required.

In fact, the law states that you don't need to gain specific consent when personal data is collected for the legitimate interest of the data controller (as long as that interest doesn't inflict unjustified adverse effects on the individuals concerned).

See Provision 2 for more insight.

Tip. A digital visitor management system gives you legitimate interest justifications for personal data collection, namely your management of:

- Physical security procedures
- Data security procedures
- Health and safety procedures



Provision 2.
Clarity and transparency

The GDPR requires businesses to provide clarity and transparency around how and why personal data is being collected and will be used.

For businesses collecting customer names and email addresses online, for example, it's straightforward to provide that transparency through a website link to an up-to-date privacy policy.

But how do you provide that clarity of intention when collecting data for visitor management?

Tip. Using the 'agreement' feature of a digital visitor management system (VMS) enables you to provide your office visitors with both clarity and transparency around the use of their data.

A VMS empowers you to provide clear details as to why you are collecting a visitor's personal data, your legitimate business interest for doing so, and how the data will be stored and used.

Then you can, if you choose, easily ask the visitor to confirm their understanding by digitally signing the agreement.

Best practice

A visitor management system enables you to additionally capture your visitors' agreement to your health, safety and security requirements.

Without this, you would not be able to waive liability in case an unexpected incident occurs due to visitor negligence.

Provision 3.
Limited data collection

The GDPR stipulates: "Personal data collected must be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed."

How does this affect your visitor management?

The fact is you will almost certainly have different categories of visitor to your building, (e.g. contractor, applicant, business visitor, family).

In some of these cases, you may need to collect more data than in others, e.g. to manage 'sensitive' area access.

If you're using a paper visitor book process, then unless you use a different book for each visitor category, the chances are you are collecting the same information across the board – potentially violating this provision within the GDPR.

Tip. A visitor management system enables you to fully customise both your data collection requirements and your data agreement, based on the category of visitor whose data you are collecting.

Provision 4.
Storage limitation

The storage limitation principle of the GDPR states: “Personal data shall be 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.”

In the case of visitor management, it’s arguable that storage life of visitor data should be relatively short.

Tip. For organisations using a paper visitors’ book, the common practice is to use the book until it runs out of pages. This could take a week, a month, or even a year, depending on the number of pages and the number of visitors to your office.

If you’re following this practice you could be storing your visitors’ personal information longer than necessary.

A VMS can enable you to define data storage lifespan and automatically clear down all visitor data after a set time, ensuring GDPR storage limitation compliance.

Provision 5.
The right to be forgotten

According to the GDPR: “The data subject shall have the right to withdraw his or her consent at any time.”

It further states: “The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay…”

Tip. Digital data storage makes the ‘right to be forgotten’ logistically manageable. (It’s almost logistically impossible to comply with this GDPR requirement with a paper visitors’ book.)

Provision 6.
Security and data recoverability

According to the GDPR: “Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.”

Tip. Any storage of your visitors’ personal data should be encrypted, password protected and backed-up.

The latter is important because data protection regulations require “the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.”

(It’s unlikely any organisation would be able to comply with this requirement following the loss of a paper visitors’ book, as creating multiple copies isn’t a practical option.)

Part 3

How an advanced Visitor Management System (VMS) supports compliance with the GDPR and other UK privacy laws

1. An advanced VMS allows you to add a paragraph in your visitor agreement that clearly informs your visitors on how you are intending to use their personal data, and enabling them to signify their understanding of these intentions.

2. Using the 'agreement' feature of an advanced VMS, you can lay out the legitimate business interest grounds for why you are collecting your visitors' personal data.

3. With a VMS, your visitors' personal data is handled electronically, in a similar way to how information collected online is processed and managed. This makes the entire process private and secure.

4. An advanced VMS has fully customisable privacy settings to ensure that no personal information is compromised. For example, you can switch off the "auto-suggest feature" so the name of a visitor who has recently logged in doesn't appear as new visitors sign in.

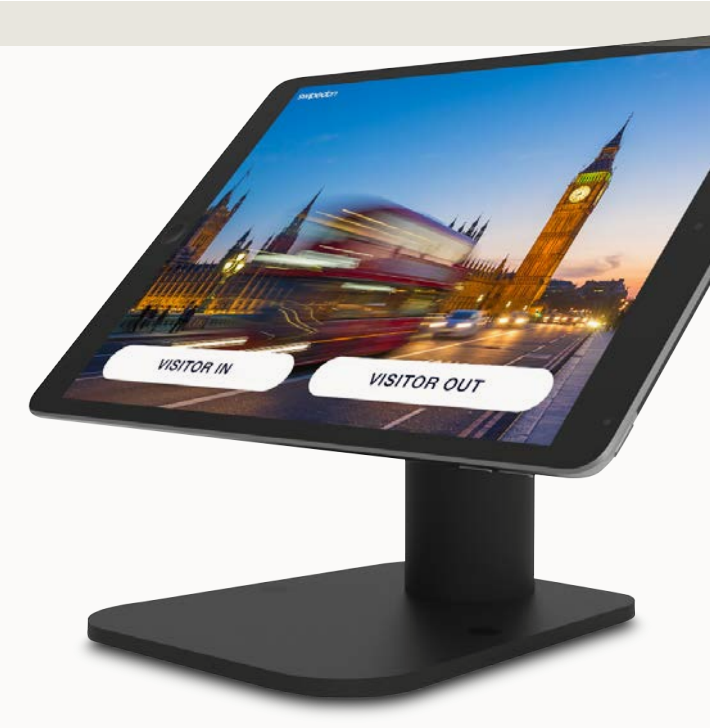
5. Electronic handling of personal data through a VMS enables you to comply with all the articles under the GDPR specified above in this guide, including data recoverability and limited storage.

6. With a VMS, compliance with the 'right to be forgotten' principle is simple and transparent, enabling you to permanently anonymise personally identifiable information, giving your visitors and employees utmost data privacy and protection.

7. Under the GDPR, your visitors and employees should be able to request a copy of the personal information you have about them. A digital VMS has an export functionality that will allow you to do this.

8. Not being able to comply with the GDPR can expose your organisation to complaints, negative publicity, and brand damage, and cost your organisation financially through legal procedures and even fines.

9. Implementing an advanced, digital VMS is the best way to ensure compliance right at your front desk.



How SmartSpace Software can help with your business space management

SmartSpace is the world's leading, fully flexible workspace management platform.

Our modular solution is unique in its ability to fit your needs, engage your employees, scale with your business and integrate with your existing tools.

A single powerful platform and our uniquely user-friendly mobile app integrate a range of smart-building modules including:

- Visitor management
- Meeting room management
- Desk management
- Wayfinding
- Analytics
- Smart car parking
- Employee engagement

Just some of our happy customers include:

UBM

UBS

MITSUBISHI MOTORS

Mobil

BOSS HUGO BOSS

gsk

EVOKO

ESTĒE LAUDER

Find out more at smartspaceplc.com

Or call us on +44 (0)845 0945 686

Or email us at sales@smartspaceplc.com