15 Things Commercial Agents Need to Know About GDPR

As of the **25th of May 2018**, all companies will have to conform to the **General Data Protection Regulations (GDPR)** when operating within the E.U. You can ignore Brexit on this one (as in GDPR will go ahead whether we are in or out of the E.U.) If you are in the U.K. you need to comply. If you don't conform you can receive a big fine.

The issue is particularly relevant to commercial agents because you can be fined (up to 4% of turnover) if you send a marketing email to someone who has not 'opted in'. You need to be able to prove that they have consented to being sent marketing information.

0800 142 5604 **srb@caldes.com**

Here are the key things that you need to know:

1. **Does GDPR affect B2B?** When sending out marketing material, employees will not be able to quickly differentiate between what is and what is not allowed, who can and who can't be sent information, which and what marketing material they can send. So, to avoid costly mistakes you need a system, such as Caldes HUB, that manages this automatically.

2. **Everyone is affected.** Whether your company is big or small, everyone from Directors through to part-time employees need to know about GDPR and they need to be aware of your internal data security policies.

3. **Personal data.** Corporate email addresses and other contact details are personal data. Personal data is anything that identifies or belongs to an individual. e.g. jo.bloggs@caldes.com would identify an individual at Caldes and therefore would be classified as personal data. So, if someone gives you their business card, although it is business information it does identify them as an individual and therefore can be classed as personal data. Personal data includes cookies and IP addresses.

   Information about Sole traders and partners should be treated as personal data.

   Personal business data is treated as personal data, but you can market relevant services as long as you provide an opt-out. You should therefore gain opt-in consent in those relevant areas to avoid any confusion.

   Generic business email addresses (e.g. info@caldes.com) are not personal data and do not require an opt in but must have an opt out.

4. **Opt in only?** This is the big one for estate agents, commercial agents and surveyors. You need to have ***unambiguous consent*** to process their information, such as to ***email them property marketing details*****.** You need to be able to show that this consent was given. Pre-filled tick boxes are not consent. They must make an active decision. A deliberate yes / no option is preferred. For any B2B marketing communications, regardless of channel, the content must be about products and/or services that are relevant to the recipients' job role. Therefore, an opt-in process will confirm that. Caldes HUB helps you achieve this.

   Whilst compliance may seem onerous, it's important to focus on providing a great service through more effective marketing. This will be achieved by better-performing contact lists and databases, better privacy, protection of customer data and more trust in your brand.

5. **Processing of data.** If you email someone then you are 'processing' data. This means that if you are marketing properties then you are processing data. Property agents will therefore be processing personal information.

6. **The Data Controller.** "Data controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data is processed. In the case of a property CRM database this will usually mean someone at the company using the software.

0800 142 5604 **srb@caldes.com**

7. **The Data Processor.** "Data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. Put simply this will usually be your CRM software provider such as Caldes.

8. **Security Breach Notification.** *72 hours*. That's how long you have to notify your supervisory authority. Let's say you have a cloud-based database and someone leaves the company. If they then access the information in an unauthorised way and the information that they access is personal data (see above) then this will be seen as a security breach. Another breach might be someone who is with your company downloading a list of contacts and taking them out of the office, perhaps for personal use. If you find that such a breach has occurred, then you need to make a security breach notification. There will be levels of data breach. For instance, data that is sensitive, protected or confidential will hold more importance than perhaps an email address or a phone number.

9. **Privacy by design.** Caldes HUB focuses on privacy by design. This is a concept that marketers and other business divisions need to come to terms with quickly. Put simply, it means that privacy and data protection concerns must be at the forefront of an organisation's plans when it comes to managing data. Privacy can no longer be an afterthought. For instance, if you are using Outlook for emailing and you CC contacts who have not agreed for their email addresses to be shown, then you have revealed their email address without their consent.

10. **Security Policy.** This will include a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. It will define who has access to what and who can do what with that information. For instance, who can send out mail outs? Who can export data and under what situations? All staff will need to be fully aware of the policy and regularly reminded. Systems should help with that policy.

11. **System Security.** Your data needs to be secure obviously, although most data breaches will most likely be from staff and users than via insecure technology. Data processors and Controllers will jointly need to agree on security measures to make the data as secure as possible and the type of security will also depend on the sensitivity of the data. Most agency information is not that sensitive, but when it comes to transactions that changes. Continuity is also important. Data should be backed up off-site and there should be a plan to restore that should the worse happen.

12. **The Right to be Forgotten.** You need to be able to purge data. This might be automated (e.g. delete data after 3 years) or it might be manual (e.g. a delete button.) Caldes allows for both options.

13. **Data Visibility.** It is important to know where data is stored and be able to access all your information regarding an individual as quickly as possible, in case an individual puts in a 'Subject Access Request' to your firm, asking for information that you have on them. In reality this is not likely to be a big issue for Agents compared to say insurance companies or solicitors.

14. **Updates to privacy notices:** These need to be readily available and free of complicated jargon, stating who you are, what personal information you hold and what you plan to do with it. You must also highlight that individuals have a right to complain if they are unhappy with your use of their data.

15. **Fines.** It is unlikely that you will be fined if there is an issue if you have shown to have taken all the right steps and then you fix any issues once found. The fines will probably only apply to companies that do nothing. Whilst we cannot confirm this, that is the expected outcome.

If you are a Caldes.com customer, rest assured you are in good hands and will have an all-encompassing solution to meet the GDPR in full.

Click here to contact us to find out how we can help you meet your GDPR commitments.

0800 142 5604 **srb@caldes.com**