# CYBERRISKS+LIABILITIES

March/April 2018

## IN THIS ISSUE



Crendon Insurance Brokers

## Content Incentivises Consent: Marketing Under the GDPR

Since its introduction, the General Data Protection Regulation (GDPR) has been poised to radically change the way that organisations handle their digital business operations—and that includes digital marketing. Failing to update the way you handle data and digitally market to comply with the GDPR could result in significant fines and even prosecution.

While the GDPR governs overarching data protection law, the Privacy and Electronic Communications Regulations (PECR) specifically deals with electronic communications. Not only must you comply with the GDPR, you must also abide by existing PECR rules. These rules stipulate that you need consent to send marketing emails (with the exception of the 'soft opt-in' for existing customers), while new GDPR rules ban pre-ticked consent boxes and expand the definition of personal data to include business addresses such as joe.bloggs@anybusiness.com.

Marketing under the GDPR can be simple, as long as you adopt the following guidelines:

- **Content incentivises consent.** Send prospects a consent request that includes a piece of useful, free content. It could be a brief about important legislation, a risk that impacts their sector, or health and safety guidance. Just be sure you are able to contact them according to PECR rules. This strategy incentives consent by providing content. While the rest of your competitors will be sending bland consent requests that offer nothing to the recipient, your requests will stand out for the valuable content you include.
- **Do double opt-ins.** Although not necessary, double opt-ins, which ask the user to confirm in an email their consent preferences, help you keep track of consent and automatically builds in a mechanism to allow recipients to consent to specific types of processing.
- **Social media extends your reach.** Boost your social media presence, as connecting with prospects on social media and sharing relevant content with them does not violate the GDPR and can significantly expand the reach of your advertising message for a fraction of the price of traditional methods.

# WHAT IS PERSONAL DATA?

- Name


- Identification card number

- Home address

- Email address

- Location data (such as a geolocator used by certain apps)

- Online identifier (such as a username)


- Medical information

Source: European Commission

## How to Handle Data Breaches Under the GDPR

In 2017, 46 per cent of all UK organisations experienced at least one cyber-security breach or attack, according to government data. Personal breaches can be especially harmful as they can lead to the destruction, loss, alteration or unauthorised disclosure of, or access to, personal data. If the breach is likely to significantly impact individuals' rights and freedoms, your organisation must inform them without delay.

Under the GDPR, organisations are required to report certain types of personal data breaches to the relevant supervisory authority within 72 hours. If it doesn't, then an organisation could be fined up to €10 million or 2 per cent of its annual turnover, whichever is higher. Along with significant fines, personal data breaches could also have a profound impact on your organisation's reputation—even if you promptly inform all those affected.

Your reputation is intrinsically linked to your brand and if you experience a data breach, individuals may then view you as being untrustworthy and take their business elsewhere. What's more, failing to meet data breach requirements may hold your directors and officers liable for their inability to implement the necessary safeguards.

Protect your organisation from hefty GDPR penalties and reputational damage by following these three steps:

1. Contact the relevant supervisory authority of a breach within 72 hours.
2. Directly contact individuals affected by a breach if it is likely to result in a high risk to their rights and freedoms. (Note: The Information Commissioner's Office defines a high risk as 'the threshold for notifying individuals is greater than notifying the relevant supervisory authority'.)
3. Complete a breach notification containing the following information:
    - The categories and number of people affected by the breach
    - The categories and number of personal data records affected by the breach
    - The name and contact details of the data protection officer or an additional contact where more information can be obtained
    - A detailed description of the breach's potential consequences
    - A detailed description of what measures your organisation has taken or will take to address the data breach
    - A detailed description of the measures your organisation has taken or will take to mitigate any possible adverse effects to either itself or the individuals affected

**Crendon Insurance Brokers Ltd**

***Bespoke Insurance Products for Specialist Markets***

**0121 45 45 100**

**www.crendoninsurance.co.uk**