Roxburgh Milkins

General Data Protection Regulation (GDPR)

A 12-month retrospective

July 2019

For more information call +44 (0)117 928 1910 or visit www.roxburghmilkins.com

Roxburgh Milkins Limited, Merchants House North, Wapping Road, Bristol BS1 4RW

Common myths debunked

In advance of 25 May 2018 - the effective date of the GDPR - there was a startling amount of speculation and misinformation about how things would change once it came into force. So much so, that the Information Commissioner's Office itself started a blog series debunking the most common misunderstandings.

In the year since the GDPR came into force, it has become clear that some fears were unfounded. Here are 3 of the most common myths, which have been debunked over the past 12 months:

1. Consent is key

One of the most common misconceptions was that the GDPR would bring the use of personal data to an end, unless you had the consent of the data subject. In fact, consent is one of six lawful grounds for processing personal data, and others may well be more appropriate grounds for processing personal data.

For example, most data processing will be taking place because there's a contractual relationship between the parties, in which case the lawful ground would be that "processing is necessary for the performance of a contract to which the data subject is party…".

A lot of the misinformation around the need for consent related to e-marketing, which the GDPR does not actually cover specifically. E-marketing is governed more by the Privacy and Electronic Communications Regulations, which set out the requirements for getting opt-in consent for certain electronic marketing, and which didn't change as a result of the GDPR coming into force. What did change was the standard for consent, which is now higher than it was before and requires clear, positive action. Many businesses made the mistake of thinking that fresh consent was the only option, leading to the so-called "bonfire of the mailing lists".

2. Mass data deletion

The GDPR places more significance on the proportionality of holding and using data, with greater emphasis on data only been held for as long as necessary, and a number of enhanced data subject rights to control the use of that data.

A misconception was that this would beckon the end of data retention, meaning all data would have to be deleted as soon as the primary purpose for collecting that data had expired or ended. This is not true.

In fact, the rules around data retention aren't too different from the previous law. The key is that the data controller has taken the time to establish and document their reasons for retaining personal data and (if relevant) continuing to use it even though the primary data processing activity has ended. Provided that the controller can justify its position, it would not be in breach of the GDPR requirements by retaining personal data for longer.

3. Data subject is King/Queen

Whilst the rights of the data subject are undoubtedly important, both businesses and individuals made the mistake of thinking that the GDPR would give data subjects absolute authority to determine how their personal data was used. This is incorrect.

The GDPR does certainly give enhanced rights to data subjects in terms of access to their data, information about how it is processed, and the ability to control that data use. However, it does not give data subjects carte blanche to demand that data processing is stopped, or data is erased, in all circumstances.

Many commentators warned about an influx of data subject access requests and requests for erasure (or the 'right to be forgotten'), and some businesses may indeed have received higher than normal requests, but it wasn't the Armageddon that some predicted.

This is partly because the right to request erasure (and also the restriction of processing) of data is actually qualified in a number of ways. For example, a data controller would not be required to comply with a request if it can show that the processing is still necessary, it has a legal ground for processing such data, and/or there is a legitimate interest in processing the data, which overrides the data subject's rights.

A few lessons learned

Over the past year, we have learnt a few things about the interpretation of the GDPR and its enforcement in the UK.

1. No rush to issue fines

The Information Commissioner's Office (ICO) has not been in a rush to exercise its new enforcement powers. Under the GDPR, the maximum fine has increased from £500,000 under the old law, to €20 million, or 4% of annual worldwide turnover, whichever is higher. This struck fear amongst businesses and led to a fair amount of scaremongering around the risks associated with the GDPR and data processing.

Thus far - aside from the recent high-profile British Airways announcement (see below) - the ICO has not really used its enhanced fining power. This is partly because it has been actively engaged on investigations which pre-dated the implementation of the GDPR, so fell under the old regime, though the ICO has also stressed that it wouldn't rush any enforcement action and that its focus was on achieving the right outcome - and improving compliance - rather than arbitrarily issuing punishing fines.

The lesson for businesses is that proportionality is key. The risk will always depend on the nature of the data involved, the processes in place to protect such data, and a company's adherence to those processes, as well as the nature of the breach or non-compliance. As before, the ICO's focus will always be on the worst offenders and the vast majority of issues and complaints are unlikely to warrant even a reprimand from the ICO, let alone a multimillion pound fine.

Of course, that doesn't mean that compliance should not be taken seriously. Only through constant vigilance and good practice can a business be confident that the ICO will never need to come knocking.

2. GDPR compliance - a marathon, not a sprint

In the rush to become compliant with the GDPR by the time it came into force on 25 May 2018, it may have been easy for businesses to forget that data protection compliance is an ongoing challenge and not a one-off hurdle.

While the upfront work will stand businesses in good stead for years to come, a lot of the requirements under the GDPR are ongoing or require constant review:

(a) **Processing activities -** most businesses will undertake new or different processing activities over time, as products and services develop. It is not always enough to rely on the same justifications for those activities as the original purpose for which the data was collected. Any new processing activity should involve an assessment to determine whether it is consistent with the reasons for which the data was collected, whether there is a lawful basis for processing, and whether any further notification or consent is required with data subjects. The results of this should be recorded.

(b) **Technical and organisational measures -** one of the key GDPR requirements is to maintain appropriate technical and organisational measures to protect personal data from intentional or accidental misuse, loss etc. This is an ongoing requirement and any business should keep its measures under review to ensure they remain appropriate. The proper protection of data is dependent on a number of interconnected elements, including IT and storage systems, technical security such as password protection and encryption, personnel, premises and physical security. All of these may shift, change and evolve and a business needs to ensure that its policies and procedures remain relevant and appropriate at all times.

(c) **Data retention/deletion -** The assessment of whether continuing to hold and use personal data is appropriate is an ongoing process. Businesses should keep their storage and processing of data under regular review and delete data when it is no longer relevant or necessary.

(d) **Data subject requests -** having the process and resource to deal with data subject requests is an ongoing requirement.

(e) **Record-keeping -** the GDPR sets out record keeping requirements. Whilst they don't apply to small businesses, any business would be well-advised to keep accurate and up to date records of its data processing activities, any notices/consents used for such data processing, its security measures, and other compliance issues.

(f) **Third party relationships -** many businesses will use third parties to process personal data on their behalf (data processors). In order to do so, you must now have a written contract in place with GDPR-compliant data processing clauses. Businesses may also share personal data with other controllers, which may require contracts to govern the sharing of data and how it is used. Businesses should keep an up to date record of such third-party relationships and ensure that it is legally able to share personal data with any processors or other data controllers, keeping a record of its justification for doing so.

3. ICO registration still a must

When the GDPR made no mention of data controllers having to register with national regulators, there was speculation that the need to register with the Information Commissioner's Office may be abolished, sparing businesses an administrative hurdle (and recurring fee).

The UK Government put an end to such speculation, by implementing regulations requiring every organisation or sole trader which processes personal data to pay a fee to the ICO (subject to some exemptions).

The ICO publishes details of all data controllers who pay the data protection fee, thereby maintaining the data protection register, which remains publicly accessible via the ICO website. This includes details of the business and its data protection representative (if provided), though it no longer includes details of the processing activities undertaken as the previous register did.

The fee is now tiered, from £40 to £2,900, depending on the size of the data controller (based on turnover and number of employees). It is down to individual businesses to assess the level of fee they should pay based on their business type and size.

Previous registrations remain valid until they expire, at which point a registration under the new scheme should be made.

It is important that any business which processes personal data electronically (non-electronic processing is exempt) continue to pay the fee annually, as otherwise the ICO may take enforcement action, as it has done in a number of cases already in the past year.

4. The GDPR is still evolving

When the GDPR came into law, there were a fair few grey areas and question marks over how certain aspects would be interpreted and enforced. Many of those questions still remain to some extent and may take time to resolve. Ultimately, it will only be through enforcement and improved guidance that we'll get full clarity on some of the vaguer elements of the GDPR.

In the spotlight: Cookies

Website cookies have been back in the spotlight recently, as the ICO website (www.ico.org.uk) came under fire for not having a fully compliant cookie notice. As a result, the ICO has not only updated the cookies notice to include a specific opt-in for non-essential cookies, but it has also updated its guidance for other businesses.

The use of cookies and similar technologies are governed by the Privacy and Electronic Communications Regulations (PECR). The PECR requires that websites obtain consent from individuals for the use of any non-essential cookies. 'Non-essential' cookies are those which aren't strictly necessary for the provision of the website and any services the individual accesses via the services.

When the PECR first came into effect, it was feared that it would effectively mean the end for the use of cookies for analytical and advertising purposes, due to the need to provide a notice to users when they first access the website and give them the option to consent or set their preferences.

In reality, partially due to the relatively lax approach taken by the ICO in its guidance, most websites relied on a fairly simple notice with a simple 'okay/accept' acknowledgement option, or continued to rely either on presumed consent (i.e. an individual consents if they see a notice about cookies and continue to use the website regardless).

However, the GDPR changed the standard for consent, meaning non-specific or presumed consent is no longer valid. Under Article 7 of the GDPR, the requirements are:

- You must be able to demonstrate that you have valid consent;
- Your consent requests must be clearly distinguishable from other matters - i.e., in the context of cookies, you cannot bundle consent for non-essential cookies with essential or necessary cookies;
- Consent requests must be in an intelligible and easily accessible form, using clear and plain language; and
- Individuals must be able to withdraw their consent at any time.

Silence or inactivity **does not** constitute consent.

As a result of the new publicity, the ICO has now issued firmer guidance, making it clear that simple notices with a generic acknowledgement or consent to cookies, or presumed consent, are not good enough. Also, the ICO has stated that websites should **not** set any non-essential cookies until consent has been given. This means that many business websites are failing to fully comply with the PECR requirements on cookies.

Businesses should urgently review their cookies policy and website notices and will need to consider reworking their websites to (a) get specific consent to all non-essential cookies, (b) prevent the setting of any non-essential cookies until such consent is given, and (c) provide full information about the cookies they use and any third party cookies used. You will find further guidance regarding this on our website.

Looking ahead: further developments

1. The GDPR and Brexit

The UK's exit from the European Union may have been delayed but, whether in October or at some future date, it looks inevitable. In the event of a deal being reached, the UK will continue to be subject to the GDPR for the duration of the transitional period and likely for some time after.

However, even in the event of a no-deal, the current UK Government has said that the GDPR will continue to apply unchanged. What may change is the ability to transfer data between the UK and other European countries, particularly if the EU does not recognise the UK as an 'adequate' country for the purpose of international transfers, which would require businesses to take additional steps (such as signing up to EU model data transfer clauses) in order to be able to continue receiving data from the EU.

For more on this, see our blog article on the no-deal implications at https://www.roxburghmilkins.com/latest/blog-articles/guidance-published-on-data-protection-implications-of-no-deal-brexit.

2. Enforcement and Fines Ahoy

As we've covered above, it has taken more than a year for the first high profile fine to be announced by the Information Commissioner's Office under the new GDPR regime.

On 8 July, the ICO announced that British Airways, which suffered a data breach affecting up to 500,000 customers in September 2018, will potentially be hit by a fine of £183.39 **million**, far higher than any fine the ICO has previously been able to issue. This announcement is provisional, and the ICO will take representations from BA and other interested parties before making its final decision, but it is significant nonetheless.

On the smaller end of the spectrum, we have seen a number of enforcement actions and fines for companies which have not paid the data protection fee (i.e. registered with the ICO). These are likely to continue as it is a simple investigation and easy enforcement win for the ICO. It is important to make sure you have paid the fee if you process personal data. You can find out more here - https://ico.org.uk/for-organisations/data-protection-fee/.

3. PECR Updates

There has been talk of the Privacy and Electronic Communications Regulations (PECR) being updated for some time. Whilst minor changes have been made, most recently in January 2019 to reflect the impact of the GDPR, the European Union has been planning a much more fundamental overhaul.

At the moment, the PECR is based on an EU e-Privacy Directive. EU directives provide general legal conditions, which are then implemented separately in each EU member state through national regulations.

The EU is planning to replace that directive with a new EU-wide regulation, which - like the GDPR - will apply to all member states, without the need for any local implementation. This will make the e-privacy laws more consistent across the EU.

The ePrivacy Regulation has been agreed by the EU and was originally due to be implemented in 2018, but is now slated for some time in 2019. A fixed implementation date has not yet been announced.

Regardless of the status of Brexit, it is highly likely that the UK will align itself with the ePrivacy Regulation once it comes into force, so businesses will need to be aware of it and ensure they continue to comply with the rules around e-marketing and cookies. We will provide more information on the new Regulation as and when an implementation date is set.

GDPR compliance – how we can help

As we have explored above, GDPR compliance is an ongoing challenge. Roxburgh Milkins has a number of services which can help businesses keep on top of their data protection obligations and apply best practice.

Data Protection Audit

Ahead of the implementation of the GDPR, many businesses underwent audits of their data, policies and practices. Whilst this is an important first step, the obligation to monitor and audit data protection compliance is an ongoing commitment. Any business which processes a high volume of data, is engaged in a range of processing activities, and/or processes data in a higher risk or sensitive context, should regularly - and, ideally, at least annually - audit its business and processes.

Roxburgh Milkins is able to offer assistance with conducting a legal data protection audit. We can provide a questionnaire, which is set out by reference to the key GDPR obligations and requirements. We then review the answers submitted to the questionnaire, along with the supporting documentation, to prepare a report on GDPR compliance.

This report will include a risk assessment of any deficiencies or non-compliance issues, along with advice on best practice and potential actions to improve compliance. We can assist in updating documents, improving policies and procedures, and implementing changes to meet the data protection requirements as closely as possible.

GDPR Data Protection Checklist

As well as a full audit, we can also provide a simpler GDPR compliance checklist, ideal if you have already had an audit done, or feel a full audit would be OTT based on the type of processing you do.

This checklist broadly covers the same GDPR principles and requirements as the audit but focuses on the absolute fundamentals and is quicker and easier to complete. As with the audit, we will review your responses and documents, provide a report highlighting any shortcomings and recommending improvements, and provide as much help as you need to make the necessary changes and improvements.

Internal Policy Documents

Roxburgh Milkins is able to assist with the preparation and implementation of the full suite of internal data protection policy documents. Whether you're a small business in need of a simple data protection policy, or a larger data processing company requiring detailed security policies, breach reporting procedures, and employee training, we can help.

Policies play an important part in GDPR compliance, not only by providing a written record of how you protect personal data, but also by raising staff awareness of their role in protecting personal data. The GDPR requirements will have had an impact on internal policy content, as it changed several requirements around the storage and use of personal data, notification requirements, and data subject rights, so it is important that policies are kept under review and updated if necessary. Again, we can assist you in reviewing the policies/procedures you have in place and bringing them in line with the latest requirements.

Contract Templates

Any well organised business should have appropriate contracts in place for its dealing with customers and suppliers. If these contracts involve the exchange and processing of personal data, those contracts should now include GDPR-compliant processing clauses.

Roxburgh Milkins can help review your relationships with suppliers and sub-contractors to determine whether you need data processing clauses and provide suitable provisions if so. Likewise, if you process personal data on behalf of others, you should consider updating your contracts to include data processing clauses, so your customers don't have to ask for them or insist on you using their contract terms, which we would be happy to help with.

Contact us

If you'd like to get in touch with us regarding any of the contents of this note, or to discuss your own GDPR requirements, please feel free to do so. Our commercial team details are:

Ian Grimley - ian.grimley@roxburghmilkins.com

Carl Spencer - carl.spencer@roxburghmilkins.com

Helen Naylor - helen.naylor@roxburghmilkins.com

You can also contact the office by telephone on 0117 928 1910.