qLegal

The small print for BIG IDEAS

Disclaimer: This toolkit describes the law in general terms. It is not intended to provide legal advice on specific situations and should not be relied upon as a source of legal advice.

Date produced: May 09, 2019

qLegal Toolkits

The Impact of the GDPR for Start-ups: A UK Perspective

The General Data Protection Regulation 2016/679 (commonly known as the GDPR) came into effect throughout the European Union (EU) and in the United Kingdom (UK) on 25 May 2018. The GDPR has been implemented into UK law by the Data Protection Act 2018, which replaces the Data Protection Act 1998.

What does the GDPR do?

The GDPR has been implemented to:

- Unify and standardise fragmented data protection laws across Europe, thereby increasing certainty in their application, interpretation and enforcement.
- Strengthen individuals' (i.e. "data subjects") control over their personal data by granting them rights such as data portability and the "right to erasure", amongst others.
- Provide a broad and modern framework to data protection in order to account for advances in technology.
- Encourage greater compliance with wider extra-territorial application and heavier penalties for breaches.
- Impose direct liability on processors (rather than just on controllers).
    - Controllers are responsible for determining the purposes and means of processing personal data.
    - Processors, in contrast, merely process personal data on behalf of controllers.

qLegal

The small print for BIG IDEAS

The GDPR and Start-ups

Overview of the Compliance Process

If you are a start-up beginning the process of reviewing your GDPR compliance, you should start by carrying out an internal assessment. This should involve all parts of your business in order to identify and audit all the different types of personal data being processed, as well as identify the purposes of that processing and map data flows into and out of the start-up. This will help you identify and focus on any higher-processing activities, begin documenting their processing activities and strategise the procedures and changes needed to comply with the GDPR.

In addition, you should create awareness amongst your members and employees about the necessity of properly processing personal data and the internal policies put in place.

Credit: Dylan Gillis

An immediate example of where you may need to address the GDPR's requirements relates to electronic direct marketing activities, such as newsletters and e-mail marketing. In most cases, these requirements include:

- Establishing a legal basis for processing personal data in connection with such direct marketing (e.g. names and e-mail addresses) – this will typically be consent from the individual data subjects;
- Where applicable, obtaining valid consent from the data subjects;
- Being able to demonstrate that such consent was obtained; and
- Putting in place measures to ensure that if a data subject later withdraws their consent for direct marketing (or otherwise objects to the use of their personal data for such purposes), that no additional direct marketing is sent to that data subject.

Complying with the GDPR

The GDPR applies to all personal data processing activities by your start-up established in the UK, including for example, personal data processed in respect of your start-up's employees, providers, website visitors and customers, regardless of your start-up's size or its commercial purpose. For a UK start-up, it does not matter if certain processing activities only relate to data subjects outside the UK or EU – all personal data, irrespective of the location of the data subject will be in scope for the purposes of the GDPR.

In the UK, the Information Commissioner's Office (ICO) is the supervisory authority responsible for enforcing the GDPR. The ICO has a variety of powers at its disposal, including undertaking investigations, requiring the provision of certain documents, issuing warnings, applying temporary or permanent restrictions on data processing, suspending personal data transfers and issuing fines for non-compliance, amongst others.

qLegal
The small print for BIG IDEAS

In the UK, depending on your start-ups particular personal data processing activities, you may need to dedicate relatively extensive time and financial resources to ensure GDPR compliance. Consequently, for accountability purposes, you should consider allocating a budget reserved for GDPR compliance, including for specialist legal or business counsel, where required.

Some compliance measures include:

- Appointing a Data Protection Officer (DPO)
  - More often than not, you will not need to appoint a DPO, however, you should still consider whether you need one. The DPO would be responsible for data protection compliance within the organisation to ensure that your start-up meets its GDPR obligations.
  - In line with the GDPR, you are obliged to designate a DPO when your start-up's main activities relate to data processing that requires regular monitoring of individuals, or when you carry out large-scale processing of special categories of personal data, such as: health records or criminal convictions and offences.
- Completing Records of Processing Activities
  - Under the GDPR your start-up and its representatives (data processors) are required to maintain a record of processing activities. This could mean including information such as:
    - The name and contact details of the controller and other parties involved with the data processed.
    - The purposes for which the data is being processed.
    - A description of the categories of data subjects (people) and the categories of personal data collected.
    - The categories of recipients where personal data may be disclosed to, including whether they are in third countries or to international organisations.
    - The estimated time limit for erasing the data held.

  For more information on how to comply with the GDPR's Privacy Register requirement, watch our short webinar. In addition, Privacy Register, a free online privacy management system, offers a standardised privacy register.
- Putting in Place Privacy Notices
  - When data related to a data subject is collected from the data subject directly, the data controller must, at the time of procurement of the data, provide the data subject with information such as:
    - The identity and the contact details of the data controller and if applicable, the details of the controller's representative or data processor.
    - The DPO's contact details.
    - The intended purposes for which the data is collected and the legal basis for the processing.
    - The recipients of the personal data, if any.

- Putting in Place Security Measures
  - You need to ensure that you have implemented appropriate technical and organisational security measures in relation to your start-up's specific data processing activities. This is relative to, the standards, the cost of implementation and the nature of the data processed, including the risks for the rights of a data subject, start-ups and their data processors.
  - It may be worth referring to Article 32 of the GDPR since it outlines required implementations of security measures. Some requirements include:


Credit: @rawpixel

    - The pseudonymisation (the replacement of all data in a database etc. that identifies a person with an artificial identifier) and encryption of personal data.
    - The ability of ensuring ongoing confidentiality and resilience of data processing systems and services.
    - The ability to restore the availability and access to personal data in a timely manner should a physical or technical event occur.
    - Having a process in place regularly testing and evaluating the technical and organisational measures adopted for the security of the data processed.
    - Assessing an appropriate level of security by considering the risks which could occur through data processing, in the event of accidental or unlawful, loss, unauthorised disclosure or access to the personal data transferred or stored.
  - Your start-up, as data controller, and its processors should ensure that anyone with access to personal data does not process the data held except unless instructed to do so by you or if they are obligated to do so by EU or member state laws.
  - The main purpose of these security measures is to prevent data breaches from occurring but also implementing measures to minimise and mitigate any risks arising from a breach of personal data held.

Penalties

The GDPR's penalty regime provides a strong incentive for you to ensure that your start-up's personal data processing activities are carried out in compliance with the GDPR.

In particular, in addition to the ICO's enforcement powers outlined above, the ICO can issue fines for non-compliance. The level of such fines will depend on the particular requirement of the GDPR that has been breached, as well as the severity of the breach and certain other factors.

For example, a failure to:

- Adhere to the GDPR's data processing principles or to comply with a data subject's rights in respect of their personal data could result in a fine of up to €20 million (or the equivalent amount in GBP) or 4% of a start-up's global annual turnover, whichever is higher.

- Implement appropriate technical and organisational measures to keep personal data secure or to report a personal data breach to the ICO when required to do so could result in a fine of up to €10 million (or the equivalent amount in GBP) or 2% of a start-up's global annual turnover, whichever is higher.

The GDPR and Brexit

The government has confirmed that the same data protection rules under the GDPR will continue to apply in the UK even after a hard or no deal Brexit (albeit with some minor adjustments to ensure consistency with the UK's departure from the EU). In this sense, you should implement all the measures required to comply with the GDPR to the same extent that other EU start-ups would.


Credit: John Cameron

Brexit may, however, have an impact on data protection for your start-up in the following ways:

- If your start-up processes personal data about individuals in the EU in the context of offering goods or services to (or monitoring the behaviour of) those individuals, you may be required to appoint a formal representative in the EU. This person would be required to act as your start-up's local representative for data subjects and supervisory authorities in the EEA.
- If your start-up receives personal data from third party controllers in the EEA, those third-party controllers may require your start-up to enter into certain contractual terms approved by the European Commission (known as the standard contractual clauses). This is because the UK will be treated as a third country under the GDPR (at least if/until it is awarded an adequacy decision), meaning that transfers to controllers and processors in the UK will be restricted for other controllers and processors in the EEA. However, it is worth noting that EEA member states will be treated as having an adequacy decision (meaning transfers into the EEA will not be restricted).

Conclusion

Even though the GDPR creates a sizeable burden for your start-up, it can also provide competitive advantages by encouraging you to demonstrate compliance with data protection rules as a benefit for customers and other stakeholders. In an increasingly privacy-aware consumer market, being able to reassure individuals that their data is being handled with the utmost care is surely a competitive advantage.

Regardless of the UK's exit from the EU, the data protection rules currently in place, will continue to apply after Brexit. Consequently, you should continue to ensure that your start-up complies with the GDPR in order to avoid incurring any regulatory penalties which could be devastating to your new business, if applied to their fullest extent.

qLegal

The small print for BIG IDEAS

This toolkit was drafted by students from the Centre for Commercial Law Studies, Queen Mary University of London: Pavlos Dekatris and Natalia Gonzalez, as part of the eHealth Hub project.

The eHealth Hub project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No727683.