CAREY OLSEN

Data Protection – The Privacy Force Awakens?

Service area / Dispute Resolution and Litigation
Location / Group
Date / January 2016

Had it not been for the release of the latest Star Wars film, the fact that agreement was reached on the new EU Data Protection Reform package may have made rather more of a splash in the media.

Introduction

The European Council, Commission and Parliament agreed the text of the EU Data Protection Reform package (originally proposed by the Commission) on 15 December 2015. The package is part of a range of measures being progressed to facilitate the vision of a Single Digital Marketplace in Europe. Data protection legislation across the EU is currently outdated as much of it was introduced at a time when many of today's online services were not yet in place. Differences in implementation have also led to uncertainty and additional cost for businesses. There has been an increased focus on the impact of cross-border data transfers following the abolition of the Safe Harbour regime[1], and new legislation is needed to ensure that the Article 8 right to protection of personal data is suitably enshrined in the digital world in which we live.

The aim of the new package is to strengthen the rights of individual citizens via the use of global data protection standards, more robust enforcement of the rules and the streamlining of international transfers in order to facilitate business. However, it is important that the individual's control over how, where and for what purpose their personal data is processed is maintained within this context.

There are two elements to the package:

- the General Data Protection Regulation (GDPR), which gives consumers more control over their data, and
- the Data Protection Directive (DPD), which covers data transfers and the exchange and protection of information as between law enforcement agencies in the context of the investigation of crime and prevention of terrorism.

The GDPR and DPD are likely to be formally adopted in early 2016, meaning that the GDPR will apply from early 2018. The DPD has a two-year implementation period, during which time the Member States are required to update their legal frameworks. However, bearing in mind the nature and scope of the changes, there is a significant amount of preparatory work to be undertaken by businesses in order to be prepared for the new regime.

Key changes

Whilst the reforms are many and wide-ranging, some of the key points are set out below.

Tighter rules on consent

- It will now be necessary for consent to be freely given, specific and informed. It should also be an unambiguous indication of consent by statement or affirmative action which is demonstrable, easily accessible and intelligible. It can also be withdrawn at any time.

1 See our previous briefing notes Safe Harbour in a Storm? and Another Safe Harbour?

Easier access to data

- Individuals will have better and more information on how their data is processed and it should be available in a clear and understandable way.

A formalised "right to be forgotten"

- Following the famous Google decision, individuals can require their data to be deleted under the existing regime, providing that there is no legitimate reason for it to be retained by the data controller. This right is extended and formalised under the new legislation.

Right to know when one's data has been hacked/breached

- Stricter timescales apply for notification to the supervisory authorities of a data breach - 72 hours "where feasible". The individual(s) concerned should also be informed "without undue further delay" if there is a "high risk" to their rights and freedoms.

Data protection by design/default

- Safeguards will be expected to be built into services and products from the earliest stage of development and privacy default settings will be the norm.

Stronger enforcement of the rules

- Non-compliance could lead to hefty fines being imposed, the largest outlined in the GDPR being 4% of global turnover of the breaching entity.

Extra-territoriality

- If there is one aspect of the new provisions which will be of interest to businesses in Guernsey and Jersey (and other jurisdictions outside the EU), it is their extraterritorial application.
- There will be one single set of rules applicable across the EU and as such it will make it easier and cheaper for companies to do business across the EU. The rules will also apply to companies doing business in or marketing into the EU, thus extending the scope of the jurisdiction to territories and businesses based outside of the EU which either have an establishment within the EU or who are:
  a. offering goods or services (whether or not for payment) to individuals within the EU; or
  b. monitoring/profiling individuals within the EU.
- Following the collapse of Safe Harbour, the GDPR maintains the "adequacy" requirement for data transfers to countries outside the EU. The guidelines remain strict and negotiations with the USA are ongoing, so there will likely be additional guidance on this aspect in due course. There is a new menu of options to legitimise such transfers, including BCRs and codes of conduct.

"One Stop Shop"

- There will be a single supervisory authority, the European Data Protection Board, which will be the sole point of contact for businesses operating in the EU. This should result in large savings for businesses.

Data portability

- It will be easier for individuals to transfer their personal data between service providers (i.e. purchasing a new smart device or IoT technology item and "porting" one's profile to the new device).

Data protection officer

- Companies processing a large amount of sensitive personal data or monitoring on a systematic basis are required to appoint a Data Protection Officer. There are certain exemptions for categories of SME which should minimise the cost to those businesses.

The DPD will enable law enforcement agencies both within and outside the EU to exchange information more effectively, enabling more efficient and less costly investigations. There are also clearer protections for the personal data of individuals involved in criminal proceedings, whether as victims, witnesses or suspects.

Impact

This is the largest change to data protection laws for many years, and a significant one in terms of the need to start planning for the changes at an early stage. There are substantial additional requirements which will inevitably lead to increased cost of compliance. However, that could be offset by the ability of businesses to make use of a single applicable law and regulatory body in Europe.

The legislators have attempted to adapt to the changing technological environment and sought to "future proof" as much as possible, but there will inevitably be a continuing tension between the tech companies' plans for innovation and compatibility with the new regime.

The tension between protecting citizens' personal data and the desire by the authorities to monitor data for the purposes of crime and terrorism prevention will continue to rear its head. Indeed, this issue is currently the subject of discussions between Apple and the UK government.

For those businesses operating from Guernsey and Jersey, it remains to be seen whether the local regulators will adopt the measures taken by the UK government (when the time arises) or whether there are any local adaptations which could or should be made.

Continued

For other jurisdictions outside the EU, it will be a question of whether their local regulators adopt similar legislation, adapt existing legislation, or choose to follow their own route. Given the clear movement towards a Single Digital Marketplace in the EU, it makes sense for the Channel Islands in particular to follow suit and take similar steps, which should facilitate continued access to the EU marketplace. It is also consistent with Guernsey's stated aim of being a safe place for the hosting and storage of data and both islands' work towards a digital future.

Irrespective of what the local regulatory approach is, Channel Islands businesses of any size (particularly those in the financial services sector) are likely to be caught by the extraterritorial application of the new rules – meaning that such businesses are likely to have to comply with the new rules as if they were directly applicable to them.

As ever, we are happy to discuss the potential impact of the new provisions with our clients. We will issue further updates in due course.

Subscribe for more

FIND US

Carey Olsen
Rodus Building PO Box 3093
Road Town Tortola VG1110
British Virgin Islands

T +1 284 394 4030
E bvi@careyolsen.com

Carey Olsen
PO Box 10008 Willow House
Cricket Square Grand Cayman
KY1-1001 Cayman Islands

T +1 345 749 2000
E cayman@careyolsen.com

Carey Olsen (Guernsey) LLP
PO Box 98 Carey House
Les Banques St Peter Port
Guernsey GY1 4BZ
Channel Islands

T +44 (0)1481 727272
E guernsey@careyolsen.com

Carey Olsen Jersey LLP
47 Esplanade St Helier
Jersey JE1 0BD Channel Islands

T +44 (0)1534 888900
E jerseyco@careyolsen.com

FOLLOW US

Subscribe for more

Visit our dispute resolution and litigation team at careyolsen.com

PLEASE NOTE