

# ECTA

European Communities Trade Mark Association

ECTA Bulletin June 2018



## GDPR: What now?



Author: **Simon Miles**  
Partner, Head of Intellectual Property/IT  
Edwin Coe LLP  
Simon.miles@edwincoe.com

Co-author (non-ECTA member):  
**Yoon Hur**  
Solicitor, Edwin Coe LLP  
Yoon.hur@edwincoe.com

The General Data Protection Regulation (“GDPR”) has been *the* regulatory reform topic in everyone’s minds for the past two years, impacting businesses across all sectors and territories, and finally coming into force on 25 May 2018. Our focus on GDPR until now has been preparing for its implementation and below we summarise seven major changes under the regulation which are particularly likely to present compliance challenges going forward.

### 1. Tougher sanctions

The “headline” news surrounding GDPR has been the dramatic increase in maximum fines: a two-tier system of penalties (depending on the nature of the breach) of up to either (i) €10m or 2% global annual turnover, or (ii) €20m or 4% of global annual turnover, in both cases whichever figure is higher.

To put this in perspective telecommunications provider TalkTalk’s £400,000 fine for security breaches of customer data in 2016 could have amounted to £50 - £60m under the GDPR. In the UK whilst the Information Commissioner’s Office (“ICO”) Head of International Strategy & Intelligence Steve Wood has indicated that the ICO is taking a risk-based, pragmatic approach to enforcement, these figures speak for them-

selves as regards the increased scrutiny over and importance of compliance with dealings with personal data. Demonstrating compliance (see point 4 below) is a key priority.

### 2. Wider scope

The GDPR is an EU regulation but it is not an EU-only issue. It applies to all entities which process personal data of EU-resident data subjects by offering goods or services to them or monitoring their behaviour, regardless of where such entities are based. Overseas organisations with current or anticipated future business dealings in the EU will need to keep abreast of developments in data protection law as they occur.

### 3. Managing data subject rights and data breaches

The GDPR greatly enhances the scope of rights individuals have over their personal data. Individuals are able, in certain circumstances, to request the access, deletion, restriction or transfer of their data or object to further use of it altogether, and they must also be clearly notified of their rights to do so. Additionally, the GDPR obliges the prompt reporting of data breaches to both the relevant regulator and the affected data subjects.

The rules around these rights are complex and effective business procedures to manage them are critical, not least because failure to do so may also lead to individuals lodging complaints against entities directly to their data protection regulator (and such individuals must be informed of their rights of complaint in advance of collecting their data).

### 4. Demonstrating compliance and accountability - on an ongoing basis

Underpinning the GDPR is the principle that organisations must not just comply with the rules, but also be able to demonstrate that they do so. Entities must keep records of all processing activities, logs of data breaches and records of consents received/withdrawn. They must also document their prior risk evaluation and mitigation strategy process for certain processing activities, through privacy impact and legitimate interests assessments.

While many organisations have worked hard to get their processes compliant in time for May, the content of these documents will need to be reviewed and re-assessed over the life cycle of a processing activity. These documents are

generally only for internal use, so their primary purpose will be to satisfy regulatory audits and they are likely to be particularly scrutinised for compliance.

### 5. Making notices shorter...with more information

Transparency is a key new principle of the GDPR, and requires entities to overhaul core consumer-facing documents to ensure they provide information in a clear, concise, intelligible and easily accessible way. This mainly affects privacy policies and consent forms used to obtain individuals’ consent to the use of their data for certain purposes. These should have been updated in time for the GDPR, but any material changes in processing activities to the information already disclosed (particularly in relation to the purposes for processing and categories of data collected) will need to be updated and re-notified to affected individuals.

Simultaneously, the GDPR is very prescriptive about the content and form required in these documents. This presents an ongoing challenge for balancing the two compliance obligations, and also means that there will be more certain criteria for data subjects or regulators to assess whether a compliance obligation has been met.

### 6. Reviewing supply chains

Businesses are likely to use suppliers to process information on their behalf. Arrangements involving personal data must now always be in writing, and the contracts must include/be updated to include an array of prescribed requirements imposed upon a processor. The general obligations in these requirements are mandatory, but the specific mechanics for enforcing them are not (e.g. timeframes), so there is still some scope for negotiation on both sides.

Overseas suppliers unfamiliar with the scope of GDPR are often alarmed by the introduction of these new contractual requirements. In fact the regulation, in another expansion of scope, also imposes a number of obligations directly on processors themselves (including enforcing appropriate data security measures, which is one of the obligations required to be in the contract), so compliance is in everyone’s interest.

### 7. Limited “grandfathering”

In the UK the ICO has emphasised that compli-



ance is expected from Day 1 and that no 'grace period' will apply. This means that as of 25 May, entities will be assessed by GDPR standards in respect of all personal data, regardless of when the data was originally collected or when an original breach occurred.

Personal data that was collected on the basis of consent prior to the GDPR will no longer be lawful, unless the original mechanisms for collecting consent originally already met the higher GDPR standards, or have subsequently been 're-permissioned' with updated forms to meet

these. Breaches that occurred years ago but have only been reported subsequently (such as the recent *Facebook Cambridge Analytica* case) are now likely to be judged under the harsher current rules, with the higher fines to match.

Therefore it is important for entities to thoroughly audit processing activities and data management systems on an ongoing basis to not only ensure compliance for new activities going forwards, but for all current processing activities operated by the business to avoid any unexpected skeletons in the closet coming to light.



Verifier:  
**Patrick Wheeler** (ECTA Member)  
Partner, Head of IP and data protection  
Collyer-Bristow LLP

# ECTA

EDINBURGH

26-29 JUNE 2019

# NEW HORIZONS

THROUGH THE  
HIGHLAND HAZE

# 38<sup>TH</sup> ANNUAL CONFERENCE

*In* a period of change within the EU, cool heads and constructive ideas are needed. As the UK leaves the EU we might see the shape of the 'New Horizons' through the 'haze of uncertainty' that currently clouds our view.

ECTA's 38th Annual Conference in the stately charm and elegance of Scotland's capital city Edinburgh will provide the ideal setting to meet friends and colleagues and take part in an informed debate on "New Horizons through the Highland Haze". Edinburgh is one of northern Europe's most ancient and historic cities, which has enjoyed trading relations with its European neighbours across the North Sea for more than 800 years.

Edinburgh's "New Town" (which dates from the mid-1700s) and the adjacent "Auld Toon" (Old Town) which has preserved much of its medieval street plan and buildings dating from the 16th century form part of a protected UNESCO World Heritage Site. The famed "Royal Mile" runs from Edinburgh Castle (which overlooks the conference hotel) to "Holyrood Palace" (the Queen's official residence in Scotland), and the new Scottish Parliament building.

There are limitless sights, scenes and monuments. Tweed and tartan abound with many excellent bars and restaurants, and of course the glorious scenery of mountains and lochs can be found in the city's environs. Add to this excellent hotels, a state of the art Conference Centre, 33 airlines serving 188 routes from 130 destinations into Edinburgh, and

**YOUR WELCOME TO SCOTLAND  
IS ASSURED.**

[www.ecta.org](http://www.ecta.org)

# ECTA

European Communities Trade Mark Association

ECTA Bulletin June 2018

[www.ecta.org](http://www.ecta.org)