Summary of Juergen Brandstaetter's lecture at Alliott's EMEA Meeting in Prague, 10. May 2018

GDPR: Legal perspectives to be considered by lawyers, accountants and their clients

Austrian lawyer Juergen Brandstaetter (BMA) provides guidance for organisations on how to ensure they are GDPR compliant but also challenges the new rules in terms of the conflicts they present to lawyers and accountants in carrying out their everyday client business according to national laws.

A political perspective

From what I am seeing and reading, some in the political arena see the approach taken by GDPR as something of a socialist approach in that the view is being taken that each and every human being needs to be protected from the cradle to the grave.

Mismatch of priorities?

There is also a stark contrast with every business having to provide a register of beneficial ownership by 1st June 2018 – on the one hand, there is protection for the 'innocent consumer', yet on the other hand, the entrepreneur or business person, also a consumer, is having to reveal everything.

Fines for non-compliance also appear to be excessive – in a clever political move, the Austrian Government has for example, said that its National Data Protection Agency will not fine organisations for their first breach over the next 1-2 years, but instead will act as its service provider to those affected by the GDPR to mitigate the impact of the new regulation.

Damaging to organisations?

Rather than GDPR enabling a 'clean-up' of an organisation's data, in my view, GDPR will be damaging to many organisations that may have collected valuable data over the years.

What needs to be done and how practical is it?

In terms of what companies need to do, the first wall of defence should involve your website which may not currently be compliant with GDPR. In your privacy and cookie policies, you need to declare who at your organisation is responsible for the website, for collecting data, who can be contacted within your organisation, what you do with the data that is collected. You also need to explain how you use website analytics tools such as Google Analytics and what rights users have over the data you collect about them e.g. the right of erasure or correction. You also need to outline their right to file a complaint against you with your country's national data protection body.

As a recommendation, professional firms should build into their letter of engagement a section on data collection, data storage and data protection so that you secure explicit written consent when on-boarding the client to use his or her personal data. This letter needs to provide full details about how you will use their data and how long you will store it for.

I question however how carefully this has been considered and whether it presents a conflict of legal concepts for some businesses? Consider a law practice where lawyers are trained on the need to retain client files for a certain time period. Yet under GDPR rules, if a lawyer is required to delete much of this data, how can a proper conflict of interest check take place? The bigger the law firm, the bigger the problem is likely to be.

With regards to your current database of clients, emails can be sent out to inform recipients which data the organisation holds on them, asking them to check its accuracy and to click a button to explicitly give their consent for you to store their data for specific purposes (these need to be stated). One justification for keeping data is an 'overriding legal interest' – it will certainly be interesting to see how this is interpreted in practice!

Organisations also need to inform users to whom their data is transferred and where the data is stored. A specific contract with the third party storing the data needs to be in place to ensure data is secure, will not be passed on, etc.

Organisations are also required to let the user know if their data will be transferred to countries outside of the European Union as the standards of data protection afforded by countries outside the EU may be lower.

How long data will be stored for also needs to be explained clearly. Because GDPR rules provide for a principle of keeping as few data as possible for the shortest period of time. Again, this could constitute a problem. In all economically and legally developed countries, like all European countries, lawyers and accounting firms are required by law to retain client's financial data for several (in Austria seven) years. In my view, there is an overriding legal interest to keep the data, but this is not specified in the details of the GDPR.

Under GDPR rules, the user also needs to be informed of his or her rights e.g. to complain at the national level. Organisations need to be aware that fines could emanate from two sources - their national data protection body but also from a civil law suit seeking damages for a breach or misuse of data.

Lastly, anti-money laundering laws also present a conflict of interest with GDPR. It will be intriguing to see how this plays out with AML rules requiring firms to store data about their clients. We live in interesting times!