

18 February 2015

A Chief Data Officer is not a Data Protection Officer!

[UK](#) > [Knowledge & Insights](#) > [Insights](#) >

A Chief Data Officer is not a Data Protection Officer!

At the end of November 2014, I spoke at the [Chief Data Officer \(CDO\) Forum](#) in London. The forum included sixteen CDO presentations “*showcasing board level data management strategy*”, delivered by a variety of CDOs and other data experts from major financial institutions and corporates.

Data is widely seen today as being as one of the most valuable assets in business. Accordingly, many of the presentations, which were sophisticated and enlightening, explored the best methods of monetising data, involving its collection, analysis and targeted use. The overriding concern coming across from the Q&A and discussion sessions was the problem of low quality, inaccurate or outdated data.

I was asked to put the role of the CDO and the management and exploitation of data by organisations, into their legal context. My original intention was to focus on the sweeping reforms to data protection law which will apply around two years after the EU Data Protection Regulation (DPR) is finalised – the DPR “should” have been finalised by June this year, but serious differences both within the Council of Ministers – where different Member States are taking different positions – and between the European Parliament and the Council, are causing delay. This makes it more likely that we will have a final, agreed text in 2016.

Preliminary Issues: Education

Before looking at the chief effects of the DPR on CDOs, two issues in particular caught my attention.

The first issue was that although the Forum took it for granted that “CDO” stands for Chief Data Officer and this is part of the vernacular, a quick Google search for the meaning of this acronym shows that it is not yet true. Chief Data Officer does not even feature in the list of over 180 definitions of CDO in *acronymfinder.com* (although I have now submitted it as a suggestion), and comes well below an interesting and varied list, including *central dense overcast*, *chief dreaming officer*, *countertop deck oven*, *chronic duodenal obstruction* and even *come down Ollie*. Some education seems needed to ensure this changes, as the position of chief data officer increasingly becomes a senior executive position in most large

businesses.

The second issue was that a quick audience survey revealed nearly all CDOs present to be unfamiliar with the basic substance and detail of current EU data protection law. Looking at the changes to be brought about by the DPR is meaningless without a good understanding of existing law, because it takes that as its starting point and then enhances and amends it. If even CDOs, those with ultimate responsibility for data within major organisations, require basic education about data protection, then the same must surely be the case for all levels of management within businesses if we are to achieve effective compliance and resulting risk management.

This unfamiliarity with data protection law may be unsurprising, when the role of a CDO - as per most of the commercial presentations - is to ensure the commercial exploitation of data as an immensely valuable asset. But data protection is the corollary of data exploitation and faced with the proposal under the DPR that companies can be fined up to 5% of turnover, or €100m if higher, this is not something that can be left to chance

Key Effect of new European Data Protection Law: a CDO is not a Data Protection Officer!

An outstanding new feature of the DPR, and the most relevant for most CDOs, is the requirement under the current DPR proposal approved by the European Parliament that every organisation must [\[1\]](#) designate a *data protection officer* (DPO) if it has more than 5,000 data subjects in a 12 month period or its core activities require regular monitoring or processing of data in “special categories”, location data, or data on children or employees in large scale systems.

The obvious conclusion many people would draw from this requirement is that the CDO, the chief data officer, should or can be one and the same person as the DPO, the data protection officer, the person “*to be involved in all issues which relate to the protection of personal data*”.

Looking at the qualities required of a DPO, this would appear to make sense: the polymath abilities the DPR requires of this individual would certainly seem to merit that he or she holds at least a board position, if indeed such a special person can be found, given that a DPO must have **at least** the following qualifications: “extensive knowledge of substance and application of data protection law, including technical and organizational measures and procedures; **mastery** of technical requirements for privacy by design, privacy by default and data security; industry-specific knowledge in accordance with the size of the controller or processor and sensitivity of data to be processed; the ability to carry out inspections, consultation, documentation, and log file analysis and the ability to work with employee representation.”

With reference to my comments above, might this indeed be the opportunity and rationale for DPOs to become fully educated in data protection law?

However, on closer inspection, not only would it be inadvisable for a CDO to also play the role

of a DPO, it is actually impossible for them to do so, for the following reasons.

- The task of the DPO is essentially to raise awareness and advise the organisation of its data protection obligations and to ensure compliance. Any other professional duties must be compatible with this core task and must not result in a conflict of interest. Given that CDOs are likely to be under a competing commercial imperative to exploit personal data in the interest of their organisation's bottom line, it would seem impossible for such a conflict of interest to be avoided.
- DPOs must perform their duties and tasks independently and not receive any instruction as regards the exercise of their function – again, it is difficult to see how a board director or other senior executive within a chain of command could maintain this level of independence.
- DPOs must directly report to executive management – given that a CDO is likely to be part of executive management this reporting line seems inappropriate: in fact, a CDO would seem to be the appropriate executive manager for the purpose of this reporting, but as noted above, CDOs should not put any pressure on DPOs as to how they perform their tasks or as to any decisions they make regarding personal data.
- Employees appointed as DPOs must be designated as such for at least four years and can only be dismissed if they no longer fulfil the conditions required to perform their duties. Such restrictions are not appropriate for a board member or other executive manager.

In relation to data protection, the way forward for CDOs may then be relatively straightforward under the DPR. Appoint a highly skilled DPO and allow him or her to perform independently and without pressure. Nevertheless, given the reporting requirement and the effects of non-compliance, including massive fines and reputational damage, CDOs would still be well advised to themselves gain as full an understanding of data protection law as possible.

When it comes to the appointment, a DPO can either be employed or can fulfil his or her tasks under a contract for services. Although the “headline” cost of appointing an external contractor may be higher than paying the salary of an employee, this may be the preferred route; independence may be easier to establish and external contractors need only be appointed for two years, as compared to the minimum of four years for employees.

The message is clear: as data becomes increasingly valuable, data protection is becoming increasingly important and data protection laws are tightening; in this landscape the roles of CDO and DPO, which must not be confused and must remain separate, will inevitably become fundamental positions within all significant organisations.

[1] Although the Council of Ministers has recently suggested that Member States should have the ability to make this non-mandatory.

Key contact



Andrew Shindler

Partner

London

T +44 (0)20 7111 2638



Subscribe to Technology pICTure

Commentary on legal
developments in the
Technology sector.

You may also be interested in...



Legal services for your business



Telecommunic
ations, Media,
Entertainment
& Technology

Corporate,
Private Equity,
M&A and
Commercial