MACFARLANES

THE ROLE OF THE DATA PROTECTION OFFICER – FIVE THINGS YOU NEED TO KNOW

As programmes gather pace within organisations to meet the General Data Protection Regulation (GDPR) compliance deadline of May 2018 (and if you haven't started something, we would suggest that it would make a good New Year's resolution), some interesting questions start to emerge. One of these is the often thorny question of whether a formal Data Protection Officer (DPO) needs to be appointed, and how best to accommodate that role within an organisation.

The role has previously not always been considered to be a welcome addition to an existing workload, and is usually placed within the HR or legal teams. Data protection as a subject area has suffered from poor PR, and attendant lower levels of engagement amongst staff and management. The arrival of the GDPR is intended to change that, heralding a brave new dawn for data privacy amongst consumers, who are themselves now realising some of the more personal consequences of the wonders of modern technology.

1. When do I need to appoint a DPO?

Under the GDPR, you need to appoint a DPO in the private sector if your core activities consist of processing operations which requires the regular or systematic monitoring of data subjects on a large scale. There is no definition of "core activities" and whilst the precise wording identifies "the core activities", this should not be taken literally, and "any core activities" would be a more appropriate reading. You will also need to appoint a DPO if you undertake large scale processing of sensitive or criminally-related data.

2. Who should it be?

The DPO must have an "expert knowledge of data protection law and practice". Whilst there is no objective standard attached to this, doubtless employers will want to see some track record in the field. Given the relatively limited prior appetite for individuals to profess/confess to such knowledge, the size of the pool of those with genuine "expert knowledge" across the EU must be questionable.

Help is at hand here though, because as an employer, you will also have a statutory obligation to provide the "necessary resources" to perform the role and "maintain his/her expert knowledge". No distinction is drawn between employees and contractors, so you can outsource the role to a specialist third party provider, and still be required to pay for their continuing education. Surely an unintended consequence?

3. What must the DPO be able to do?

The DPO necessarily plays a key role in the assessment of a company's data processing operations. His/her core function is to ensure compliance with EU and local data privacy laws and regulations, acting as the organisation's conscience on the issues, raising awareness and providing training, and at the same time operating as the company's link with the regulator.

4. Can I share a DPO within a group?

Yes, and those companies need not be related in any way, provided that such an individual is "easily accessible" from each establishment. The reference to "access" is to the ease of contact rather than (we assume, within reason) geography. The opportunity for non-competing businesses to share a DPO is an attractive one to mitigate the impact of potentially increased headcount.

The appointee can be employed or contracted, but importantly, if that person has other functions to fulfil within the business, such other functions cannot cause a conflict of interest. Because of the risk-based approach which the GDPR adopts, the opportunity for conflicts to arise where judgement-calls need to be made might put those who exercise, for example, legal functions in an awkward position.

5. Does the DPO need to be independent?

An organisation is not allowed to direct the DPO in the performance of his/her duties, so much so that you cannot dismiss or penalise the DPO "for performing his tasks". We presume that this does not protect those who do the job badly, but the text of the law is certainly unfortunate. The DPO's reporting line must be directly to "the highest management level", so it is not obvious to see how such an individual has a day to day line manager for all other functions which might also include data protection matters. This reporting structure is the regulatory means of instilling the need for key stakeholders to take data privacy seriously, and to push this issue up the corporate agenda as far as all of the other competing compliance and regulatory issues.

CONCLUSION

Compliance with the GDPR will require organisations to undertake some quite material projects to log data capture and subsequent data flows. Once such projects are completed, in a world which is increasingly nervous about the risks of personal data loss, the DPO will play an important role in a company's operations, and accommodating the right individual in the structure whilst avoiding conflicts will require some judgement, especially where the organisation does not require a full-time DPO.

CONTACT DETAILS

If you would like further information or specific advice please contact:

RUPERT CASEY
PARTNER
COMMERCIAL
DD +44 (0)20 7849 2256
rupert.casey@macfarlanes.com

JANUARY 2017

MACFARLANES LLP
20 CURSITOR STREET LONDON EC4A 1LT

T +44 (0)20 7831 9222 F +44 (0)20 7831 9607 DX 138 Chancery Lane www.macfarlanes.com