Expert comment

Rob Corbet is a Partner at Arthur Cox and Member of the Examination Board for the Practitioner Certificate in Data Protection — the views expressed are his own

As was widely predicted, organisations are struggling to find the talent they need to support their GDPR compliance efforts. The issue is particularly stark for those who are required to appoint a Data Protection Officer ('DPO'), who must struggle to identify candidates who have the 'expert knowledge of data protection law and practices' required by Article 37(5), the capacity to be 'involved, properly and in a timely manner in all issues which relate to the protection of personal data' (Article 38(1)), and the good judgment to 'inform and advise' the controller under Article 39(1), including reporting 'directly to the highest management level' of the controller/processor as per Article 38(2). If you are a person with all of these qualities, you will know that you are currently in high demand.

Separately, Article 27 of the GDPR requires that organisations who have no establishments within the EU, but who are offering goods or services to persons within the EU (or who are monitoring behaviour of persons in the EU), must appoint a representative within the EU. This requires the relevant controller or processor to mandate the representative to be addressed by Data Protection Authorities or by data subjects 'on all issues related to the processing, for the purposes of ensuring compliance' with the GDPR. Article 27(5) provides that 'the designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves'. Hidden away in Recital 80 is the more stark statement that "the designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor".

The question arises as to whether or not DPOs and/or representatives will be personally liable for acts of non-compliance. There has been a lot of commentary to suggest that personal liability is a potential factor and, given the scale of potential sanctions and civil claims which might arise under the GDPR, this is undoubtedly contributing to the lack of candidates who are putting themselves forward to undertake these roles.

The difficulty is compounded by the fact that the GDPR exempts neither DPOs nor representatives from personal liability. If anything, Article 27(5) and Recital 80 almost seem to imply that the representative could be liable in addition to the relevant controller/processor who appointed him/her/it.

In the case of DPOs, the Article 29 Working Party guidance on DPOs which was revised in April 2017 provides comfort in that it baldy states that "DPOs are not personally responsible in case of non-compliance with the GDPR. The GDPR makes it clear that it is the controller or the processor who is required to ensure and to be able to demonstrate that the processing is performed in accordance with its provisions (Article 24(1)). Data protection compliance is a responsibility of the controller or the processor".

While this guidance is helpful, it is not legally binding. It is a shame that the GDPR text itself does not provide the same clarity.

So, let's take the case of Ireland – can DPOs or representatives be personally liable for non-compliance with the GDPR?

Criminal law

If we look to the criminal case law under the Data Protection Acts 1988 and 2003 ('DPAs'), it is clear that company directors can be prosecuted personally where an offence by a company can be attributed to either their neglect or complicity. For example, the Data Protection Commissioner ('DPC') successfully prosecuted Glen Collection Investments Limited and its director, Michael Ryan in 2016 and convictions were secured against both parties.

The law supporting this is in section 29 of the DPAs, but it is not limited only to directors and extends to prosecutions of 'a person, being a director, manager, secretary or other officer of that body corporate, or a person who was purporting to act in any such capacity'. This principle is expected to survive under the Data Protection Bill 2018 which carries over the equivalent of section 29(1) in section 144 of the Bill (as passed by the Seanad).

So, it seems to be reasonably clear that personal criminal liability can attach to a DPO (clearly an 'officer') if an offence is committed with their 'consent or connivance' or is 'attributable' to their neglect. Whether a representative would also be in scope is probably a little less clear-cut, given that the role of the representative

under the GDPR is far less involved than that of a DPO.

While this position is clearly causing concern among the community of potential and existing DPOs, it is important to note that, as is the case currently, criminal liability will only arise under the Data Protection Bill 2018 in very limited circumstances. For example, the existing offences of unauthorised disclosure of personal data are included in section 142 and 143 of the Bill, whilst section 128(7) carries forward the existing offences of obstructing/impeding DPC investigations. Existing offences of failing to comply with an Information Notice or an Enforcement Notice will also survive under the Bill. However, the vast majority of instances of non-compliance with the GDPR do not and will not constitute a criminal offence under Irish law.

So, while it would not be true to say that a DPO or a representative has any immunity from a criminal lawsuit, the circumstances in which a prosecution could arise are quite narrow, and the level of involvement of the person in the offence will be critical. Clearly, the DPC has only previously exercised the powers of personal prosecution where a particularly egregious breach of the DPAs was identified, and where there were one or two central persons who actively undertook the unlawful activity in question.

This has been the case more generally in Ireland — where directors' and officers' criminal liability is provided for frequently in statutes — so it is only in very rare cases that the Office of the Director of Public Prosecutions or other agencies with prosecutorial power have attempted to exercise those powers.

Civil liability

In relation to civil liability under the GDPR (whether to pay fines on foot of an order from the Data Protection Commissioner or to pay damages to an aggrieved data subject), while the Article 29 Working Party guidance is of some comfort to DPOs, it is a shame that there is not a greater level of legal certainty to assure those DPOs and representatives who dutifully attend to their roles that they will not have to defend any civil actions or sanctions procedures on a personal basis.

For representatives who agree to assist non-EU controllers or processors to meet their Article 27 obligations, careful consideration is required as to if and how the representatives will be indemnified for losses attributable to the acts of the controller/processor. On a practical level, one has to wonder if any such indemnities would be worthwhile in circumstances where a controller/processor walks away from its agreement with its representative, potentially leaving the representative "high and dry" to enforcement actions taken by reference to Article 27(5) and Recital 80.

Conclusion

The sanctions and civil liability regimes under the GDPR and the Data Protection Bill 2018 are undoubtedly driving corporate controllers and processors to raise their standards in relation to all aspects of personal data processing. Fines based on worldwide turnover were conceived of for this singular purpose. The additional governance requirements that are imposed in relation to DPOs and representatives also make sense in ensuring that there is an appropriate level of accountability within organisations for compliance, reflecting the risks and geographic locations attaching to their activity.

However, while it is clear that DPOs or representatives would only be joined in any criminal proceedings in Ireland in exceptional circumstances, there is a lack of certainty beyond that. This law of unintended consequences appears to be contributing to an already thin market for controllers and processors endeavouring to find candidates to fill these important roles.

Rob Corbet
Partner
Arthur Cox
rob.corbet@arthurcox.com