UK Court Ruling Limits Liability of Data Protection Representatives

Date : June 2, 2021

What's this all about?

In the case of Baldo Sansó Rondón v. LexisNexis Risk Solutions UK Ltd. the High Court in London, UK recently gave an important ruling about EU GDPR Data Protection Representatives and liability. This article looks at the issues.

Some data protection terms are used in this note which are explained at www.bit.ly/gdprwords.

The legal background

EU GDPR has extra-territorial scope as it covers non-EU-based data controllers or processors who offer goods and services to data subjects in the EU/EEA, or who monitor data subjects' behaviour in so far as that behaviour takes place within the EU/EEA. Organisations who fall within this extra-territorial scope have to designate, in writing, a Data Protection Representative (DPR) in the EU/EEA.

The appointment requirement is subject two exceptions: first, where the data processing is occasional, does not include large-scale processing of special category data or data relating to criminal convictions and offences, and is of low-risk to individuals' data protection rights – this exception is difficult to apply as there is a low threshold for "occasional" processing; or, second, where the controller or processor is a public body or authority.

A DPR can be either an individual, company or organisation, established in the EU/EEA, who, is designated by the controller or processor (in writing) and represents the controller or processer with regard to their respective obligations under EU GDPR. A single DPR can act for a number of non-EU controllers and processors. The DPR should be located in one of the EU/EEA countries where the data subjects whose data are being processed by the appointing organisation are located – local law and guidance should be checked for any possible additional specific requirements that may apply. If data subjects are located across a number of EU/EEA countries, the DPR must be easily accessible to data subjects wherever they are located.

The DPR's details should be included in the appointing organisation's (external) Privacy Policy. A DPR should be able to communicate in the language of the relevant data subjects and data protection authorities (DPAs). A data processor should act neither as a DPR for its own data controller, nor as the appointing organisation's Data Protection Officer (DPO).

EU GDPR sets out a DPA's specific obligations as being: to maintain a record of processing activities under the controller or processor's responsibility; and, to co-operate with a DPA (as requested by the DPA) in the performance of its tasks.

EU GDPR states that a DPR is to be addressed in addition to or instead of a data controller or processor by, in particular, DPAs and data subjects, on all issues related to processing, for the purposes of ensuring compliance with EU GDPR.

As regards the issue of liability/enforcement, EU GDPR Article 27(5) states as follows:

"[t]he 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."

EU GDPR does not prescribe the (written) terms of an appointment as such – consequently they may vary. Core issues that are likely to be to be covered (along with any of the more usual clauses) are as follows: the terms of the appointment; the respective obligations of the DPR and the appointer; liability, indemnities and insurance; payment (for the DPR services); and, confidentiality and compliance.

UK GDPR has mirror provisions requiring the appointment of DPRs in the UK. You can read about the post-Brexit GDPR position in the UK here https://www.corderycompliance.com/brexit-uk-vs-eu-gdpr-faqs/.

There can be consequences for the failure to appoint a DPR. We recently wrote about a €525,000 fine imposed for failure to appoint a DPR here https://www.corderycompliance.com/locatefamily-fined-by-ap/.

The factual background

The claimant is a businessman residing in Italy. World Compliance Inc. ("WorldCo") is a US company which owns and is the "data controller" of a database designed to help subscribing businesses globally to comply with laws combating money laundering and terrorism financing which includes millions of profiles of individuals. The claimant's profile was included in the database which the claimant was objecting to and in his claim he argued that that WorldCo had not respected his rights under EU GDPR. The defendant is a data analytics, risk intelligence and compliance business, incorporated in England and Wales, and is WorldCo's formally designated DPR (under EU GDPR).

The claimant issued a claim in August 2020 which set out a number of alleged breaches of EU GDPR in WorldCo's processing of his personal data in producing the profile to which he objected. The claimant also alleged that the defendant "is liable in respect of breaches of the GDPR for which World Compliance Inc. is liable as data controller".

The defendant applied for the claim to be either, struck out, or alternatively for summary judgment to be entered in its favour on the basis that, either, there were no reasonable grounds for bringing the claim, or alternatively the claim had no realistic prospect of success, because it had been brought against the wrong defendant as a DPR could not be held liable for the actions of a data controller (as the claimant was proposing) and the remedies sought could be obtained only from a controller, not its DPR.

What did the court decide?

After a very thorough and detailed analysis the judge concluded that there was no legal basis for the claim to be brought against the defendant, in its capacity as the DPR for WorldCo, and accordingly the claim was struck out. The judge made a number of important observations and conclusions about DPRs including the following:

- "At the least, the picture which emerges is of a considerably fuller role than a mere postbox 'to be addressed'. Even the language of 'conduit' or 'liaison' does not fully capture the job the GDPR gives to representatives. The role is an enriched one, active rather than passive. At its core is a bespoke suite of directly-imposed functions. These are crafted to fit together with, and belong in the triangle of, the relationships between controller, ICO and data subject. The job focuses on providing local transparency and availability to data subjects, and local regulatory co-operation. And the appointment is of course an opportunity for foreign controllers to give representatives any other ambassadorial - 'shop window' or customer-facing - functions, additional to the core 'mandate' functions, as they consider desirable demonstrations of their compliance credentials";
- "Standing in the controller's shoes for enforcement purposes implies [DPRs'] ability to provide, or require the controller to provide, remedies which involve direct access to and operations on the personal data themselves. That includes rectification and erasure of data, and giving subject access not just to ancillary information but to the actual data. That is nowhere discernibly provided for in the GDPR (or the [UK] 2018 Act). The GDPR neither expressly confers those functions on [DPRs] nor places them under anything like the duties controllers and processors – and data protection officers – are under, concomitant to their access to personal data";
- "It is not apparent that the GDPR envisages [DPRs] processing personal data themselves at all, whether directly or via contractual powers to compel controllers. 'Standing in the shoes' of controllers for enforcement and remedial purposes sounds like a simple proposition. It is not. The enforcement powers of the courts and the ICO mirror the full range of the duties of controllers and processors which are imposed because of the power they have on a day to day basis over how and why data are processed. A representative does not have that; it is not constituted as a controller or processor in its own right";

- “If the policy of the GDPR had been to require foreign controllers to appoint and establish local processors […] to access the data on the controller's behalf for the purposes of substantiating local liability, it could have done that. But [DPRs] are different from processors. The [DPRs’] 'mandate' bears no visible resemblance to the processor's contract […]. The core job the GDPR specifically gives [DPRs] has to do with (is 'related to') the activities of a controller or processor – processing personal data – but stops short of doing those activities and becoming one. How would it then deliver remedies requiring operating on (processing) personal data?”; and,
- If a [DPR] stands in the shoes of a controller, the package of duties the GDPR imposes directly on it is otiose. No visible difference need be made between the investigative and corrective powers of the ICO […] if both can be exercised against a [DPR]. A [DPR] need not be given special record-keeping responsibilities if it is liable to guarantee full transparency (information provision and subject access) rights in any event”; and,
- “What the GDPR does say about the liability of [DPRs] appears directed at excluding rather than emphasising it”.

Although the ICO did not formerly intervene in the court case it is worth noting that in response to a request from the defendant (who enclosed documents of the court proceedings) to the ICO to express an interpretative view about the issue at hand the ICO responded as follows:

“It is the view of the ICO that the role of [a DPR] of overseas data controllers and processors is limited to that of conduit of communications between the overseas entity and the ICO or relevant data subjects. Therefore the ICO is not seeking an interpretation of Article 27 [of EU GDPR] that allows [DPRs] to be held directly liable should a controller or processor they represent fail in their data protection obligations. An Article 27 [DPR] does not undertake any other business activity related to the processing of the controller or processor, other than acting as a contact point for data subjects and the ICO. From the point of view of the ICO, the existence of a [DPR] makes it easier to take action against a controller by acting as a conduit, but any enforcement action is directed against the controller itself.”

Key takeaways

This judgment is very clear that, at least according to the courts in England & Wales, a DPR is not directly liable should a data controller or processor they represent fail in their data protection obligations. This does not mean to say that a DPR carries no liability at all under EU GDPR – it does, but only with regard to *its* direct obligations under EU GDPR.

The judgment also indicates that a DPR is more than just a postbox, given the focus of the DPR role in providing local transparency and availability to data subjects, and local regulatory co-operation; that role can also be enlarged as agreed between a DPR and either a data controller or a processor if they so wish.

Organizations should consider the following:

1. Look at each of your corporate entities outside the EU to see if they are subject to EU GDPR. Remember that the need to appoint a DPR is for each entity subject to DPR so check group entities providing services to others (e.g. a US based entity providing payroll services to EU subsidiaries; an Indian entity providing back office systems handling EU customer data; a US entity providing a B2C ecommerce site for the group’s worldwide sales etc.);
2. Check the EU-UK aspects too – a DPR may need to be appointed in both the UK & the EU. Note that following Brexit there are similar obligations to appoint a DPR in the UK. As yet there is no reciprocity between the EU and UK regimes, so, currently: a UK-based organisation may need to appoint a DPR in the EU; an EU-based organisation may need to appoint a DPR in the UK; and, a US-based organisation may need to appoint a DPR in the EU and the UK. There’s a more detailed explanation of GDPR after Brexit in our FAQs and film here https://bit.ly/brexdpfaq;
3. Determine who the best DPR might be for your organisation. That could be another entity in your group or an outside DPR. Exercise caution however as some organisations advertising DPR services may not be appropriate. You’ll need to do due diligence on any outside agency you use;

4. Make sure you appoint a DPR in writing complying with the formalities of EU and/or UK GDPR – amongst other issues, carefully consider the aspects concerning liability, indemnities and insurance. It is important to get the written agreement right as you may need to produce this to a DPA or court;
5. Make sure you've also checked other requirements including the possible need to register with and pay a fee to the UK ICO if there's a UK involvement (see here https://www.corderycompliance.com/solutions/privacy-registration-and-renewal/); and,
6. Make sure you have a proper plan in place with the DPR to enable you to react quickly to concerns and reach out to DPAs when necessary to alert them to issues.

There is more information about this type of issue and other data protection topics in Cordery's GDPR Navigator subscription service. GDPR Navigator includes short films, straightforward guidance, checklists and monthly conference calls to help you comply. More details are at www.bit.ly/gdprnav.

Further Information

We write about data protection issues here https://www.corderycompliance.com/category/data-protection-privacy/.

You can read the court's full decision here https://www.bailii.org/ew/cases/EWHC/QB/2021/1427.html

For more information please contact Jonathan Armstrong or André Bywater who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd
Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com