Client Alert: Ireland's Data Protection Authority Halts Facebook Dating Service

Date : February 13, 2020

Yesterday Ireland's Data Protection Commission (DPC) confirmed that it had visited Facebook's premises in Ireland over concerns about the data protection aspects of Facebook's planned new dating service. This is the most high profile 'dawn raid' under GDPR to date and has led to the postponement of Facebook's planned launch tomorrow.

What is this about?

According to the DPC, Facebook told it on 3 February 2020 that it planned to launch a dating service on 14 February 2020. Under GDPR, in some circumstances, data protection authorities (DPAs) have the right to be consulted before processing takes place. They can ask to see a Data Protection Impact Assessment (DPIA). The DPC said that their initial concerns were "further compounded by the fact that no information/documentation was provided to us on 3 February in relation to the Data Protection Impact Assessment or the decision-making processes that were undertaken by Facebook". As a result the DPC went to Facebook's offices on 10 February 2020 and gathered documentation for their investigation.

Do DPAs have dawn raid powers?

Essentially yes.

They're not called dawn raids under GDPR but GDPR doesn't just give DPAs the power to fine. GDPR Article 58 gives DPAs a host of other powers including:

1. to order the controller, processor or Data Protection Representative to provide any information it requires for the performance of its tasks;
2. to carry out data protection audits;
3. to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
4. to obtain access to any premises of the controller and the processor, including to any data processing equipment and means (this can include equipment like servers);
5. to order the controller or processor to bring processing operations into compliance with the provisions of GDPR;
6. to impose a temporary or permanent ban on processing.

What is a DPIA?

DPIAs are one of the key elements of GDPR. They help organisations assess risk and deal with it in a proportionate way. The DPIA process is not new – the UK DPA issued their first guidance on Privacy Impact Assessments in 2007, but DPIAs received statutory footing under GDPR and are mandatory in some cases.

Is there any guidance on DPIAs?

Yes.

In August 2018, the European Data Protection Board (EDPB) published a short guide to DPIAs. That follows earlier regulatory guidance. In October 2017, the Article 29 Working Party (WP29) published guidelines on the DPIA process. We summarised that guidance here http://www.corderycompliance.com/client-alert-new-dpia-guidance-issued/. These guidelines were endorsed by the EDPB in Endorsement 1/2018 on 25 May 2018. Some DPAs have also issued their own guidance following the WP29 guidance – for example the ICO's guidance in the UK is summarised here http://www.corderycompliance.com/client-alert-uk-data-protection-regulator-publishes-new-

guidance-on-data-protection-impact-assessments/. There's an explanation of the role of the EDPB and the historical role of WP29 in our data protection glossary here www.bit.ly/gdprwords

When should a DPIA be carried out?

It is usually best to begin the DPIA process at the start of a project. If you do that you are more likely to be able to put remedial measures in place to deal with risk more easily and more cost-effectively. If you need to consult with a regulator, that process can take 4-5 months – this might be another reason for starting early. There are no set time limits on consultation with a DPA where that is necessary or desirable but it is now obvious (if it wasn't already) that 10 days notice is unlikely to be enough.

The EDPB guidance says:

"DPIAs must be carried out prior to any processing taking place and every time a new form of processing takes place or the processing is significantly updated. The process should be started as early as possible and undertaken as part of the design of the processing operation, even if some of the processing operations are still unknown."

An earlier draft of the WP29 guidance suggested that existing processes should be reviewed by 24 May 2021, i.e. within three years of the coming into force of GDPR. The final draft of the WP29 guidance does not include the three year rule, although some DPAs, including the DPC in Ireland, have suggested that it may still apply the three year rule.

DPIAs as a mitigating or aggravating factor

DPIAs are important not only because they reduce risk, but also because proper engagement with a DPIA process is likely to be a mitigating or aggregating factor in any penalty. As the EDPB note says:

"However, whatever its form, a DPIA must be a genuine assessment of risks, made by the controller and, in doing so, allow him or her to take the necessary measures to address them. This will result in greater trust and confidence of data subjects, which could in turn result in greater competitive advantage. On the other hand, an incomplete or poorly conducted DPIA could be a factor in a later sanction decision, or possibly result directly in a sanction imposed."

It is important to remember that a DPA has the power to order a DPIA exercise be completed. The ICO's enforcement action in the Royal Free case with Google DeepMind is an example of that in action pre-GDPR – https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/

Importance of training

From our experience, DPIAs are the aspect of GDPR that organisations (and their employees) struggle to get their heads around. With proper training however, the process can become second-nature and materially reduce an organisation's risk.

What is the significance of these developments?

The step up in enforcement activity comes at a time when many are concerned about new technological developments including AI, surveillance and facial recognition. New technologies like this almost always need a DPIA. It takes some skill to do a DPIA for something cutting-edge but that isn't an excuse for not trying. The raid is significant as it may signal a get-tough era on enforcement in Ireland which has been criticised as being too slow to investigate. This is a special concern given that so many large technology operations have the DPC as their lead regulator under GDPR. The DPC has been under pressure as a result with some DPAs considering their own enforcement action against these tech giants, as was the case with the CNIL's fine against Google last year https://www.corderycompliance.com/french-data-protection-authority-fines-google-e50m-for-violations/.

On a lighter note as a result of the raid, those seeking a date on Valentine's Day tomorrow might need to try real-life socialising instead!

More information

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

Cordery has helped organisations large and small with DPIA tools, templates and training.

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 4HHOffice: +44 (0)20 7075 1784
jonathan.armstrong@corderycompliance.com

Andre Bywater
Cordery
Lexis House
30 Farringdon Street
London EC4A 4HHOffice: +44 (0)20 7075 1785
andre.bywater@corderycompliance.com