Irish Regulator's Decision on GDPR Rights Identity Proof Requirements

Date : March 16, 2021

Introduction

In a case that came out towards the end of 2020, the Irish Data Protection Commissioner made an official ruling that the organisation Groupon International Limited (an E-Commerce platform service provider) had infringed EU GDPR in a number of ways by requiring an individual to verify their identity by submitting a copy of a national ID document in circumstances where a less data-driven solution to the question of identity verification (in this case confirmation of email address) was available to Groupon. This article sets out the highlights of the case.

What's the case about? Applicable rules

Under EU GDPR processing personal data is only lawful in a set list of EU GDPR circumstances.

Under the so-called 'data minimisation' principle of EU GDPR 'personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"'.

Under the EU GDPR Right To Be Forgotten, an individual has 'the right to obtain from [a] data controller the erasure of personal data concerning [the individual] without undue delay and the controller shall have the obligation to erase personal data without undue delay' (subject to a number of exemptions) in accordance with a set list of EU GDPR circumstances, including where 'the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed'.

As regards individuals exercising their EU GDPR rights and the issue of proof of identity, under EU GDPR: a data '[…] controller shall facilitate the exercise of data subject rights […]' and a '[…] controller shall not refuse to act on the request of the data subject for exercising his or her rights […] unless the controller demonstrates that it is not in a position to identify the data subject'; and, "[…] where the controller has reasonable doubts concerning the identity of the natural person making the request […] the controller may request the provision of additional information necessary to confirm the identity of the data subject".

What's the case about? The factual background

The Irish Data Protection Commission (the DPC) is the so-called "Lead Supervisory Authority" under EU GDPR for Groupon International Limited ("Groupon"). Acting in that capacity the DPC dealt with a 2018 complaint that originally went to the Polish Data Protection Authority; the complaint was dated 26 May 2018, i.e. the day after EU GDPR came fully into effect!

The complaint was about Groupon's practice at the time of the complaint which required individuals to verify their identity with an electronic copy of a national identity card when individuals made certain requests, including requests for erasure of personal data (the Right To Be Forgotten); the requirement did not however apply when individuals created a Groupon account.

What did the regulator decide?

The DPC decided in this particular case that:

- Groupon's requirement that the complainant verify his identity by way of submission of a copy of a national ID document was an infringement of the EU GDPR principle of 'data minimisation'. The infringement occurred in circumstances where no such requirement for ID was in place at the time an individual opened a Groupon account, and a less data-driven solution to the question of identity verification (in this case confirmation of email address) was available to Groupon;

- The infringement continued from 25 May 2018, when EU GDPR came into effect, until 8 October 2018, when Groupon amended its privacy policy and discontinued its requirement for requesting data subjects to verify their identity by way of submission of a copy of a national ID document;
- Groupon also infringed EU GDPR by requesting additional information as to the complainant's identity at the time he made his request for erasure in circumstances where Groupon had not demonstrated that reasonable doubts existed concerning the complainant's identity that would have necessitated Groupon requesting the provision of additional information necessary to confirm the identity of the complainant;
- Groupon also infringed the EU GDPR Right To Be Forgotten ground allowing for the erasure of personal data where 'the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed' when Groupon failed to comply with the complainant's erasure request because the circumstances were such that Groupon's requirement that the complainant submit a copy of a national ID document was not in compliance with EU GDPR; and,
- Groupon also infringed the EU GDPR 'lawfulness of processing' obligation because, after it received the complainant's erasure request, Groupon continued to process the complainant's personal data without a lawful basis.

The DPC noted that Groupon had however taken certain remedial measures: concerning the principle of 'data minimisation' Groupon had discontinued its practice of requiring an individual to submit a copy national ID document when making a request to Groupon in order to verify their identity – instead, Groupon verifies an individual's identity by way of the individual confirming their email address, and Groupon had also updated its privacy policy to reflect this change.

In respect of the complainant's request for erasure of personal data, the DPC also noted that Groupon had in fact erased the complainant's personal data, although Groupon hadn't acted on the initial request for erasure (made on 26 May 2018) but on the basis of a second erasure request (made in July 2019).

The DPC concluded by issuing a formal reprimand (but not a fine) to Groupon for the EU GDPR infringements committed; a formal reprimand is a sanction available under Article 58(2)(b) of EU GDPR.

What are the takeaways?

Does this decision weaken the requirement of proof of ID when someone exercises either an EU GDPR or a UK GDPR right? No, requiring proof of identity remains an important compliance check – the key thing is getting it right according to the particular circumstances. Personal data can't be sent to the wrong person – this would constitute a data breach; the risk of fraudulent/deceptive requests is also a real one.

As the UK ICO's (revised) guidance on Subject Access Requests (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/what-should-we-consider-when-responding-to-a-request/, which we have written about here: https://www.corderycompliance.com/sars-under-gdpr/) says:

'You can ask for enough information to judge whether the requester […] is the person that the data is about. The key point is that you must be reasonable and proportionate about what you ask for. You should also not request formal identification documents unless necessary. First you should think about other reasonable and proportionate ways you can verify an individual's identity. You may already have verification measures in place which you can use, for example a username and password. However, you should not assume that on every occasion the requester is who they say they are. In some cases, it is reasonable to ask the requester to verify their identity before sending them information. The level of checks you make may depend on the possible harm and distress that inappropriate disclosure of the information could cause to the individual concerned.'

When dealing with either an EU GDPR or a UK GDPR data subject rights request, making an identity check clearly therefore has to be determined and handled on a case-by-case basis.

Is there anything that I can do in practical terms?

Organisations can consider doing the following:

- Reviewing data subject rights policies and procedures to make sure that they are up to the job – for many organisations the main focus is likely to be on how they handle Subject Access & Right To Be Forgotten Requests. Make sure that it is clear as regards: what the ID verification process is; what information has to be provided; and, whether any exemptions are covered;
- Ensuring that there are systems in place that can locate personal data when Subject Access & Right To Be Forgotten Requests are made, especially from an IT perspective (and don't forget the hard copy data!);
- Looking at document creation and retention – in particular ask whether all that data really needs to kept! The more that is kept the bigger the job and amount of resources that will be needed when responding to Subject Access & Right To Be Forgotten Requests. The appropriateness of large amounts of HR data should be reviewed especially in light of the large fine for H&M (which we've written about here: https://bit.ly/hamburgfine); and,
- Train staff on spotting and handling Subject Access & Right To Be Forgotten Requests, especially the former which are not always obvious.

Cordery's Breach Navigator tool helps organisations manage data incidents and make the right decisions on risk and reporting requirements – for more information please see here: https://www.corderycompliance.com/solutions/breach-navigator/.

Cordery's GDPR Navigator includes resources to help deal with data protection compliance including guidance on handling Subject Access Requests; a template policy, guidance notes and films to use in training are all part of this – for more information please see here: https://www.corderycompliance.com/solutions/cordery-gdpr-navigator/.

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

The Irish regulator's decision can be found here: https://www.dataprotection.ie/en/dpc-guidance/law/decisions/groupon-december-2020.

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

André Bywater

Office: +44 (0)207 075 1785

andre.bywater@corderycompliance.com

Jonathan Armstrong

Office: +44 (0)207 075 1784

jonathan.armstrong@corderycompliance.com