Cyber and Information Law Newsletter: Issue 1 - Enforcement

Published 30 April 2019

French data protection regulator fines Google 50 million euros for GDPR breaches

On 21 January 2019 the data protection regulator in France (Commission Nationale de l'Informatique et des libertés, known as the "**CNIL**") imposed the first large GDPR fine: a record breaking 50 million euros (approximately £44 million) against Google LLC. This caused headlines not only because of its size, but also because of the breaches in the spotlight.

The actions arose out of complaints initiated by privacy interest groups "None Of Your Business" and "La Quadrature du Net".

Articles 12 and 13 transparency and information obligations

The CNIL found that Google had not been transparent with Android users about how it collected and used personal data. Its fair processing notice was not accessible, it displayed information spread across many applications and webpages, it did not contain all required elements, and the general form and structure was non-compliant. This meant that users could not understand how personal data would be processed by Google or what the consequences of processing might be.

The CNIL drew particular attention to the number of Google services collecting personal data on the Android system (approximately 20 including phone, Gmail, YouTube, Google Maps, and Google Analytics cookies on third-party websites) and to the vagueness of the information Google gave regarding how data would be used, citing generic purposes such as to "*ensure the safety of products and services*".

Article 6 – lawfulness of processing

Google relied on consent as its legal basis for processing personal data for ad personalisation. It told Android users that "*Google can show you ads based on your activity in Google services (for example, Google search or YouTube, as well as on Google's websites and partner applications*)". However it was not possible for users to see which applications, sites, and services were involved. When creating an account the ad personalisation options were pre-ticked and the user was required to tick the boxes: "*I agree to Google's Terms of Service*" and "*I agree to the processing of my information as described above and further explained in the Privacy Policy*". This meant that the user provided his or her blanket consent for all of the processing purposes that relied on consent (including for speech recognition) and the user could not choose whether to give or withhold consent for a particular purpose.

Therefore the CNIL found that consent had not been properly obtained because it did not meet the GDPR standard of being "specific" and "unambiguous". Additionally in view of the fact that Google was in violation of its transparency requirements, the CNIL also found that consent was not "informed".

The One Stop Shop

The GDPR introduced the concept of the "one stop shop"; a mechanism to allow a single supervisory authority to act as the lead authority on behalf of other EU supervisory authorities and issue fines. Google argued that its European headquarters were in Ireland and therefore the Irish Data Protection Commissioner (rather than the CNIL) should have handled this complaint. However, the CNIL found that Google did not have a main establishment in the EU; its key decision making and processing activities under investigation were not made by the Irish entity. This meant that the "one stop shop" was not engaged and the CNIL, along with any other supervisory authority, could make a decision in respect of Google's activities. the ICO is said to be considering its possible next steps.

Google has confirmed that it will appeal the CNIL's decision.

What can we learn from the Google fine?

This fine demonstrates that supervisory authorities are not afraid of flexing their enforcement and fining powers.

It is also indicative of a new enforcement trend across which is no longer focussed just on security and data breaches, but instead looks at the lawful use of personal data. We expect that a new wave of enforcement activity focussed on

transparency and consent infringements will follow the Google fine. We recommend that all organisations review their fair processing notices (including delivery mechanisms) and consent wordings to ensure that meet the high standards set by the GDPR.

The CNIL fine press release and notice against Google (in French) can be accessed here.

Authors

Jade Kowalski

Shehana Cameron-Perera

Enforcement action

In each edition, we intend to provide a brief round up of notifiable enforcement action taken by the ICO. Firstly we turn to a prosecution taken by the ICO which is of interest due to the impending appeal of the Morrisons Supermarket case.

Employee of Nuneaton and Bedworth District Council prosecuted for passing on personal information of job applicants

Kevin Bunsell, who was Head of Building Control at Nuneaton and Bedworth District Council has been sentenced at Nuneaton Magistrates' Court to a fine of £660 (plus costs of £713.75 and a victim surcharge of £66) for passing the recruitment packs of job applicants on to his partner's Hotmail address. At the time, his partner was applying for an administrative position at the council and the recruitment packs belonged to rival candidates. He was not part of the recruitment process on this occasion. He nonetheless accessed the council's recruitment system to get hold of the packs which included the candidates' names, addresses, telephone numbers, and CVs as well as contact details for their referees.

You will recall the Morrisons Supermarket case, which has already been heard in the Court of Appeal and is awaiting appeal to the Supreme Court. The background was that Andrew Skelton, a senior IT internal auditor employed by Morrisons, posted a file containing the personal details of 99,998 employees onto a file sharing website. The data included the name, address, gender, date of birth, phone numbers, national insurance number, bank account number, sort code, and salary of each employee. He then sent copies of a CD containing the same data to three newspapers, none of which published it. One newspaper alerted Morrisons to the data leak and within hours the website was taken down. Mr Skelton was sentenced to eight years' imprisonment in the prosecution brought by the ICO.

In the action brought by the affected employees, it was found there was a sufficient connection between the position Mr Skelton held and his wrongful conduct for Morrisons to be held vicariously liable. The judgment in Morrisons makes it clear that the employee's motive is irrelevant; an employer can be vicariously liable for deliberate wrongdoing by an employee.

In this case, so far only Mr Bunsell has been prosecuted. Following Morrisons, it seems likely that those employees who were affected by the data breach will have grounds to bring a claim against Nuneaton and Bedworth District Council under vicarious liability. Whether those grounds remain solid will depend on the outcome of Morrisons' appeal to the Supreme Court.

Meanwhile, the ICO continues to focus on DSARS and marketing calls and emails. Magnacrest Limited has received a nominal fine of £300 for failing to comply with an Enforcement notice in relation to a DSAR. Leave.EU Group has received two fines (£45,000 and £15, 000), and Eldon Insurance Services Limited has been fined £60,000, for sending direct marketing emails without consent. Alistair Green Legal Services Limited has been fined £80,000 for making nuisance calls to subscribers.

The ICO has issued assessment notices to Leave.EU and Eldon Insurance Services Limited, and will now carry out an audit of their offices which will include reviewing their data protection practices and interviewing staff. The audit findings will be made public.

Investigations by the ICO into nuisance marketing have resulted in 16 company directors being banned from running a company for more than 100 years in total. The ICO has reached this key milestone by working in partnership with the Insolvency Service, referring evidence which can result in company directors being disqualified for up to 15 years. The PECR (Amendment) Regulations 2018 have the effect that the ICO now has powers to make company directors and other company officers (including the secretary, members and managers) personally liable for the fines imposed for illegal marketing. Individuals will no longer be able to hide behind the "corporate veil" by dissolving the company to avoid paying the fine, often called "Phoenixing".

Authors

Jade Kowalski

London - Walbrook
+44(0)20 7894 6744
jkowalski@dacbeachcroft.com

DAC BEACHCROFT