

WHAT IS ADEQUATE NOTIFICATION UNDER ARTICLE 14 OF THE GDPR?

Jessica Copeland, Daniel Carosa
Hodgson Russ Cybersecurity & Privacy Alert
April 30, 2019

Nearly one year since the GDPR came into effect, companies are still grappling with its provisions. Of primary concern is whether the GDPR applies to their organization. If it does, organizations need to establish risk management strategies in order to avoid or minimize the penalties that can be levied for noncompliance. The cost and effort required to be GDPR compliant as compared to the potential fine assessment are important considerations. Unfortunately, it is the early fine recipients who continue to enlighten us and provide a better understanding of each Article found to have been violated under the GDPR, as well as the true calculation of fines assessed.

Most recently, the Polish Data Protection Authority (UODO) imposed its first fine for violation of the GDPR against the Swedish data aggregation company Bisnode for approximately €220,000. The fine was assessed for violation of Article 14 of the GDPR which addresses the failure to provide adequate notice to data subjects for how their data was being collected and processed by the data aggregation company.

The GDPR, which came into effect in the European Union on May 25, 2018, creates an obligation on organizations to inform individuals whose personal data they intend to process if the organizations did not obtain the personal data from the individuals directly. Under the GDPR, personal data includes information related to an identified or identifiable natural person, including personal names, identification numbers, location data, and more. Data aggregation organizations often obtain this data by scraping social media websites or other publicly available databases.

Under Article 14, data aggregation organizations must notify data subjects of the following: (1) who has their data, (2) what types of data have been obtained, (3) how the data will be used, and (4) how long the data will be retained. These organizations must also inform the data subjects about how to object to the collection and processing of their data if they wish to do so.

Article 14 contains two exemptions from this notification requirement: (1) if “the provision of such information proves impossible or would involve disproportionate effort;” and (2) if the notification requirement “is likely to render impossible or seriously impair the achievement of the objectives of that processing.” So what does “disproportionate effort” actually mean? Bisnode found out the hard way...

Attorneys

Jane Bello Burke
William Ciszewski III
Alfonzo Cutaia
Reetuparna Dutta
Michael Flanagan
Michelle Merola
R. Kent Roberts
Gary Schober
Amy Walters

Practices & Industries

Cybersecurity & Privacy

WHAT IS ADEQUATE NOTIFICATION UNDER ARTICLE 14 OF THE GDPR?

Bisnode obtained an array of personal data of millions of business owners and entrepreneurs from public registers and public databases. In its effort to comply with the GDPR, for the approximately 700,000 individuals whose records included an e-mail address, Bisnode sent out e-mails informing those individuals of the use of their personal data and their right to object under the GDPR. Of those 700,000 individuals, approximately 12,000 objected to the use of their data. However, the records of over 6 million individuals did not include an e-mail address, only mobile phone numbers and postal addresses. Bisnode did not notify those individuals via SMS or postal mail, but instead simply posted a notice on their website. Bisnode claimed they were exempt from notifying the over 6 million individuals, as the costs of notification via SMS or postal mail would have been “disproportionate.” Bisnode estimated the postal costs alone as around €7.7 million, which would exceed their 2018 profits. This estimate did not include internal staffing and resource costs to facilitate the notification process.

Regardless, the UODO ruled Bisnode had failed to meet its obligations under GDPR Article 14. In its ruling, the UODO found that contacting the over 6 million individuals without an e-mail address would not be impossible or involve disproportionate effort.

Notably, the UODO based its determination, in part, on the fact that the high number of objections of notified individuals demonstrated the importance of the notification requirement.

The UODO further stated that the €220,000 fine was set at a high level to act as a deterrent, rather than simply a cost of doing business.

Accordingly, any organization which is collecting or processing personal data of EU residents from a source other than those same residents (with permission of course) **must** notify them. More significantly, the notification **must** provide the affected data subjects with the means to object to the use of their data. If the individuals do not have a known e-mail address, notification by phone or postal mail appears to be required. Further, the postal or administrative costs of such notification **do not** trigger an exemption of this notification requirement. Organizations engaged in data scraping face significant challenges to satisfy the notification requirement, and will be exposed to significant penalty if notification is deemed inadequate.

Is your organization in compliance with Article 14 of the GDPR?

If you received this alert from a third party or from visiting our website, and would like to be added to our Cybersecurity & Privacy mailing list or any other of our mailing lists, please visit us at: <https://forms.hodgsonruss.net/sign-up-for-email-and-other-communications.html>.