Bernold Nieuwesteeg

The Dutch DPA adding fuel to the fire

Brussels and the Dutch Council of State recently blew the whistle on the practices of the Dutch Data Protection Authority (hereafter: Dutch DPA). According to the European Commission and the Dutch Council of State, the Dutch DPA interpreted privacy legislation too strictly. It concerned a concrete case in which the Dutch DPA launched against Voetbal TV, a broadcast company for amateur football games. Voetbal TV went bankrupt after the imposition of the fine by the Dutch DPA.

We could see this case coming for a long time. It confirms that the Dutch DPA is not executing privacy legislation, but instead sits on the chair of the legislator and chair of the judge. For years, the Dutch DPA, led by Aleid Wolfsen, has been drawing its own dogmatic plan and diverts from other European data protection authorities. This results in large social costs, which I will illustrate in three examples:

First, the Dutch DPA does not disclose data breaches for scientific research. The data breaches that have to be notified by organizations that suffered from a data breach remain in a digital drawer and nobody can learn from them. In 2018, I performed scientific research, together with the TU-Delft, in which we assessed that there are hardly any disadvantages in making this dataset public, and numerous advantages. In 2020, even the Dutch Cyber Security Council advised in favor of making it public. But nothing happened so far.

"The high fines and arbitrary allocation of these fines results in high compliance costs."

Second, the Dutch DPA sets (because of its strict activist approach to the law) the notification threshold for data breaches far too low, which leads to a 'tsunami' of notifications made by Dutch organizations. In the Netherlands, there were a total of 24866 data breach notifications in 2021. In Belgium this was only 1529. Earlier I warned together with prof. Michael Faure about this 'notification fatigue' in a peer reviewed article in the journal Computer Law & Security Review. We concluded that there are also social costs of data breach disclosure: "First, individuals and organizations whose data have been breached incur direct costs because they have to spend time and money in order to analyze and mitigate their impact. This might be a minor cost per record, but if hundreds of thousands of records are being breached, the numbers quickly add up. The cost of consumer actions might be greater than expected because consumers can spend several hours of time on their accounts and impose costs on firms by requesting more information on, for instance, new credit cards. Lenard and Rubin estimate that this cost is $10 per data subject. Second, an increase in the amount of notifications can lead to a

decrease in the positive effects of disclosure, because data subjects can pay less attention to each individual data breach. Subsequently, the information diffusion becomes less meaningful and eventually all data breaches could just be perceived as irrelevant information."

In other words, notification fatigue does not only affect minor data breaches, but also has negative effects towards other bigger data breaches. All data breaches become less important when additional data breaches are introduced. Likewise, as soon as more notifications are being made, for example because a single DPA is behaving differently than their counterpart DPAs in other member states, the benefits of the additional data breach will decrease and the costs to the system will increase.

Third, the Dutch DPA is creating a compliance culture. The Dutch DPA threatens Dutch organizations regularly with imposing high fines. It also imposes these fines arbitrarily: many organizations are formally violating the GDPR but only a few are fined. The high fines and arbitrary allocation of these fines results in high compliance costs. The Dutch DPA is adding fuel to the fire by even interpreting the GDPR more strictly than its partner DPAs in member states. This results in a situation where organizations are more concerned with being compliant than actually taking measures that improve privacy and security.

Personally, I applaud that Brussels and the Council of State now say: up to here and no further. The Dutch government should start a serious conversation with the Dutch DPA about their current practices. These practices should be revised in order to be more in sync with other DPAs in Europe.

About the author
Bernold is director of the Centre for the Law and Economics of Cyber Security at Erasmus University and entrepreneur. He recently founded www.cybersecuritybooster.nl, a webinar series that boosts cybersecurity knowledge.