Bernold Nieuwesteeg

The GDPR lottery

The Netherlands is a country of cyclists, of which many are driving without lights in these dark days. They are well protected by the law in terms of liability when it comes to a collision. However, they are not protected by their bicycles against the unforgivable steel of a big car. That is why our government enforces the legal requirement to ride your bicycle with proper lights. You may have experienced the fine of riding without light of 55 Euro yourself.

But allow me to take you into a hypothetical thought experiment. Imagine that the fine to cycle without lights is 10,000 Euro. And imagine that, after writing the ticket, the very policeman that fined you drives away in his fancy police car with malfunctioning lights! And on top of that, the only offender that gets fined is you.

Welcome to the illustrious dynamics of compliance in the world of the GDPR, now almost two years into force. In the world of the GDPR, the government that enforces

"Businesses also overestimate to 'win' the GDPR 20 million Euro fine lottery."

and fines you as a business, violates the very regulation it aims to fine. For instance, many Dutch municipalities still have such a poor data security policy and practices.

In the world of the GDPR, we know that fines can be very high and the allocation of the fine can be arbitrary. In other words, many organisations are formally violating the GDPR but only a few are fined. Arguably, the GDPR regime could be compared to a lottery where some businesses get the 'prize' and others do not. For instance, British Airways is now facing a record fine of 183 million Great British Pounds for last year's breach of its security systems, while many others did not get fines or warnings.

The high fines and arguably arbitrary allocation of these fines results in high compliance costs. We know from behavioural economics that people tend to overestimate the likelihood of winning the lottery. That is why people buy lottery tickets. Likewise, businesses also overestimate to 'win' the GDPR 20 million Euro fine lottery. That is the exact reason why so many businesses hire legal experts to mitigate the risk and increase the likelihood of compliance. We do not have the exact figures, but from the entry into force of the GDPR in May 2018 onwards, there has been an unprecedented growth in the number of GDPR legal advice companies. These companies might have won the real lottery.

Does this desire for compliance result in clear goals and actions? No, because the GDPR is quite vague. Ask ten legal advisors for interpretation of a clause of the GDPR and you possibly will get ten different answers. Consider for instance the data breach notification obligation, as incorporated in Articles 33 and 34 of the GDPR. The data breach notification obligation imposes an obligation on organizations to disclose certain breaches of personal data to a notification authority and to affected individuals. Only breaches that have a likelihood to impact the rights and freedoms of individuals have to be notified. The question quite naturally arises when an organisation has to notify a data breach. It is striking that the European Data Protection Board, which provides examples when or when not to notify in its Guidelines on Personal data breach notification, states that the examples they give depend 'on the scope and type of personal data involved and the severity of possible consequences'. So even the examples by the lawmaker itself do not give the clarity which is so desired.

Hence, there is a regulation with very high fines, which are imposed quite randomly. Compliance with this regulation is hard because of its vagueness. Nonetheless, the value of a sensible cyber security and privacy strategy should not be underestimated. However, currently, the GDPR has increased transaction and compliance costs on businesses, while the impact of the regulation on real world security and privacy is questionable.

Businesses would be better off by studying the societal goals of the regulation rather than drowning into the details, and could focus on reasonable levels of cyber security and data protection rather than purely complying with the GDPR in fear of high penalties. Legislation needs legitimacy in order to function. A lot of hard work is needed for the mistiness of compliance with the GDPR to move away.

The Centre for the Law and Economics of Cyber Security (CLECS) offers an executive master at the Erasmus School of Law in The Netherlands. For more information, please visit: https://www.executivemasters.nl/leergangen/cybersecurity/

About the author
Bernold Nieuwesteeg is director of the Centre for the Law and Economics of Cyber Security at Erasmus University and partner at CrossOver. He regularly advises public and private actors on their cyber security strategy and studies methods to increase knowledge about sensible investments in cyber security.