A warning for data hoarders: the case of electronic invoicing

Regulating for Globalization
19/12/2018

Marco D'Ostuni, Andrea Mantovani (Cleary Gottlieb)

Please refer to this post as: Marco D'Ostuni, Andrea Mantovani, 'A warning for data hoarders: the case of electronic invoicing', Regulating for Globalization, 19/12/2018, http://regulatingforglobalization.com/2018/12/19/a-warning-for-data-hoarders-the-case-of-electronic-invoicing/

A recent ruling about electronic invoicing talks about the risks of collecting very large volumes of data under the EU's General Data Protection Regulation ("GDPR").

For the first time, the Italian Data Protection Authority ("DPA") used the general warning powers granted by the GDPR. It did so to prevent the National Revenue Agency from interfering too much with citizens' privacy when handling electronic invoices.

Should private data hoarders also take notice of the DPA's ruling?

The facts

Italian Law No. 205/2017 made electronic invoicing mandatory from 2019 for anyone established in Italy. The law does not give much practical detail on how the new system should work.

In April and November 2018, the Italian Revenue Agency ("IAR") adopted two decisions to regulate transmission of electronic invoices, storage and third-party access to collected data. The new rules were to apply to vast volumes of data about almost every aspect of a person's private life. Like shopping choices, professional activities, medical expenses and private hobbies.

Reacting quickly, on November 15, 2018, the DPA struck down the system devised by the IAR to manage the incoming flood of data from invoices.

The DPA spotted several "*serious issues*" under the GDPR. The IAR's storage and disclosure conditions were so wide as to be out of proportion with the scope of the law. Security measures against data breaches were weak in light of the data's volume and nature.

The DPA warned the IAR that, without major changes, the new system would violate the GDPR. The DPA asked the IAR to clarify urgently which remedies it would adopt.

This is the first time that the DPA has used its power under Article 58.2(a) of the GDPR. It is the power "*to issue warnings to a controller*" that its actions are "*likely to infringe*" the GDPR.

The DPA addressed the IAR as a common data controller. Thus, while the ruling involves a public authority, its contents could concern all controllers, including private companies. The case (and its expected follow-up) provides useful guidance on how to process large volumes of data in compliance with the GDPR.

Limit data processing

Controllers can collect only data that is "*adequate*", "*relevant*" and "*necessary*" with respect to the "*purposes*" pursued. This is the data minimization principle (Article 5.1(c) of the GDPR).

Controllers must also take precautions to ensure "*by default*" that data processing is limited to what is strictly necessary (Article 25.2 of the GDPR).

The DPA found that the IAR's system went beyond what the law required.

The IAR would not only collect data needed for tax reasons, but also other information contained in the invoices. This could include details about health conditions or criminal offenses (for instance, in invoices issued by doctors or lawyers) and reveal all kinds of personal habits and preferences.

Thus, the IAR was violating the minimization principle. Public interest did not justify such a vast data collection.

Design effective protection

The GDPR also establishes the rule of privacy by design (Article 25.1 of the GDPR).

Controllers must adopt "*appropriate technical and organizational measures*" to protect personal data. They must do so both when they design the "*means for processing*" and in the actual processing.

The measures and the organization must adequately counter the risks of data breaches. This requires careful planning and continuous attention to operations through the whole data processing chain.

According to the DPA, the IAR system did not comply with these rules. Security measures were not enough to protect the files from data breaches. No encryption tools were in place. In other words, because the wealth of collected data was attractive to cybercriminals, the IAR should have taken stronger countermeasures.

The DPA also found that ordinary access by third parties to this massive database posed additional risks. Accountants acting as intermediaries would be able to access "*an enormous bulk of information*" about thousands of clients. But the IAR had not set up safeguards to prevent them from using

the data for unpermitted purposes.

Compliance tools

Several tools can help design a system in compliance with the GDPR.

Public authorities have to "*consult the supervisory authority*" about law proposals or regulatory measures relating to data processing (Article 36.4 of the GDPR). However, the IAR had not consulted the DPA.

Additionally, when planned activities pose a "*high risk*" for data protection, controllers should run a prior impact assessment. They should think about "*measures*" to "*mitigate the risk*" (Article 35 of the GDPR). Then they may have to consult with the supervisory authority.

The IAR had not carried out this assessment either.

According to the Article 29 Working Party's *Guidelines*, a prior data protection impact assessment is always "*a useful tool to help controllers comply with data protection law*". This assessment could be required for large-scale data processing.

A list issued by the DPA in November 2018 also includes extensive processing of data "*of a highly personal nature*" (such as financial data) among the activities requiring an impact assessment.

A few final points

The minimization and privacy-by-design requirements apply to all data processing. Minimizing the use of large volumes of data may sound challenging. But no data controller can overlook the exercise.

Under Article 6 of the GDPR, processing must be tailored to fit its legal basis. A legal basis could be the data subjects' consent or, like in the IAR's case, the performance of a task in the public interest. The DPA's ruling shows that infringements to the minimization principle can also amount to violations of Article 6.

Privacy by design is crucial to ensure compliance. The risks of data breaches (such as unauthorized access, accidental loss, damage or destruction of data) increase as the volume of processed data grows. But even when measures are badly designed, effective remedial action can still mitigate fines.

In November 2018, the supervisory authority for the Baden-Wuerttemberg region fined a social media company that had stored unencrypted data (including passwords and e-mail texts) of hundreds of thousands of customers and suffered a data breach. The fine could have gone up to the highest of €10 million or 2% of the company's total worldwide annual turnover. But the actual fine was much lower (€20,000), because the company had cooperated effectively and reacted quickly to the data breach, with extensive improvements to its security systems.