Laura Liguori Partner
lliguori@portolano.it
Marco Bellezza Associate
mbellezza@portolano.it
Portolano Cavallo, Rome

The Garante's Sigue fine: a warning on financial services companies' compliance with data protection law

A recent fine handed down by the Italian data protection authority, the Garante, to UK company Sigue Global Service Limited alongside four of its agents in regards to the processing of personal data without consumers' consent stands as a warning not only of the incoming EU General Data Protection Regulation but also of how compliance with data protection law is essential for financial services companies as much as in any other sector. Laura Liguori and Marco Bellezza of Portolano Cavallo analyse here the circumstances and implications of the Garante's fine, which is the largest that the authority has ever issued.

On 2 February 2017 the Italian Data Protection Authority ('Garante') sanctioned five companies providing money transfer services with an overall fine amounting to more than €11 million for processing personal data without consumers' consent.

These are the highest fines ever issued by the Garante, and among the highest ever issued by any European data protection authority. The DPA decision has been widely viewed as an anticipation of the level of sanctions provided under the General Data Protection Regulation ('GDPR'). The DPA focus on financial services providers confirms that compliance with data protection rules is becoming a key issue for companies operating in this industry.

The facts

The proceedings before the Garante originated from the criminal investigations carried out by the Rome public prosecutor for infringements of Italian anti-money laundering law provisions.

According to the outcome of such investigations, the UK company Sigue Global Service Limited ('Sigue' - which operates in Italy through a local branch) - jointly with another four companies acting as Sigue's agents - carried out activities that are commonly known as 'fractionation.' Such practice consists of scattering large transactions amongst several accounts to circumvent the anti-money laundering rules that set forth the thresholds for allowed money transfers. In the case at hand, the public prosecutor found that large monetary transfers to China were split and attributed to more than 1,000 individuals distinct from the actual senders.

Moreover, the identification data used were collected from the Centralised Computer Archive (Archivio Unico Informatico), which is a database that financial intermediaries are required to keep for the purposes of counter-terrorism compliance and anti-money laundering.

The reasoning of the Garante

In parallel with the Rome public prosecutor investigations, the Garante started autonomous proceedings to understand whether the described criminal offences could also amount to data protection infringements. Eventually, the Garante found that, while fractioning the transactions in different accounts, the companies involved unlawfully processed the personal data of the account holders used to split the amounts that were sent to China, in contrast to the general rule provided by the Italian Data Protection Code (Legislative Decree no. 196/2003) under Section 23.

In particular, according to the Garante, the holders of the accounts to whom the relevant transactions were attributed did not consent to the use of their personal data for these purposes. The Garante inferred the absence of the account holders' consent from the following factual circumstances: (i) the account holders never coincided with the actual senders, (ii) the payment orders were not subscribed or, on some occasions, they referred to either fake or deceased individuals, and (iii) the money transfers were operated within a narrow range of time, for amounts that were almost equal to the prohibited threshold and they were addressed to a sole recipient.

In addition to the above, the Garante found that the infringements were especially harsh, considering that:

- the Centralised Computer Archive must be considered as a particularly important database given its institutional aims, regardless of the possible use for commercial purposes of the personal data contained in the database; and
- contrary to Sigue's defence arguments, each money transfer amounted to a separate infringement, since the companies could prevent the infringements following the first one and, therefore, a sanction had to be applied for each money transfer.

In light of the above, the Garante fined the involved companies for unlawfully processing the personal data of some of their clients and issued Sigue a sanction amounting to €5,880,000, the other companies acting as agents for Sigue were fined with sanctions amounting respectively to €1 million and €590,000, €1 million and €430,000, €1 million and €260,000 and €850,000.

Conclusive remarks

The fines issued by the Garante on this occasion are among the largest ever issued by a European data protection authority and the decision at hand might constitute a turning point in the authority's approach on the level of fines. The above is particularly true considering that the fine issued in the past by the Garante against Google in the *Street View* case - which amounted to €1 million - was the highest fine imposed by a European data protection authority before 2017.

In terms of the level of fines, the decision might be viewed as in anticipation of the GDPR in order that the shift from the currently-in-force national data protection law to the GDPR is smoother when the latter becomes directly applicable in 2018. Indeed, the GDPR provides for relevant sanctions, i.e. fines up to the greater of €20 million or 4% of a business group's annual worldwide gross revenues. Such amounts are largely higher than those provided by Member States' data protection laws that are currently in force, including those provided by the Italian Data Protection Code. The decision by the Garante in this case could thus be seen as a signal aimed at companies and designed to stimulate awareness in connection to the economic risks arising from non-compliance with data protection rules.

The decision is also a warning to the industry in general. Financial services providers should be aware of the specific data protection risks related to the provision of their services. In other words, compliance with the financial statutory and regulatory framework will not be the only issue at stake for such providers.

Traditional providers but also FinTechs are and will be more and more impacted in the future by the need to fully comply with data protection regulations. The large amounts of data available to FinTechs coming from different sources does not imply that such data are freely usable absent the specific and informed consent of the data subjects. Awareness in terms of data protection compliance should be an aim for the industry and decisions like the one briefly analysed above might help to increase such awareness.

EC Consumer Financial Services Action Plan includes focus on electronic ID

The European Commission ('EC') published on 23 March 2017 its Consumer Financial Services Action Plan ('Plan'), which aims to increase access and choice for EU consumers in the area of financial services, and which features a significant focus on technology.

"The national legislators and regulators tend to focus on their territory of competence which is why there are still so many country-specific rules in financial services law. The Plan may help to focus more on the big picture on the way to a real harmonisation of the rules," explains Lutz Auffenberg, Attorney-at-Law at Winheller.

Noting that presently only 7% of consumers in the EU buy financial services from another Member State, the Plan identifies three strands of work towards the realisation of the EU Single Market for financial services, namely clearing legal and regulatory obstacles facing businesses looking to operate cross-border, developing innovations in the digital space to remove barriers - such as through business' use of electronic identification and trust services to identify customers - and increasing consumer trust and empowerment, for instance through making cross-border non-euro transactions cheaper. "With a view to improving customer experience, the pressure on incumbents will remain high or even increase," said Dr Carsten Lösing, Partner at White & Case LLP. "This is for example expressed in the EC's requests for lower charges on non-euro transactions, more transparency in currency conversion, increased consumer protection rules, easier product switching, digital identity checks, better creditworthiness assessments and support for new competitors such as FinTechs."

The EC highlights that the 4th Anti-Money Laundering Directive allows for the use of electronic identification means under the EU Regulation for the electronic identification and trust services for electronic transactions ('eIDAS Regulation') as tools to meet customer due diligence requirements. The EC explains that it is, *inter alia*, working on testing the ability of banks to identify customers cross-border using e-ID means, through its Connecting Europe Facility. Dr Lösing believes that the Plan's exploration of how the eIDAS Regulation could be utilised by banks to engage with customers at a distance "addresses the increased need for a widespread use of distance/electronic identification and contracting. Cross-border use of electronic identification and the use of electronic identity schemes, as set out in the eIDAS Regulation, would make it possible to open a bank account online while meeting the strong requirements for customer identity proofing and verification for know-your-customer or customer due diligence purposes." "The most important point is the stronger promotion of the use of electronic identities and signatures," adds Auffenberg. "Regulators as well as firms are currently still used to paper-based identity/signature-proofs. Firms and regulators must be encouraged to develop electronic alternatives in digital times."