SQUIRE PATTON BOGGS

Data Protection in M&A Transactions in Italy

18 January 2021

Since the entry into force of European Regulation 679/2016, (GDPR), on 25 May 2018, GDPR compliance has become an increasingly relevant element in M&A processes in Italy.

The main issues giving rise to the increased focus on GDPR in the context of Italian M&A transactions include heightened awareness that:

1. Buyers may ultimately have to bear the costs for historical data protection breaches committed by the target, which can trigger heavy administrative fines from the Italian Data Protection Authority, *Garante per la Protezione dei Dati Personali* (Garante).
2. Data security breaches that have occurred pre-completion but are not detected until post-completion, may result in significant costs, penalties and claims. Data protection compliance breaches can also prevent the buyer from exploiting valuable personal data of the target.

In this context, GDPR compliance has acquired a far more relevant role in the overall due diligence process in Italy, and, indeed, in the related business negotiations.

For targets with significant reliance on personal data, particularly in such sectors as telecommunications and digital services, both buyers and sellers are more than ever conscious of the fact that a failure to comply with the GDPR may end up having an impact on the final pricing of the target company.

In certain cases, a target company's non-compliance with GDPR requirements may result in a reduction in the agreed price of the target, due to the inability of the buyer to lawfully exploit the personal data held by the target post-completion, plus the projected costs and resources that the buyer may need to spend to get the target's GDPR compliance up to an acceptable standard.

Potential Sanctions

The maximum administrative and pecuniary fines provided for companies that breach the GDPR, in Article 83, paragraphs 4 and 5, as implemented in Italy through Legislative Decree 101/2018, are:

- Fines of up €10 million, or up to 2% of total annual worldwide turnover for the preceding financial year, (whichever is higher) for certain types of violation, such as a failure to have the required processor terms in place or appropriate data security measures.
- Fines of up to €20 million, or up to 4% of total annual worldwide turnover for the preceding financial year (whichever is higher), in cases of more serious violations such as, *inter alia*, violations of the basic principles for processing, including conditions for consent, violations of data subjects' rights or unauthorised international transfers of personal data.

Recently, the Garante has adopted an ever more severe approach towards GDPR non-compliance.

In January 2020, the Garante imposed a fine on telecommunications operator TIM S.p.A. of over €27 million for a number of instances of unlawful data processing for marketing purposes, as well as a fine of €11.5 million on the company Eni Gas e Luce S.p.A. for unsolicited telemarketing and unsolicited activation of contracts.

Furthermore, the Garante also recently issued costly fines for data security breaches, which may be particularly relevant in the context of post-acquisition expenses, where a target has suffered a data security breach that does not come to light until post-completion. For instance, in June 2020, the Garante fined UniCredit S.p.A., a major Italian banking and financial services company, €600,000 for a data breach that occurred between April 2016 and July 2017, which affected personal data of approximately 762,000 data subjects.

These fines, even if not strictly connected with M&A processes, are relevant for M&A transactions, as buyers may have to face expensive costs or penalties that could potentially be avoided (or factored into the value of the transaction) through the adoption of a thorough data protection due diligence exercise.

The key issue is that a buyer inheriting a business that has significant GDPR compliance issues may have to bear costs to deal with such non-compliance: expenses to cover potential sanctions, expenses to render the business into a compliant state and potentially the inability to lawfully use a target's database, which could have been a key asset in the transaction.

Even though, to date, the Garante has not imposed fines strictly related to a breach of the GDPR in the context of an M&A due diligence, it may be that looking forward, the Garante will be influenced by the actions of its peer authorities, particularly in relation to the attention it gives to due diligence processes.

A fine of £18.4 million recently imposed by the UK data protection authority, the Information Commissioner's Office (ICO), on the Marriott group, will not have gone unnoticed in Italy.

In the *Marriott Inc.* case, the ICO initially proposed a fine of over £99 million that was specifically linked to a lack of privacy-related due diligence in the context of its acquisition of the Starwood hotel chain. Approximately 339 million guests worldwide were affected by a cyberattack on the hotels, which did not have appropriate technical or organisational measures in place to protect the data, in breach of the GDPR.

Although the breach occurred two years before the Marriott group acquired the Starwood hotels, the ICO reasoned that Marriott should be fined for "insufficient due diligence at the time of the acquisition of Starwood". Marriott Inc. had acquired Starwood Hotels and Resorts Worldwide, Inc. in 2016 without being aware that in 2014 Starwood had suffered a significant data breach, which was only discovered four years later, in 2018.

Information Commissioner, Elizabeth Denham, pointed out that, "GDPR has made it clear that organisations must be responsible for the personal data they process. This may include performing appropriate due diligence when making an acquisition, and implementing accountability measures to ensure not only how personal data has been acquired, but also how it is protected."

In July 2019, the ICO issued Marriott with a notice of intent to fine. As part of the regulatory process, the ICO considered representations from Marriott, including the steps Marriott took to mitigate the effects of the incident and the economic impact of COVID-19 on its business before setting a final penalty.

Eventually, after a year of investigations, on 30 October 2020, the ICO issued its fine in the amount of £18.4 million.

Lawful Basis Requirement for Disclosure of Data

An issue of concern during a due diligence exercise is the question of whether the processing of personal data involved in the transaction has a lawful basis, as prescribed by Article 6 of the GDPR.

M&A transactions may involve disclosure of significant amounts of personal data and it is, therefore, fundamental that sellers rely on a lawful basis for processing such data.

The key processing condition in an M&A context is likely to be the legitimate interest condition, i.e. that it is necessary for the purposes of a legitimate interest of the seller and/or the third-party potential acquirer to receive the personal data as part of the due diligence process and that these interests are not outweighed by any potential prejudice to the individual having his/her information disclosed.

In order to rely on legitimate interest, it is fundamental that the disclosure is minimised to the personal data that the buyer necessarily needs to evaluate the transaction and that personal data is anonymised or pseudonymised wherever possible.

Disclosure of personal data should, in fact, be limited to that that is strictly necessary, and should be disclosed as late as possible in the sale process.

For example, the upload of blank model contracts is best practice in the case of non-key employees having no special clauses in their employment agreements.

Where it is necessary to disclose personal information, appropriate safeguards should be put in place, such as restricting the individuals who have access to data, ensuring non-disclosure agreements are in place prior to disclosure and that all information is kept in a secure virtual data room.

In relation to the security of the data room, since sellers will often be transferring data to external parties, they should ensure that access to the data room is monitored and the data room policies comply with all applicable legal requirements.

Importantly, the GDPR requires a data processing agreement to be in place between the seller and the data room service provider to reflect that the service provider is operating as a data processor on the seller's behalf.

Interface With Law 231 Policy

A particular issue to buyers engaged in a due diligence process on an Italian target, or indeed a group that includes an Italian entity, is the interplay between the Italian company's data protection policy and, to the extent it has one, its Legislative Decree 231/2001 (**Decree 231**) policy.

Decree 231 provides that entities, companies and associations may be held liable for certain types of offences, specifically listed in Decree 231, committed on their behalf or for their benefit by a specific class of persons who have operational authority and may be liable on behalf of the company.

Decree 231 sets forth a list of criminal and administrative offences that may give rise to liability for the company, such as corruption-related crimes, IT-related crimes and unlawful data processing (unlawful access to an IT or telematic system, unlawful possession and diffusion of IT or telematic system access codes), money-laundering related crimes and crimes against industry and trade (harming the freedom of industry and trade, and unlawful competition).

These offences may be sanctioned by fines, restraining measures and/or confiscatory measures.

Pecuniary fines range from a minimum of €25,800 to a maximum of €1,550,000.

While breaches of the GDPR do not expressly fall within the Decree 231 list, Decree 231 does cover IT-related crimes and unlawful data processing.

Hence, there may be a risk that one of the IT-related crimes provided for by Decree 231 would constitute a criminal offence on the part of the company's "*Responsabile della protezione dei dati*", i.e. the individual responsible for data processing within the company, and, thus, trigger liability for the company.

In case of a crime of unauthorised access to an IT or telematic system, expressly provided for in Decree 231, a company could potentially:

1. Be held liable under Decree 231; and
2. Be sanctioned for breach of the GDPR, since this crime would likely entail a data breach, and would, thus, trigger possible sanctions for the company.

In light of these risks, buyers, as part of the due diligence process, are increasingly examining the interplay between the company's data protection policy and its Decree 231 policy in order to assess potential liabilities.

Conclusion

As a result of the above issues, sellers involved in M&A processes in Italy sometimes conduct a specific vendor due diligence exercise on GDPR aspects prior to putting a business on the market, in order to identify key areas of non-compliance and remedy them where possible, so as to mitigate potential transaction risks and their impact on the target's value, in addition to being ready to respond to a buyer's enquiries.

Buyers are more and more aware of the importance of paying due regard to data protection compliance as part of their due diligence, so that they can identify any issues that could be costly to deal with post-completion or even significantly reduce the value of the target business.

It is now not unusual in certain sectors for a buyer to engage a supplier to carry out separate IT security due diligence alongside legal due diligence, which may prove critical to identify any vulnerabilities that could lead to a Marriott-style fine post-completion.

If a thorough data protection due diligence exercise has been carried out, buyers may be able to reallocate the risk to the seller under the sale and purchase agreement through enhanced warranties or, where specific risks have been identified, insisting on conditions precedent to the transaction – to ensure that deficiencies are remedied pre-completion – and/or obtaining specific indemnities from the seller.

Increased sensitivity to the importance of data protection, recent increases in reported cases of damaging cybersecurity breaches, and increased activism in respect of data protection by the Garante has led to investors focusing more on GDPR-related aspects of due diligence on Italian targets.

We expect this trend to continue.

Contacts

Ian Tully
Partner, Milan
Corporate
T +39 02 1241 27702
E ian.tully@squirepb.com

Daniela Sabelli
Partner, Milan
Corporate
T +39 02 1241 27703
E daniela.sabelli@squirepb.com

Fabrizio Vismara
Partner, Milan
Litigation
T +39 02 1241 27707
E fabrizio.vismara@squirepb.com

Rosa Barcelo
Partner, Brussels
Data Privacy and Cybersecurity
T +322 627 11 07
E rosa.barcelo@squirepb.com

Francesca Fellowes
Director, Leeds
Data Privacy and Cybersecurity
T +44 113 284 7459
E francesca.fellowes@squirepb.com