EU General Data Protection Regulation: A Primer for Funds and Portfolio Companies

By Friedrich Popp, Associate, Debevoise & Plimpton LLP

Fund managers, investment advisers and portfolio companies doing business in the European Union have recently been required to adjust their procedures for data handling in light of Europe's new privacy law, the General Data Protection Regulation ("GDPR"). While this process has required the investment of significant resources, many businesses have taken the opportunity to improve the way they manage personal data more generally.

Data protection: a wide ranging fundamental right

Data protection is a fundamental right in the EU and from May 2018, the GDPR protects the personal information of individuals in the EU irrespective of their citizenship. Importantly, the new rules do not protect data relating to legal entities like corporations or funds.

The Regulation replaces the existing patchwork of EU data protection rules with (almost) uniform law across the EU and restricts member state discretion to certain limited areas such as employment law. Not only do individuals have several new rights to put them in control of their personal data, but the new rules are also backed by strong enforcement, including civil liability.

Processing of personal data

The GDPR will apply whenever personal data is processed. Funds process a variety of personal information, including data relating to its partners, employees, portfolio company management teams and investors. Portfolio companies also hold data relating to their customers, employees and other individuals. Some of that data may also come into the possession of the fund, including during due diligence on prospective investments, as well as during the life of the investment itself.

> "Not only do individuals have several new rights to put them into control of their personal data, but the new rules are also backed by strong enforcement, including civil liability.

The broad definition of personal data includes any information relating to an identified or identifiable individual, including their name, address, but also bank account details or investments made. Special categories of data, for example, health data, enjoy an even higher standard of protection. While anonymization of data can bring the

processing outside the scope of the law, breaking the link between the individual and their personal information is in practice not easy. Processing, the second element of the trigger, is virtually any use of data, including the collection, storing, sharing, transfer and erasure.

In other words, private equity fund sponsors will routinely "process" a wide variety of personal data and, as a first step, now need to understand what they hold and where.

While the GDPR was primarily intended to address concerns arising from data handling by large internet companies, the law does not distinguish between industries or take much account of the size of the business. European data protection authorities have made it clear that they expect all businesses to address data protection.

Extra-territorial application

The new rules do not only apply to businesses established in the European Union. Businesses with no physical presence in the EU are bound by the rules when they offer goods or services to individuals in the EU (even if no payment is required), or monitor their behavior, for example, by using webtracking tools for profiling purposes. In particular, using a website that is available in German, French and English and providing for payments in an EU currency may be characterized as reaching out to individual investors in the EU. If the GDPR applies to the non-EU business, it has to appoint a representative in the EU as a contact point for data protection authorities and individuals, unless the processing is only occasional and does not affect special categories of data.

Data controllers and data processors

The GDPR imposes obligations on both the data controller, the person responsible for the method and purposes of the data processing and the data processor, the person who processes data on behalf of the controller (which would include, for example, the provider of a virtual data room or a payroll service provider). The controller must enter into a written contract with the processor, specifying certain minimum privacy and security requirements. The controller also has joint and several liability with the processor if the processor infringes the GDPR. Therefore, the selection of reliable service providers is key and companies should look again at the data protection terms in existing contracts to check that they comply with the regulation.

Guiding principles

Several principles guide the GDPR, including the overarching principle of accountability: the new law not only requires compliance with the rules, but also the ability to demonstrate compliance, for example, by documented procedures. Personal data must be processed in a manner that is transparent to the individual and privacy notices should inform individuals specifically about the way in which their data will be handled. Further, the principle of purpose limitation requires the controller to use data only for specified, explicit and legitimate purposes and does not permit further processing that is incompatible with the original purpose. This principle makes it unlawful to collect customer data and then pass it to third parties for marketing purposes without prior consent. Data that is no longer needed must be deleted and data protection authorities expect businesses to have a policy detailing the time limits for erasure of different categories of data.

Do I need consent?

The GDPR provides several legal bases for data processing, including consent of the individual concerned. However, consent has to be freely given, specific and informed by a statement or a clear affirmative action (no pre-ticked boxes) and must not be hidden in lengthy terms and conditions. Consent can be withdrawn at any time and the individual has to be informed of their right to withdraw consent before giving it. Consent obtained prior to the GDPR can only be used if it demonstrably meets the new requirements. That means that, in practice, many businesses have had to seek fresh consent – explaining the volume of "opt-in" emails received in the run-up to 25 May 2018.

Processing is also lawful if it is necessary for the performance of a contract with the individual, which may, for example, include the use of contact details for correspondence with an individual investor. Processing is permitted if necessary for compliance with European legal obligations, to which the controller is subject, which causes some headaches for firms that have to comply with non-EU obligations. The use of "legitimate interest" as lawful base may be most appropriate if the processing is not required by law but of clear benefit to the business and there is only a limited privacy impact on the individual, in particular, in case the individual should reasonably expect the use of its data in that way.

"Businesses with no physical presence in the EU are bound by the rules when they offer goods or services to individuals in the EU (even if no payment is required), or monitor their behavior, for example, by using webtracking tools for profiling purposes.

Individual rights

Individuals have a number of rights, including a right to detailed information about the data processing and access to their data. Businesses have to comply with these requests without undue delay and in any event within one month. The same timing applies to requests for rectification of inaccurate data, the right to erasure and the right to data portability, which permits an individual to receive their data in a format that allows them to transfer it to another business. Compliance with these sometimes tedious requests within relatively short timeframes requires an established procedure.

> “Compliance with these sometimes tedious requests within relatively short timeframes requires an established procedure.

Internal processes and data security

Every data controller is required to maintain a record of processing activities with certain minimum content, including the purposes of the processing and the categories of data and the European supervisory authorities have emphasised that they expect compliance from all businesses, even very small ones.
The GDPR requires the implementation of state of the art technical and organizational measures to address data security, including tested procedures to ensure the integrity of personal data. This duty is underscored by a strict regime in case of a data breach: the controller must inform the data protection authority without undue delay, but at the latest within 72 hours of becoming aware of the breach. Furthermore, if the breach results in a high risk for the affected individuals, the data controller must also tell the individual without undue delay. Companies subject to the GDPR need to have a cyber incident response plan in place.

High risk processing

If a type of processing is likely to result in a high risk to data protection rights, for example, customer profiling, the controller must, prior to the processing, carry out an assessment of the impact of the proposed processing on the protection of personal data. This data protection impact assessment should describe the processing that is envisaged, assess its necessity and proportionality and explain how risks to the rights and freedoms of natural persons will be managed. The controller is required to consult with the supervisory authority before processing if the assessment suggests that the processing is high risk.

Controllers or processors that engage as their core activity in “regular and systematic monitoring of individuals in the EU,” or large-scale processing of special categories of data, must appoint a data protection officer reporting to the most senior level of management. EU member states may lower the threshold and Germany, as an example, requires the appointment of a data protection officer if there are at least ten employees dealing with automated data processing.

Transfers of data

A transfer of personal data to non-EU countries is only permitted if the Third Country either provides for an adequate level of data protection. The EU-US Privacy Shield enables transfer to the United States (subject to conditions) and transfers to Switzerland and certain other non-EU countries are also permitted under an adequacy decision. If there is no such decision, the parties can use the EU Commission’s Standard Contractual Clauses or other approved mechanisms to facilitate lawful transfers. Unfortunately, there is no exemption for intra-group data transfers and authority-approved binding corporate rules, a GDPR-mechanism binding all group members to EU data protection compliance, are meant to facilitate transfers to group members outside the EU. In practice, many transfers rely on an exception, for example, on the individual’s explicit and informed consent. If there are proceedings before a non-EU regulator or in other litigation, data may be transferred outside the European Union to the extent necessary to defend legal claims.

Supervision and penalties

Independent supervisory authorities in every EU member state monitor data protection compliance within their territory. If a case affects several EU member states, a lead supervisory authority coordinates the other supervisory authorities. However, businesses established outside the EU cannot rely on this one-stop-shop mechanism and have to deal with the regulator in every member state in which they are doing business.
The supervisory authorities enforce the Regulation, handle complaints lodged by an individual and conduct investigations. Such investigations can take place in the form of data protection audits and supervisors can obtain access to any premises of the controller or the processor. The authority issues warnings, orders compliance and can also impose a temporary or definitive limitation, including a ban on processing or transferring of data.

The GDPR specifically provides for the cooperation of supervisory authorities, including mutual assistance and joint operations, to address panEuropean risks. The Regulation seeks to ensure the consistent application of the Regulation throughout the EU and abolish the forum shopping of more relaxed regimes. Further, representatives of supervisory authorities of all EU member states convene in the independent European Data Protection Board to ensure the consistent application of the

GDPR; while the guidelines and recommendations issued by this body are not binding for local authorities or courts, practitioners closely follow guidance given by this forum.

An individual has the right to raise a complaint with a supervisory authority and challenge its decision before a court. Importantly, he or she can bring a civil lawsuit not only before the courts of the controller or processor, but also before the court in the member state in which it has its habitual residence. While there is a tendency in the EU to facilitate collective redress, there are no US-style class actions yet.

An individual who has suffered physical or financial damage as a result of an infringement of the Regulation has the right to receive compensation from the controller or the processor.

In accordance with the principle of accountability, it is the controller or processor who has to demonstrate that it is not responsible for the event giving rise to the damage.

The supervisory authorities can impose sanctions in accordance with criteria set out in the Regulation, which include the nature, gravity and duration of the infringement, as well as whether it was intentional or negligent. The maximum fines are very significant: the higher of 2% of the total group turnover or EUR 10 million. In addition, more serious offences, such as data processing on the basis of invalid consents, or violations of the data transfer rules, could result in fines of up to 4% of the total group turnover or EUR 20 million. Criminal liability may also attach to violations if stipulated by the local law of the EU member state.

So, what should I do?

Going forward, it is clear that the GDPR will have a dramatic effect on the way organisations handle their data. While it may seem like a daunting task, businesses can establish competitive advantage through rigorous and effective compliance. So, what should be done now?

1. Determine to what extent your organization is subject to the GDPR
2. Consider hiring a data protection officer (although it is generally not advisable to have a formal DPO unless it is required by the Regulation because it imposes further responsibilities)
3. Update fair processing and privacy notes
4. Assess (ongoing) validity of consents previously obtained
5. Consider conducting a data protection impact assessment
6. Implement a data breach response plan
7. Review and update data processing agreements
8. Be prepared to comply with new and enhanced individual rights, including subject access requests and the right of erasure
9. Identify your supervisory authority
10. Train staff

About the Author

Friedrich Popp is Associate at Debevoise & Plimpton LLP