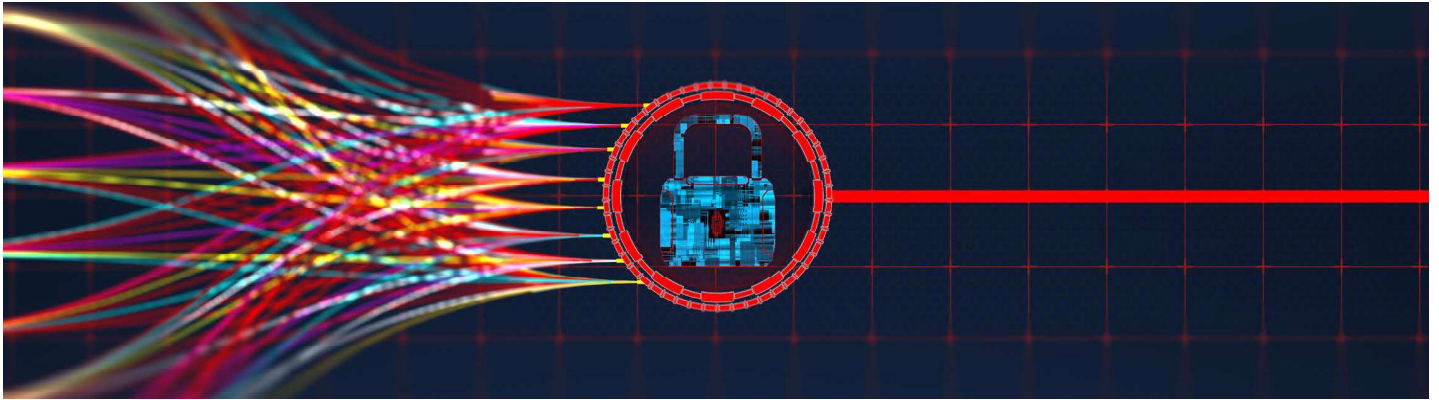




DATA PROTECTION GUIDE IN PRIVATE EQUITY DATA ROOMS WHERE THE TARGET COMPANY IS EUROPEAN

By Ignacio Lacasa & Manuel Martínez Ribas, Across Legal SLP

What documents or information should or should not be included in a Data Room?

What contracts must be signed before giving third parties access to a Data Room?

Here is a guide for when the target company is European, or processes data of European citizens.

In nearly all circumstances, documentation included in Data Rooms for the purposes of Private Equity (“PE”) investment, and other M&A transactions includes confidential, sensitive and/or personal information, sometimes irrelevant to the main purpose of the deal. The parties that share this information usually just sign an NDA without attending to other relevant matters of European Competition Law (although not always applicable) or European Data Protection Law (always applicable where personal data is included in the Data Room). However, this practice is not always correct.

In this article, we consider how European data protection obligations (and member state regulation) apply to due

diligence in PE transactions, whether the acquiring or investing party is within or outside the European Economic Area.

Up to a few years ago, Data Rooms used to be physical rooms that safely kept the original documents (or copies) on physical paper and it was forbidden to remove them from the Data Room or make copies except in some exceptional cases. This practice relied on the fact that human memory of precise details (e.g. personal data) is limited.

However, currently most Data Rooms are virtual, enabling massive and permanent electronic copying and increasing the risk of data breaches. Particular risks include a leak of the data to third parties or

processing the data beyond the legal, technical or economic analysis required for Due Diligence and subsequent negotiations of representations and warranties.

In all cases, when the target is an EU company or the data otherwise includes EU citizen data, access to the Data Room must comply with European data protection rules, in particular obligations regarding lawfulness of processing and providing information to data subjects about the access and processing of their data by the potential buyer or investor.

Considering the European General Data Protection Regulation (GDPR) and as a national example, the new Spanish Data Protection Basic Law (LOPDGDD), the following recommendations should be considered:

1 Remove personal data. This involves a (usually manual) process of redacting documents to remove all traces of personal data to the extent this is possible, partic-

ularly when the analysis of the documents does not require the disclosure of any personal data. In many cases, this will not be possible or will be counterproductive as the names/identification of certain persons is required to carry out the Due Diligence (e.g. to check that certain authorised persons signed an agreement).

2 Divide Data Rooms into two sections: Data Rooms can be divided into sections according to the classification of the documents. For our purposes, we propose one section that contains documents with personal data (contracts, staff lists, staff tax certificates, etc.) and another that contains documents without personal data (accounts, etc.).

3 Limit and monitor access: Access to the section of the Data Room that includes documents with personal data should be limited, documented and monitored

>> Continued on Page 18

>> Continued from Page 17

in order to ensure that only authorized persons access this section. This should also ensure that no documents with personal data are removed or copied, and that the documentation is only analyzed for the limited purposes of the Due Diligence report and, where the deal goes through, to negotiate representations and warranties.

4 **Interpose a third party between the target and the potential buyer:**

A conservative solution used in the past, that is still currently being used in some operations, is to interpose a consultant or lawyer between the target and the potential buyer so that this intermediary, although paid by the potential buyer, is subject to the contractual control of the target for data protection purposes. Under this contract the intermediary is considered a “data processor” (under past and current European data protection rules) under contractual and/or statutory obligations not to reveal any personal data to the potential buyer. This solution is also still used in Europe where the target must disclose some highly confidential technical information (for example, regarding patent applications, know-how, etc.) or other sensitive information that can affect the competitive position in the market (pricing, sourcing, etc.), using the intermediary to confirm the existence and general scope of information that cannot yet be shared or transferred from the target to the potential buyer.

5 **Sign specific contracts regarding data protection:** Under the European Data Protection Directive there were no express provisions for the communication of personal data from a target to a potential buyer

and, where communication did not rely on a previously obtained informed consent of the data subject, it was not lawful. Accordingly, because in practice one could rarely find such prior informed consents from data subjects, the solution was to use an intermediary (as commented in paragraph 4 above), working under a Data Processing Agreement that considered the communication of data as a mere “access” to the data and the intermediary could only process the data to produce the Due Diligence report and eventually negotiate representations and warranties. In addition, the old Spanish privacy law (arts. 5 and 19, in combination with art. 27) considered that a communication of data had not taken place once the commercial operation was completed. However, with the new rules, we conceive the two following solutions:

a. **More prudential and conservative solution: consider that the buyer’s lawyers and auditors are “data processors”.**

In analogy to situations where highly confidential information has to be disclosed, e.g. in relation to patent applications or know-how, or to prevent competition law breaches while sharing information, a **Data Processing Agreement** should be signed between the target and a third-party intermediary (generally, a lawyer or consultant of the potential buyer) stating that the personal data in the Data Room cannot be disclosed to the potential buyer. This Data Processing Agreement needs to include all regulatory requirements set out in the GDPR (art. 28). Where the lawyer or consultant is a firm, **each of its professionals should also sign a confidentiality and**

security form. This solution is convenient because under the Data Processing Agreement, the access to the personal data is lawful and data subjects need not be informed about the communication of their data to the intermediary.

b. **More novel solution, but with certain risks and with the likely additional obligation to inform data subjects: to rely on statutory provisions/exceptions.**

While the GDPR does not expressly contemplate whether the communication of personal data in a potential PE transaction implies an access or transfer of the data or is lawful, it does allow EU member states to make exceptions, which at least UK and Spain have done. For example, art. 21 of the new Spanish LOPDGDD states that: (i) such a communication is presumed lawful, provided that the processing of the personal data is necessary for achieving the operation and guarantees, where appropriate, continuity in the provision of services to data subjects; and (ii) personal data must be deleted if the transaction is not consummated. However, even if the access or processing is lawful under national law, the GDPR also requires this communication of personal data to be informed to data subjects (something that either or both parties in the transaction may not want to do), unless the parties can rely on any of the exceptions under art. 14.5 GDPR. Among these exceptions, art. 14.5(d) removes the obligation to inform where the party accessing the information is subject to a duty of professional secrecy imposed by the statutory rules at a European or Member State level. This is generally the case

for European lawyers and doctors, but not for other professions or for companies and their shareholders. The other exceptions in art. 14 (e.g. impossible or disproportionate efforts) are not always applicable in the framework of a PEransaction. Therefore, these exceptions may have limited effect. In any case, in this scenario, a **Data Communication Agreement** should be signed between the target and the potential buyer or its advisors, that strictly limits the processing of personal data in the due diligence documentation. Note that if the buyer itself accesses any personal data during due diligence, it will have a duty to inform the data subjects. And where the signing parties are firms, **the individuals accessing the personal data should also sign a confidentiality form** as stated in sub-paragraph “a” above.

Failure to comply with GDPR and national provisions on personal data processing could result in a sanction from the corresponding European Supervisory Authority which could reach up to the greater of the following two amounts: 20 million Euros or 4% of the billing of the companies involved (or potentially their group of companies).



Ignacio Lacasa
Partner, Across Legal SLP



Manuel Martínez Ribas
Partner, Across Legal SLP