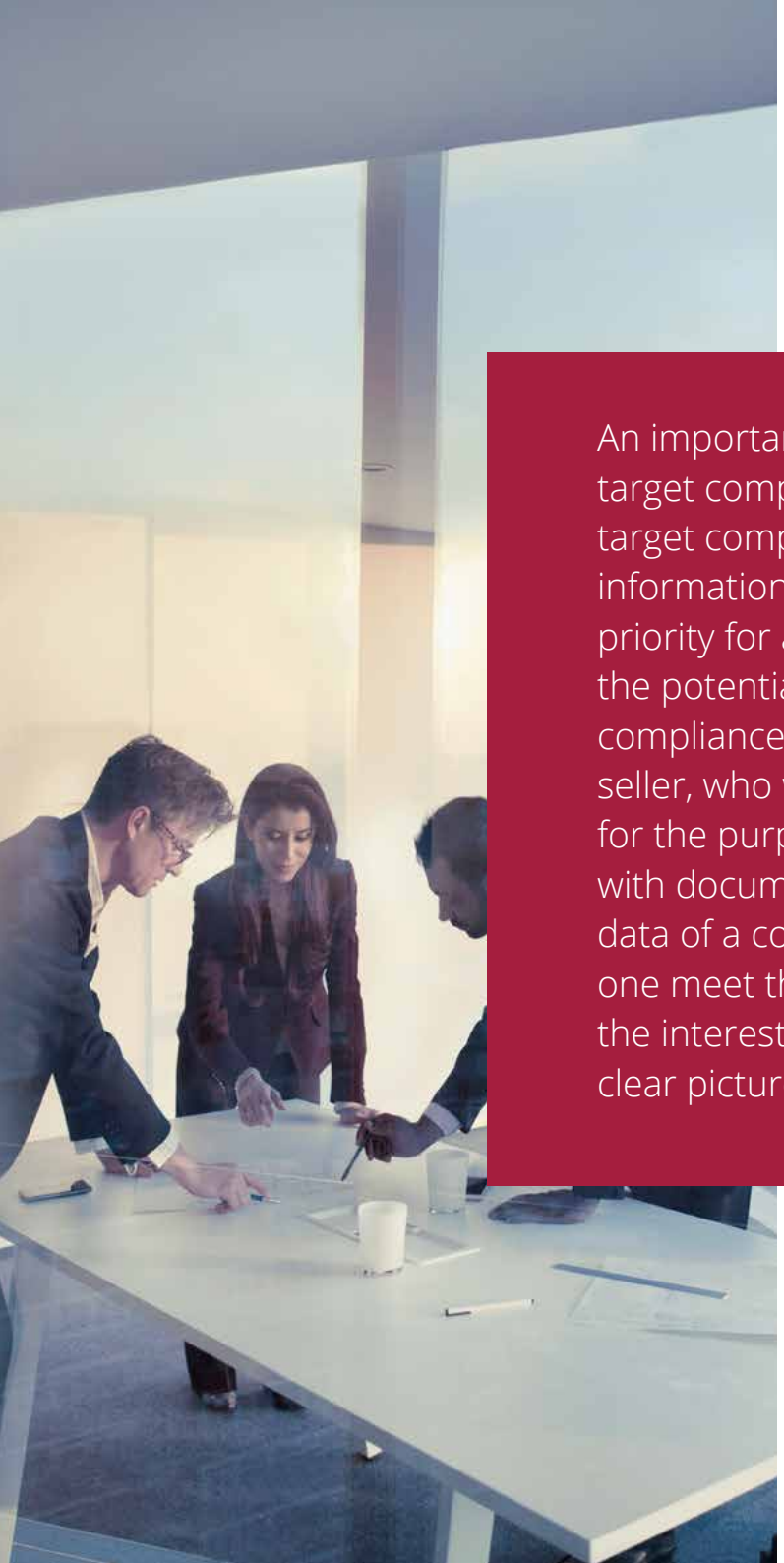
GGV Avocats . Rechtsanwälte

Drooms

DROOMS WHITEPAPER

Due diligence: A guide to protecting confidential information

drooms.com



An important step in M&A transactions is the legal and financial analysis of the target company, a process referred to as "due diligence". As part of this step, the target company will generally provide the potential buyer with large volumes of information. Data protection, including but not limited to personal data, is a high priority for all parties involved and must be considered in several respects. First, the potential buyer(s) should include an audit of the target company's compliance with data protection regulations in their analysis. Furthermore the seller, who wants to provide potential buyers with all the information necessary for the purpose of assessing price and risk, will have to provide potential buyers with documents and information containing personal data or, more generally, data of a confidential nature and/or covered by business secrecy. So how can one meet the legal constraints and/or protect the rights of third parties and/or the interests of the target company, while allowing potential buyers to form a clear picture of the target company?

All important questions

Several issues must be considered notably:

1. The qualification of the data and information and their sensitive or non-sensitive nature: does the data fall within the scope of the regulations on personal data, including the GDPR? Is the information being shared covered by business secrecy? Is it subject to a confidentiality agreement?

2. Which technical and organisational measures will be implemented in order to ensure data security and confidentiality (whether on the basis of Article 5 (f), Article 24(1) and Article 32 of the GDPR, business secrecy regulations, or by virtue of a confidentiality agreement to which the target company is a party)? One ought to consider:

- The choice of hosting provider which should meet any legal requirements (in particular Article 28 of the GDPR)
- The anonymisation or pseudonymisation of data
- Securing and limiting access to data and information to a circle of duly authorised persons or groups of persons under strictly defined conditions (management of access rights, conclusion of confidentiality agreements with sanctions in case of violation, etc.)

Deciding what data to protect

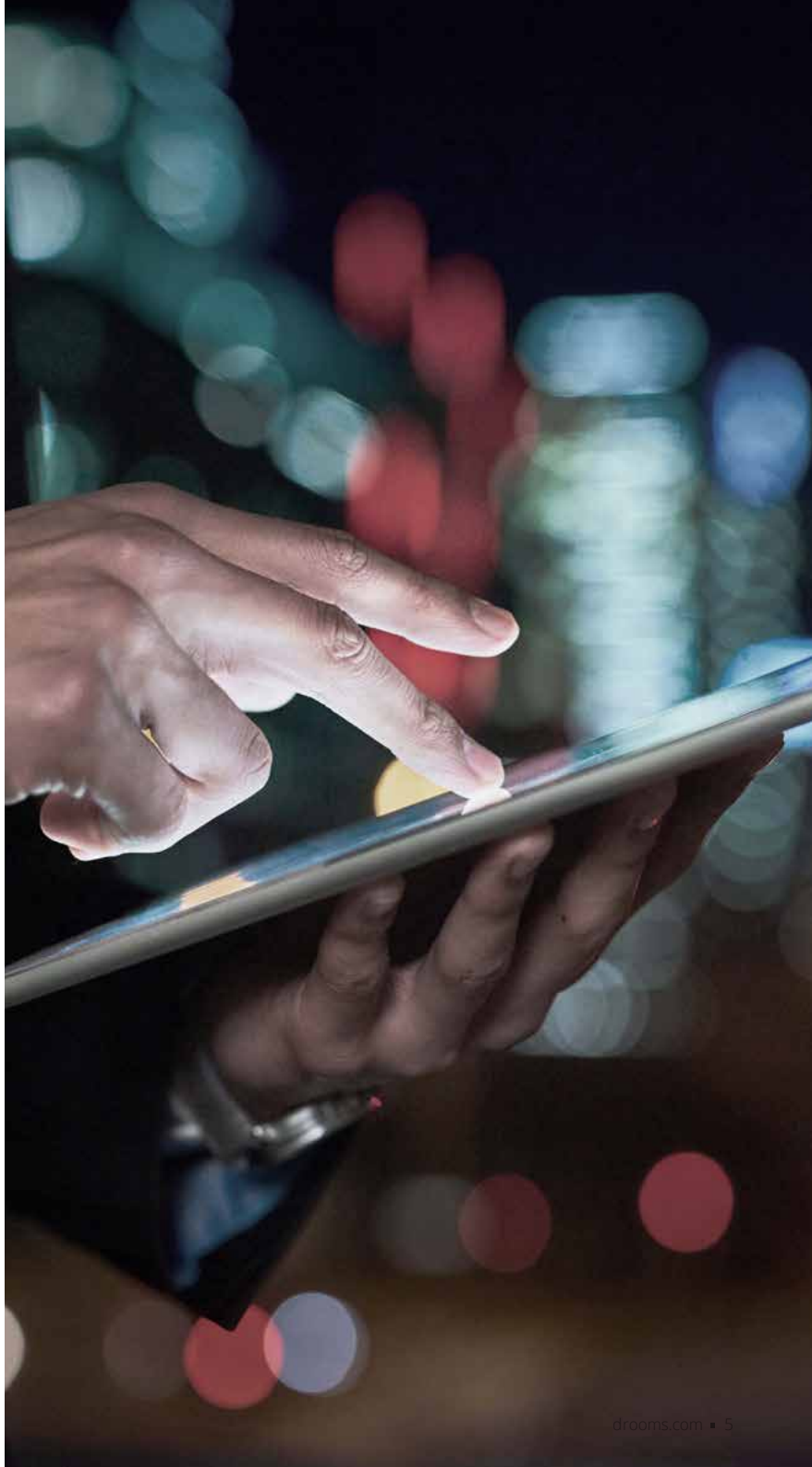
In the context of due diligence operations, different types of documents and information will generally be made available by the target company. Some of these documents contain sensitive and confidential data by nature and by law or because they have been categorised as such beforehand. Data can be classified into different categories including:

a. Data covered by the GDPR

A first category of data, to which the regulation grants a particularly protective status is that of personal data.

According to the GDPR, any information relating to an identified or identifiable natural person is to be considered as personal data. In this respect the European regulation specifies that “an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;” (cf. Article 4 (a) GDPR).

In the context of a due diligence process, the following information may be shared with potential buyers: data on employees, employee representative bodies, information relating to the management team, information relating to customers (this will particularly be the case if the target is a B2C business).



In accordance with the European legislation, as soon as data can be qualified as personal data, the processing of such data (and in particular its storage in the cloud, communication via a sharing platform, downloading, etc.) is subject to compliance with a number of obligations. One must:

- **Determine the legal basis for the processing of data:** according to the GDPR the processing of personal data is only lawful if at least one of the following conditions is met (Article 6 §1 GDPR):
  - the data subject has given consent to the processing of his or her personal data for one or more specific purposes
  - processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
  - processing is necessary for compliance with a legal obligation to which the controller is subject
  - processing is necessary in order to protect the vital interests of the data subject or of another natural person
  - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
  - processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

In the context of data made available to potential buyers, the processing of such data will mostly be based on the legitimate interests pursued by the data controller, i.e. the target company, such a legitimate interest, for example, in providing comprehensive information to a potential buyer. However, it will be up to the data controller to assess the lawfulness of the data processing operation on a case-by-case basis.

- **Comply with the principle of data minimisation:** the data controller shall only process data in a manner that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (cf. article 5 GDPR). This implies that data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means (see Recital 39 of the GDPR).

In the context of a due diligence process, this implies that only data that is strictly necessary is communicated and that data may be stored and communicated only if it is intended to enable potential buyers to form a true picture of the target company. On the other hand, when such information could also be provided without personal data (e.g. by anonymising the data beforehand), such a solution is preferred.

- **Data integrity and security:** personal data shall be processed in a manner that ensures its appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (cf. article 5 GDPR).

In the context of due diligence, this obligation will, among others, require the target company to select only a service provider that is reliable in terms of security. In addition, it will be up to the target company to ensure that the information is only communicated to a restricted circle of people who are aware of the need for data protection. Finally, a data retention policy that ensures deletion of data when it is no longer needed should be implemented.

It should be noted that these obligations will be borne both by the target company and the potential buyer who will process them once the documents are online (for instance by downloading and storing them, by transmitting them to employees and/or counsels in charge of the audit, by analysing them, etc.). In addition, the conditions must be met for each processing activity.

b. Data and information covered by business secrecy

In order to preserve innovation and strategic information, a European directive on the protection of business secrecy was adopted in 2016. The aim of the European directive is the protection of know-how and undisclosed commercial information (business secrets) against unlawful obtention, use and disclosure.

On 8 June 2016, Directive 2016/943/EU on the protection of business secrecy was implemented in France in Article L 151 of the French Commercial Code. This article defines the concept of business secrecy as well as the conditions under which information falling under this definition is protectable:

- "Any information meeting the following criteria is protected as a business secret:

  1° It is not, in itself or in the exact configuration and assembly of its elements, generally known or easily accessible to persons familiar with this type of information because of their sector of activity;

  2° It has a commercial value, actual or potential, because of its secret nature;

  3° It is subject to reasonable protective measures by its legitimate holder, taking into account the circumstances, to maintain its secrecy."

Any information falling within the scope of this definition is protectable, which means in particular that the owner of such information may prevent or limit its dissemination or use by third parties and prosecute offenders.

As an exception to the protection regime, the French law transposing the European directive, enables judicial or administrative authorities to request access to information covered by business secrecy.

On the other hand, business secrecy cannot be invoked either when the disclosure of the information was made "in order to reveal, in the interest of protecting the general interest and in good faith, illegal activity, misconduct or reprehensible behavior".

Furthermore, the information covered by secrecy may have been obtained in the exercise of the right to information and consultation of employees or their representatives.

Information covered by the protective regime may include, among others know-how, technological or technical knowledge or commercial data.

In the context of due diligence operations, the party detaining information falling within the scope of the above mentioned legal rules may assess whether the sharing of the information with a potential buyer is essential and where “reasonable protective measures” should be adopted in order for the information to remain in the scope of article l. 151 of the French Commercial Code.

In June 2016 in Germany, the European Directive 2016/943/EU was transposed into the "Law on the Protection of Business Secrecy" (Gesetz zum Schutz von Geschäftsgeheimnissen – GeschGehG), which requires a proactive approach by the legal holder in order to benefit from legal protection. In contrast to the former legal situation, a mere intention to protect business secrecy is not sufficient anymore. As a matter of fact, information will only fall within the scope of the law on business secrecy and thus benefit from the protection granted by such law if, and only if, it is subject to proportionate measures to prevent its disclosure.

If such measures are not properly adopted by the legal holder, the information to be protected will not only be accessible outside of the circle of authorised persons, but will also no

longer be protected as a business secret. For this reason, it is strongly recommended that a concept for the classification of trade secrets be implemented during due diligence. A mechanism that meets these new requirements protects the transferor, who may not have a vested interest in disclosing information.

To prevent this from happening, customer lists, innovative ideas, technical drawings and other trade secrets should only be made available within a data room when necessary and if so, only to a limited circle of people. Relevant data will have to be specifically identified as confidential and, if necessary, be protected by encryption.

In addition, to enable the secrecy holder to document the steps he/she has taken to proactively protect the information, the various participants in the due diligence process should be subjected to a non-disclosure agreement. Only a limited circle of people should have access to the information concerned.

c. Data and information covered by a confidentiality agreement to which the target company is party

The target company may, in the course of its business, have obtained information from third party companies and have undertaken a certain level of confidentiality with respect to these third-party companies.

Under such confidentiality agreements, which can be either unilateral or bilateral, the parties generally undertake to treat as confidential the information that the parties bring within the scope of the agreement. This generally implies that the information concerned may not be disclosed to third parties without the express agreement of the other party.

In most legal systems, non-compliance with contractual obligations/prohibitions may be sanctioned by damages.

This is why, in the context of an acquisition process, the target company must, before disclosing any information, check whether the data is freely communicable or covered by a confidentiality agreement.

d. All other data and information held by the target company and which are protected in another way (e.g. in the field of labour relations, intellectual and industrial property rights, etc.).

Some data may be confidential in nature without being classified as a business secret. This applies for instance to information provided to the Works' Council in the context of the search for a purchaser when the closure of an establishment is being considered (Article L1233-57-15 of the French Labor Code).

This kind of information may also be disclosed within the due diligence process.

The growing threat of data breaches

Very few organisations are prepared and expect to fall victim to a security incident until it's too late and systems and/or data is compromised. According to the latest figures by leading global provider of cyber risk and privacy management solutions IT governance, 729 security incidents took place between January and June 2021, breaching a total of 3,947,030,094 records globally. So how does this compare to previous years?

Data shows that although the number of breaches may be increasing, the number of individuals impacted by them is decreasing. 118.6 million people in the first half of 2021 were affected by a security incident, significantly less than the whopping 2.5 billion victims impacted in 2016. According to the Identity Theft Resource Center (ITRC), this can be explained by the change in focus of cybercriminals, who are looking to secure larger ransomware payments by targeting poorly defended firms and criminals. Manufacturing and professional services have seen the biggest increase in the number of cyber threats while the likes of the retail sector have seen a decline in incidences.

The Identity Theft Resource Centre (ITRC) and U.S. Department of Health and Human Services found that over 98.2 million people had been affected by the 10 biggest data breach incidents in the first half of 2021.

The records of 5.72 million people were compromised, including those pertaining to previous and current employees, following unauthorised access to Infinity Insurance Company's servers in December 2020. Data including driver's license numbers and social security information as well as staff medical history was affected.

One of the fitness industries beloved workout app's, Jetfit, fell victim to a data breach in March 2021 which affected over 9 million accounts registered before September 2020. Personal information accessed included the likes of email and IP addresses as well as password information.

ParkMobile, who specialises in electronic and digital parking solutions, was also affected by a breach originating from third-party software being used in-house. Flagged in March 2021, the incident affected 21 million individuals whose personal information including phone numbers, email addresses and license plate information was accessed without permission.

One thing we have learnt is that big or small, any business can be hit, even tech giants. Facebook was the victim of another incident despite efforts to rectify a breach in Q3 2019. A colossal 533 million users from 106 different countries were affected of which the majority had their phone numbers, user IDs, account creation date, bio, birth date, full name, location, past location and relationship status stolen.

In April 2021, Apple was also targeted. The $50 million ransomware attack reportedly carried out by Russian hacking group REvil, involved engineering and manufacturing plans stolen from its partner Quanta some of which have already been published online.

Users of private fintech company, Klarna, reported in May 2021 they were being logged out of their accounts and back into others where access to private information from other customers was accessible, including the likes of bank card details and postal addresses. The true number of customers affected remains unknown.

On the 14th of May 2021, Irish government agency The Health Service Executive (HSE) had 700 MB of patient data stolen by hackers, some of which was published online. The cybercriminals have since demanded over $20 million to stop them publishing more health records online. The agency is now facing regulatory fines and potential lawsuits from those affected.

Affecting businesses across sectors irrespective of size, The Microsoft Exchange hack appeared, at first glance, to be targeting enterprises and government agencies. According to the security firm who discovered the issue, Volexity, the hack very quickly exploded affecting mainly ill-prepared small-to-midsized businesses.

American multinational investment bank and financial services company Morgan Stanley was embroiled in a security breach incident in May 2021 affecting customer files in the hands of account maintenance service provider Guidehouse. Personal information such as addresses, names, social security numbers and dates of birth were stolen.

In June 2021 it was reported that data from 92 percent of LinkedIn users was for sale. According to VPN review site Privacy Sharks, 700 million records were found on a hacker forum. Disputed by the employment-oriented online service, allegedly names, email addresses and phone numbers were stolen.

One of the household names affected by a security breach which impacted 3.3 million individuals based in the U.S. and Canada, was Volkswagen Group of America. According to information the group disclosed in June 2021, a third party acquired information for sales and marketing purposes through a vendor used by other car manufacturers and dealers including Audi. Of the customers and prospective customers affected, 90 000 had sensitive data such as their driver's license numbers compromised, while others had their names, emails, addresses, phone numbers, date of birth, social security or social insurance numbers, account or loan numbers, tax identification numbers, and vehicle information exposed.

A lack of preparedness by organisations

According to research released by cybersecurity company FireEye, over half of organisations world-wide remain unprepared for a security incident. In its Cyber Trendscape Report 2020, that surveyed 800 CISOs and Senior Level Executives across Europe, North America and Asia, a staggering 50% of CEOs believed their business was illequipped to tackle cyber threats. A further 29% of firms revealed a lack of comprehensive testing, leaving gaps in their defences.

Many of those surveyed thought cyber threats would become increasingly prevalent and worse over time. The annual Cost of a Data Breach 2021 Report released by the Ponemon Institute and IBM Security detailed the significant increase in the average total cost of a data breach in recent months driven partly by the work from home guidance following the COVID-19 outbreak.

What factors cause such data breaches? Beyond the vulnerability in the IT system, the human factor often plays a determining role.

Heavy risks

A single cybersecurity attack can have major long-term implications for businesses. Reputational damage resulting from a lack of customer trust can cause existing clients to look elsewhere, reduce the likely hood of attracting new clients, affect a firms supply chain should partners walk away, lower investor confidence, and ultimately negatively impact profit margins and share prices.

An analytics report by Aon and Pentland looking at reputational risk in the cyber age showed just how considerable the fall out can be with some firms reporting a drop in their market value of 25% over the 12 months following an attack. Famously Yahoo suffered a breach in 2013 that significantly impacted its share price and valuation three years later when it was acquired by Verizon at a discounted rate of $4.48 billion.

Audit and assurance giant PricewaterhouseCoopers (PwC) reported a continued lack of confidence among consumers they surveyed, of which 69% thought the organisations they use are currently unprepared for a hack. According to the survey 87% of consumers are ready to go to a competitor should a security incident occur.

Telecommunications company TalkTalk got a taste of this when a hack impacting 150 000 of their customers led to the firm losing more than a third of its value and 100 000 users in 2016.

Financial loss due to customer compensation schemes, incidence response efforts, investment into new measures, investigations, operational downtime and disruption to trading can also pose a major risk to businesses who suffer a breach or hack.

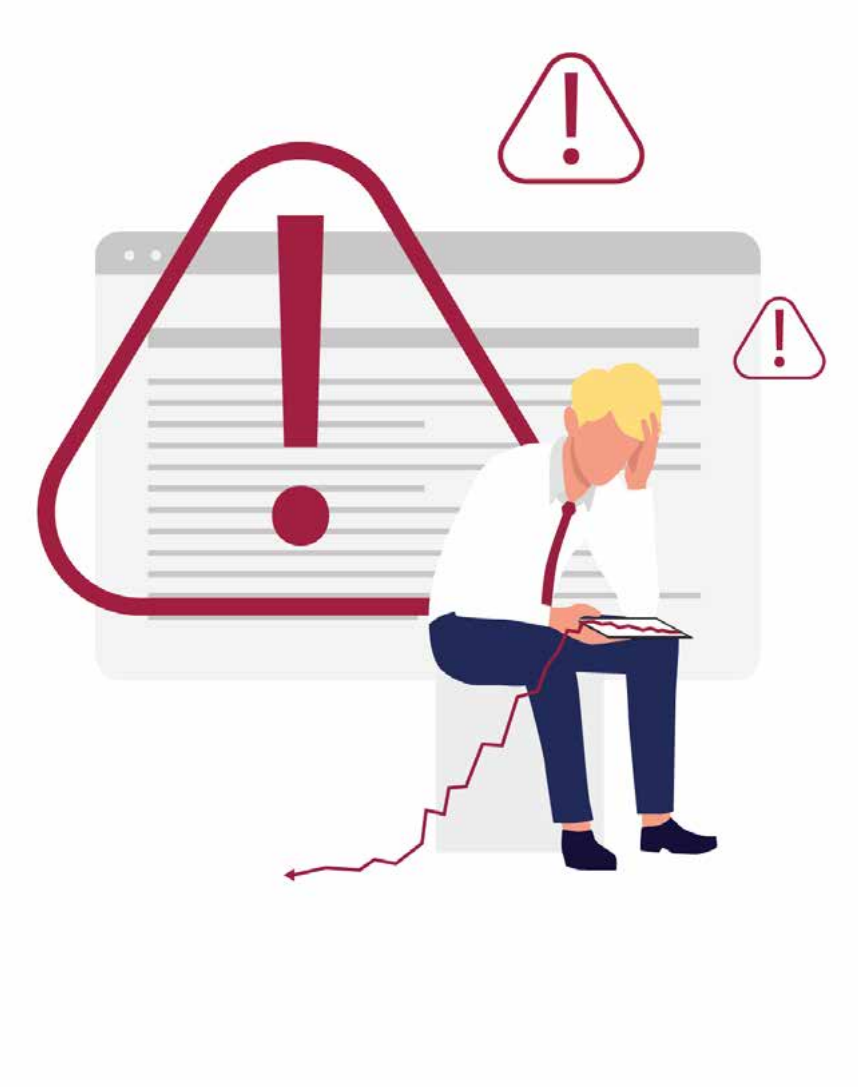
One should never underestimate the regulatory penalties and fines linked to non-compliance to the General Data Protection Regulation (GDPR) either, which can reach 4% of annual global turnover or 20 million Euros (whichever is higher).

Up from $3 trillion in 2015, global costs related to cybercrime will increase by 15 percent annually in the next five years,

reaching $10.5 trillion per year by 2025 according to Cybersecurity Ventures.

Legal action from individuals affected by a cybersecurity attack and looking to claim compensation is another risk to a business' survival. A surge in the number of class action lawsuits following loss of personal data has been witnessed in the US and UK in particular and is unlikely to slow down as the severity of cases increases. 145 million people globally were impacted by the 2017 Equifax data breach that saw the credit reporting agency pay out more than $700 million in compensation to affected US customers alone.

Finally, a loss of highly sensitive personal information following a security breach can be even more harmful than financial and reputational damage. Biometric and genetic data, which can be used to identify an individual, is priceless to cybercriminals. Medical records, if deleted, could also have a se-vere impact on a patient's medical treatment and eventually their life.



Meeting confidentiality requirements

Regarding personal data, article 32 of the GDPR requires that data controllers take "all technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing"

Similar measures should/may be adopted to protect other sensitive and/or confidential data held by the target company.

Choice of cloud service provider

While cloud computing technology can be harnessed in a variety of ways, cloud storage remains one of its most popular applications at enterprise level. Unlike traditional methods, cloud storage relies on information being stored virtually on servers. It is based on an on-demand computing model that uses an Internet connection for sharing and allowing access to data. When data is stored on the cloud, i.e. on a third-party server, it can be accessed via multiple devices and anywhere in the world with a stable Internet connection helping businesses operate faster and more efficiently.

Its success is largely due to the host of benefits it offers including added security compared to hardware, which is subject to damage and disintegration.

Cloud services are not created equal however and major concerns surrounding the risk associated with infrastructure misconfigurations remain an issue so carrying out due diligence is important. When it comes to document management, virtual data room (VDR) platforms are gaining the upper hand over generic file sharing services. While generic file sharing providers tend to focus on the ease of sharing files and their protection during the initial data transfer, VDR's also safeguard against data modification, processing or loss long-term and tend to have a whole host of security measures built in. To note just one example, in 2016, Dropbox had to admit a leak of passwords and email addresses of over 68 million of its users. Since virtual data rooms focus on security during and after uploading, data breaches are less likely.

Virtual data room environments also benefit from secure login systems that often offer multifactor authentication. In addition, they tend to guarantee fast back up and disaster recovery lowering the risk of costly downtime. Users benefit from:

- **Continuous data monitoring** – you can instantly be alerted to uncommon activity whether it's coming from an external or internal source
- **Enhanced encryption** – files can be heavily encrypted to make data much harder to hack and decipher
- **Better compliance** – data can be stored in compliance with the latest legislation including the likes of the General Data Protection Regulation (GDPR)

The infrastructure caters to a variety of needs and can be configured and customised accordingly. Aside from supporting the likes of secure file sharing and storage, due diligence processes and c-suite communications, VDR's have become an established platform for effective portfolio management. Offering a solution during the whole life cycle of assets enables users to address issues surrounding data gaps and varied file formats.

How Drooms processes information

› **Protecting the confidentiality and security of data and information by providing an infrastructure that meets the requirements of the regulation.**

With the EU General Data Protection Regulation in full force, the need for data controllers to vet their current providers and designate only reliable partners for data processing activities has become ever the more critical. As a fully GDPR compliant, European provider headquartered in Germany, Drooms has never needed to adhere to risky additional safeguards such as Model Clauses. Drooms carries out its core activities and functions including invoicing and billing, IT, Customer Services and hosting within the EU to minimise risk. Hosting, invoicing and/or IT support is not outsourced to third parties or subcontractors either who tend to be the biggest area of risk exposure for businesses. All data is stored on proprietary, ISO certified servers in Germany or Switzerland, which only dedicated Drooms employees can access for maintenance purposes. All data processing activities take place exclusively in Germany.

For Swiss customers special storage located in Switzerland is offered.

Drooms also performs internal vulnerability scans and penetration tests. In case of an emergency its disaster scenario plan guarantees that data remains unaffected. Drooms keeps data confidential, secure and highly available with N+1-concept, encryption at rest and a secure tier architecture too.

One of the ways Drooms takes the privacy of its customers extremely seriously is by not keeping and analysing personal data available within the data room for future research and repurposing. Even when it comes to billing, it only holds the minimum amount of information required within its database to process payments. To increase resilience against cyberattacks ongoing employee security awareness training for all staff is also mandatory.

How Drooms processes information

The provision of administration tools to manage access to data and information (including the definition of access rights, implementation of a data deletion policy, etc.).

Drooms' resilience-based architecture built with security in mind offers a whole host of tools to manage controlled access to data. Some of its data room features that support secure work processes include the likes of:

- IP filtering: the possibility to limit data room access at group level to specific devices with specific IP addresses is available
- Multi-factor authentication: the option to sign in to the Drooms platform using an additional security code sent via SMS is offered
- High end encryption: for premium security, data transfers are only possible via TLS connections with the latest encryption protocols & ciphers
- User rights and permission controls: individual granting of review, print, and/or storage authorisations at user and document level as well as dynamic watermarking is possible
- Detailed reporting: Drooms offers complete activity reporting of all users in the data room

Drooms is utilising artificial intelligence (AI) to help automate workflows and increase efficiencies. To ensure a high standard of security and reliability, Drooms has developed and integrated its technology in-house, instead of relying on third-party products. Drooms also considers privacy and data governance, as well as human oversight. That means, it always keeps a human in the loop to confirm suggestions generated by artificial intelligence to ensure quality of results and accountability. Similarly, it also considers guiding principles for designing intelligent solutions, aiming at responsibility, explainability, accuracy, auditability and fairness.

Anonymisation or pseudonymisation of data and information

The GDPR does not require data controllers to anonymise data, but expressly states the need to ensure data security, including encryption or pseudonymisation (article 32). While pseudonymisation means that (personal) data is processed in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, in the process of anonymisation the data can no longer be linked to an individual.

These two techniques, which are often difficult to distinguish, can thus be differentiated by the irreversible nature of the processing applied to the data. It is in this respect that anonymisation is a technique which, if properly implemented, preserves the rights of the person concerned, since it makes the data lose its personal character.

However, before considering one or the other technique, it is necessary to determine whether the process should be irreversible or not, which must be assessed according to the nature and sensitivity of that data.

Securing third party access to data by setting up confidentiality agreements

Confidentiality agreements are usually signed by the disclosing and recipient party. Data room access may also be subject to the acceptance of an NDA.

NDAs usually contain the following clauses:

- Definition: the purpose of the clause is to specify the scope of the confidentiality commitment in the context of the project considered by the parties

- Scope: the purpose of the clause is to define the rights and obligations of either party with respect to the confidential information. The parties also generally commit to confidentiality for all parties involved in the project (including their employees, consultants, agents)

- Exclusions: are generally excluded from the NDA's scope information (i) which is in the public domain at the time of disclosure or falls into the public domain after disclosure other than by an act or omission of the recipient; (ii) which the recipient can prove that it was lawfully in possession of at the time of disclosure and which was not acquired directly or indirectly from the disclosing party; (iii) which was lawfully obtained from third parties authorised to disclose it; (iv) which was independently developed by the recipient's employees without reference to or reliance on such information; (v) the publication of which was authorised by a written agreement of the disclosing party; or (vi) the disclosure of which is required by any law or pursuant to any valid governmental or judicial request, requirement or injunction)

- Term: If no term is set forth by the NDA, the contract may be considered to be for an indefinite period and either party may terminate it at any time without compensation

- End of the contract: commitment by the parties to no longer use the information and to return it (time limits and procedures to be defined)

- No transfer of property rights: the NDA generally specifies that the confidential information remains the property of each party

- No further commitment: the NDA usually specifies that the communication of confidential information does not constitute a commitment to carry out the project, which is the subject of a separate contract

- Penalty clause: the breach of an NDA is generally subject to indemnification. However, it is up to the victim to prove the damage and its amount, which can raise some difficulties. Sometimes NDAs anticipate such issues by implementing a penalty clause setting the amount of compensation in the event of a breach of the NDA

- Applicable law and jurisdiction: this clause is important when the parties to the NDA are of different nationalities

In addition to its primary function, the confidentiality agreement submitted for acceptance by each user may also have a function of raising the users' awareness of the confidentiality and/or protection worthiness of certain data.

Once the NDA is signed, it will be the responsibility of the data recipient to ensure that the commitments made in the NDA are respected by employees and external consultants. This will be done through confidentiality clauses in the employment contracts or in service contracts. In addition, it must have taken operational and technical measures to ensure data security. When data is personal, and its processing is carried out with the help of subcontractors within the meaning of Article 28 of the GDPR, an appropriate data processing agreement must be concluded with the service provider.

For all these questions it is useful to hire a lawyer, who is himself subject to an obligation of confidentiality under the code of ethics applicable to the profession and subject to criminal sanctions.

About GGV Avocats - Rechtsanwälte

With 20 lawyers covering 7 areas of expertise (M&A-corporate, labour, tax, real estate, business law, litigation, data protection-IT-IP), GGV Avocats – Rechtsanwälte is a Parisian law firm specialised in cross-border operations including: vendor due diligence, selection of documents required for data room upload, the set up and structure of data room content, Q&As, the drafting and review of NDAs, drafting of relevant agreements (SPA, asset transfer, merger, investment agreement, warranties and representations, management packages, shareholder's agreements…) and the negotiation process through to completion.

GGV contributors

Catherine Stary is a lawyer at the Paris bar, holds a CIPP-E certification and is Counsel at GGV Avocats Rechtsanwälte.

Catherine Stary is in charge of GGV Avocats Rechtsanwälte's data protection and IP/IT department. In this capacity, she also advises and assists as an external DPO to various German companies with activities in France.

Caroline Blondel is a lawyer at the Paris Bar and Partner at GGV Avocats Rechtsanwälte.

Caroline Blondel advises international companies on mergers and acquisitions, corporate law and commercial law issues concerning their French subsidiaries.