Belgium

Steven De Schrijver and Rudi Desmet
Astrea

STRUCTURING AND LEGAL CONSIDERATIONS

Key laws and regulations

1 What are the key laws and regulations implicated in technology M&A transactions that may not be relevant to other types of M&A transactions? Are there particular government approvals required, and how are those addressed in the definitive documentation?

The key laws that may be more relevant for technology M&A than for other transactions in Belgium are the following intellectual property laws.

Trademarks in Belgium are governed by the Benelux Convention on Intellectual Property of 25 February 2005. The Benelux countries (ie, Belgium, the Netherlands and Luxembourg), constitute one single jurisdiction for trademark purposes. It is, therefore, not possible to obtain trademark protection in Belgium alone. In addition, Belgium is a party to a number of international trademark treaties. It is also possible to register a community trademark (CTM): the CTM system provides uniform trademark protection throughout the whole of the European Union and is administered by the Office for Harmonization in the Internal Market.

In Belgium, copyright is governed by Title 5 of Book XI of the Code of Economic Law (articles XI.164 to XI.293). The protection of computer programs is governed by Title 6 of Book XI of the Code of Economic Law (articles XI.294 to XI.304). The content not covered by Title 6 is supplementarily governed by the general rules on copyright in the Code of Economic Law. Further, the protection of databases is governed by Title 6 of Book XI of the Code of Economic Law (articles XI.305 to XI.318). Certain provisions of Book I (definitions), Book XV (law enforcement) and Book XVII (actions for injunctions) of the Code of Economic Law also apply to the protection of copyrights, computer programs and databases.

In Belgium, the protection of patents is governed by Title 1 of Book XI of the Code of Economic Law (articles XI.1 to XI.91). Article XI.2 also includes the implementation of Directive 98/44/EC on the legal protection of biotechnological inventions. Belgium has signed the European Patent Convention of 5 October 1973, as well as the revised European Patent Convention 2000 (which came into force on 13 December 2007). Belgium is also participating in the unitary patent regulation and has ratified the Agreement on a Unified Patent Court (Regulation (EU) No. 1257/2012 of the European Parliament and of the Council of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection).

Designs in Belgium are governed by the Benelux Convention on Intellectual Property of 25 February 2005. The Benelux countries constitute one single jurisdiction for design purposes. Thus, it is not possible to obtain design protection only in Belgium. Belgium has also adopted several international conventions in the field of designs. European Commission Regulation No. 6/2002 of 12 December 2001 introduced a single, European community-wide system for the protection of designs, which exists in parallel with the Benelux system. Designs can be registered with the Office for Harmonization in the Internal Market. This system provides for two kinds of design protection: registered Community designs and unregistered Community designs.

In Belgium, trade secrets and industrial know-how are protected under the Act of 30 July 2018 and articles XI.332/1 to XI.332/5 of the Code of Economic Law. Further, article 17(3) of the Act of 13 July 1978 on Employment Contracts prohibits an employee from disclosing trade secrets (as defined in the Code of Economic Law) and secrets relating to personal or confidential matters of his or her company either during or after the end of his or her employment. Article 309 of the Criminal Code lays down penalties in the case of disclosure of industrial or fabrication secrets by an employee of a company to a party not employed by that company. Know-how or trade secrets can, furthermore, be protected indirectly under the general principles of tort or by including confidentiality clauses in contracts. Further, article VI.104 of the Code of Economic Law regarding business-to-business market practices prohibits any act contrary to fair commercial practices. In certain circumstances, unauthorised use of a competitor's know-how or trade secrets may be considered an act of unfair competition.

If it concerns an asset deal, buyers of technology assets need to ensure that the transfer of IP is registered with the relevant office where the IP is registered.

Other laws more relevant in technology M&A transactions than in other transactions are the privacy laws set out in the General Data Protection Regulation (GDPR) and the Belgian Privacy Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (which replaced the Belgian Privacy Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data, with effect from 5 September 2018). Certainly, when the transaction takes the form of an asset deal and one of the assets consist of customer data that qualifies as personal data, it needs to be checked whether the customers have given the necessary legal consent to transfer their data.

If the target is active in e-commerce, other laws that may be relevant are the Act of 11 March 2003 with respect to certain legal aspects of the services of the information society, the law of 10 December 2009 relating to payment services and Book VI 'Market practices and consumer protection' (articles VI.1 to VI.128) of the Code of Economic Law.

In principle, there are no specific governmental approvals required except for the standard competition approvals (if the merger notification thresholds are met).

Public M&A bids will be subject to the supervision of the Financial Markets Supervisory Authority.

Government rights

2 | Are there government march-in or step-in rights with respect to certain categories of technologies?

Government march-in or step-in rights do not exist in Belgium.

The Belgian telecommunications industry has been largely liberalised under the auspices of the European Union but still remains a regulated industry. However, the regulations relate mainly to matters such as the transfer or sublicensing of licences and do not discriminate between domestic and foreign investors. During the privatisation process the Belgian and Flemish governments took a 'golden share' (ie, a nominal share held by the government that is able to activate all other shares in certain specified circumstances) in certain telecommunications companies, but the EU Court of Justice held that such 'golden shares' are only permitted to the extent they are in the general interest.

Legal assets

3 | How is legal title to each type of technology and intellectual property asset conveyed in your jurisdiction? What types of formalities are required to effect transfer?

When there is an asset deal and registered IP needs to be transferred, the parties need to make sure that the transfer is set out in a written agreement and that the transfer is registered with the relevant agency:

- trademarks: the Benelux Trade Mark Office in The Hague or with the Trade Marks Section of the Intellectual Property Office of the Ministry of Economic Affairs;
- patents: the Patent Section of the Intellectual Property Office of the Ministry of Economic Affairs or the European Patent Office;
- models and designs: the Benelux Models and Designs Office in The Hague or with the Models and Designs Section of the Intellectual Property Office of the Belgian Ministry of Economic Affairs; and
- domain names: depending on the registrar (eg, for '.be' domain names it is DNS Belgium).

Valid transfer or assignment of copyrights is not subject to any conditions, although proof of transfer can only be brought against the author in writing.

All contracts are interpreted restrictively in favour of the author (article XI.167 Code of Economic Law). An important restriction is that the author cannot transfer his or her moral rights. He or she can transfer the exercise of individual moral rights to third parties (eg, collective collecting agencies) but cannot transfer the actual ownership of the moral rights as a whole.

Another restriction is that, if an author wants to benefit from tax-friendly copyright royalties under the Act of 16 July 2008, in return for the transfer (or licencing) of his or her copyrights, it is highly advisable to describe the transfer (or licencing) and the amount of the royalties in sufficient detail in a written contract.

The same applies to any trade secrets, know-how and database rights.

DUE DILIGENCE

Typical areas

4 | What are the typical areas of due diligence undertaken in your jurisdiction with respect to technology and intellectual property assets in technology M&A transactions? How is due diligence different for mergers or share acquisitions as compared to carveouts or asset purchases?

Since the target's technology and IP are the most valuable assets to an acquiring technology company, a thorough and comprehensive due diligence of such assets is essential to ensure future revenue streams and restrict legal actions in the post-merger phase. Such due diligence usually focuses on owned IP, third-party IP, IP disputes and IT assets.

An important feature of the review is analysing the ownership of the IP. Under Belgian copyright law, software is protected for up to 70 years after the death of the author. However, only the form and expression of the idea is protected.

Anyone is allowed to write a program with the exact same functionality, provided that it is based on a self-developed source code. Just because the target company owns the IP of a certain software, does not mean that it is protected against the copying of the idea. A solution could be found in patenting the software but that method is, in the European context, no guarantee, since there is great disagreement about the patentability of software.

The due diligence should not only focus on the ownership and value of the IP rights, but also – and foremost – on their transferability.

The objective of any IP due diligence audit would be to answer one or more of the following questions about the target's technology assets:

- What was the origin of the technology asset?
- When was the technology asset first conceived and when was the development completed?
- Who are the people who could claim to be an inventor or author?
- What types of IP rights might be available to protect the technology asset and have those rights been protected?
- Has any employee, consultant or other third party used any trade secrets or proprietary technology of others in the development, support, maintenance or enhancement of the technology asset?
- Does any third party have IP rights that could be violated by past or future uses of the technology asset?
- Have any offers of licences or assertions of proprietary rights infringement claims been received and is there any litigation pending or threatened?
- Where consultants or independent contractors have been used to develop the technology asset, have adequate measures and agreements been taken to protect the proprietary interests of the hiring party and to ensure that the hiring party owns the rights to the technology asset?
- If any portions of the technology asset were purchased or licensed from third parties, what rights were acquired by the technology company? Are there any obligations that, if breached, could result in a reversion of rights back to the third party?
- Have necessary registrations been made and transfers recorded with the appropriate agency?
- Has the technology asset been used to secure performance of any obligations or are they encumbered by any security interests or liens?
- Do third parties hold any licence rights, joint ownership rights or other rights in the technology asset?
- Is the technology asset substantially similar in function, appearance or coding to the technology asset of others?
- If proprietary materials and documentation of the company are held in escrow, what are the terms of the escrow arrangement (eg, conditions for release)?
- Are the technology assets sufficient to operate the licences?
- Are there any restrictions on the company's technology assets (eg, exclusive rights of first refusal or negotiation, non-competition, pricing restrictions, no-assignment or change-of-control provisions)?

The answer to these questions may affect the value of the technology asset to be acquired and be determining for the decision whether or not to acquire the target company or the technology asset at all.

Another specific area of due diligence that is typically conducted in a technology M&A transaction is privacy and cybersecurity due diligence.

If a target's data processing activities are not in line with applicable data protection laws, this entails major risks for the buyers. Violations of data protection laws within the European Union are, since the adoption of the General Data Protection Regulation (GDPR), subject to fines up to €20 million or up to 4 per cent of the total worldwide annual turnover.

Recent high-profile data breaches on companies like Yahoo!, Equifax, Target, Anthem, Uber, Facebook and British Airways have highlighted the risks associated with data security. Data breaches subject companies to significant liability arising from shareholder lawsuits, government investigations, remediation costs and reputational damages. According to Juniper Research, the global cost of data breaches will rise to US$5 trillion by 2024. Moreover, national data protection authorities (including the Belgian Data Protection Authority) have been delivering already a substantial number of decisions and have been imposing very high fines in 2019–2020, which show the importance of the GDPR in general.

Without sufficiently evaluating whether a target is compliant with data protection requirements, buyers risk acquiring a non-compliant business and thus buying into the hazard of serious fines or lawsuits from data subjects.

The only way to understand and mitigate these data protection risks is a comprehensive evaluation of the target. At best, identified non-compliance can be cured prior to closing (eg, by immediate actions of the target curing non-compliant behaviour itself). Where this is not possible or feasible, the identified non-compliance can at least be factored into the risk assessment and valuation in the course of the purchase decision.

To assess a target's data protection compliance status, the following documents should be requested by purchasers (provided by the seller) in the due diligence process:

- a record of processing activities (to verify that all of the target's processing activities were for lawful purposes and whether the data can be processed for other purposes);
- relevant data protection documents (eg, privacy notices, guidelines, works council agreements, consent forms, data-processing agreements, joint controller agreements and data-sharing agreements);
- IT, data protection and security concept, documentation of technical and organisational measures;
- an expert session with data protection officers or other informed experts, and possibly the contract, description of tasks and place in the target's organisational chart of the data protection officer;
- documentation of data protection-related self-assessment (eg, on a balance-of-interests test);
- a presentation of data protection organisation and data protection processes (in particular, relating to handling data subjects' requests or the deletion of personal data);
- documentation of all personal data breaches and evidence of related communications with the data protection authorities and the data subjects;
- any data protection impact assessments carried out;
- proof that IT programs used by the target are GDPR-compliant (eg, human resources, payroll software, monitoring equipment and geolocation equipment);
- cybersecurity policies and response policies;
- information on all regulatory or criminal proceedings in relation to data protection issues (eg, correspondence with data protection authorities);
- information on all other disputes with data subjects (eg, civil claims);
- supporting documents that the target secured all essential rights to commercially use personal data and only for current or also for new purposes (eg, provisions in general terms and conditions, individual contracts, in the supply chain); and
- data privacy or cybersecurity insurance coverage.

Also relevant in this context may be the target's compliance with the Belgian Network and Information Security Act of 7 April 2019 (the NIS Act) which applies to operators of essential services such as energy, transportation, banking and health, but also to providers of digital infrastructure (including providers of digital services such as online sales platforms, search engines and cloud computing services). The NIS Act provides for higher cybersecurity standards in these sectors and also includes obligations with regard to data protection and procedures in case of data breaches, whereby this data does not only compass personal data. Its scope is therefore broader than that of the GDPR.

A third area of specific due diligence that may be more relevant in technology M&A transactions involves the IT systems (eg, encryption, restriction of access, passwords and the safeguarding of sensitive data). IT systems will include hardware and software. With respect to hardware, relevant due diligence information could include:

- diagrams of the hardware infrastructure;
- an inventory of the relevant hardware assets;
- relevant third-party agreements (eg, vendor maintenance agreements); and
- possible disaster recovery and business continuity protocols.

With respect to software assets, relevant due diligence could include:

- an inventory of software used by the target, including information on ownership and licences;
- agreements related to software assets, such as licences, support, maintenance, development, assignment and escrow agreements;
- documentation, including policies, manuals and information on user access protocols; and
- active or planned development programs.

With respect to the IT systems, buyers should check that:

- they are free of bugs;
- they have not had any material security breaches;
- they have not had any material outages affecting business;
- they are in fair condition and sufficient for the normal functioning of the business;
- all necessary licences are in place;
- the maintenance and support agreements are still running; and
- adequate IT investments are budgeted to meet the business plan and be compliant.

This due diligence is usually undertaken by the chief information officer of the buyer and his or her team, who should be involved from the beginning on a technology M&A transaction.

A final area of due diligence that may be more relevant in technology M&A transactions relates to websites, web shops and social media assets. Privacy policies, disclaimers, general terms and conditions, supply and logistics agreements, compliance with applicable laws (eg, information obligations, advertising), investigations, complaints and disputes involving such assets may need to be reviewed.

The focus of the legal due diligence will vary slightly depending on whether the ultimate transaction is an asset or a share purchase. In an asset purchase the buyer will, of course, only focus on the assets it will purchase. Where, in general, the due diligence in an asset purchase transaction is not as demanding as in a share purchase transaction, in a technology M&A transaction, special attention will have to be given to the transferability of the IP vested in the sellers' technology assets (eg, the formalities required to transfer IP or a lack of assignment clauses in licensing agreements) or the transferability of certain data assets that qualify as personal data (eg, the data subject providing legal consent to the transfer).

Customary searches

5 What types of public searches are customarily performed when conducting technology M&A due diligence? What other types of publicly available information can be collected or reviewed in the conduct of technology M&A due diligence?

When conducting technology M&A, the buyer usually performs advanced trademark, domain name and patent searches, as further discussed below. This is in addition to standard public searches of publications in the annexes to the Belgian Official Journal, which include details on the appointments and resignation of directors, persons in charge of daily management, members of the management committee and, in some cases, proxy holders (but not shareholders). The Register of Ultimate Beneficial Owners will be consulted to find information on the shareholders and other persons which are in control of an entity (eg, through voting rights). Further, the company file, which will include the company's articles of association and other notarial deeds that have been enacted (eg, capital increases), and documents filed with the National Bank of Belgium (eg, annual accounts, report statutory auditor and annual report) should be with the registry of the commercial court.

Registrable intellectual property

6 What types of intellectual property are registrable, what types of intellectual property are not, and what due diligence is typically undertaken with respect to each?

Benelux trademarks (ie, trademarks that are valid in Belgium, the Netherlands and Luxembourg) can be registered with the Benelux Trademark Office in The Hague. European Trademarks can be registered with the EU Intellectual Property Office in Alicante, Spain. There is no separate Belgian trademark regime.

Patents can be registered with the Patent Section of the Intellectual Property Office of the Ministry of Economic Affairs or with the European Patent Office.

Benelux models and designs can be registered with the Benelux Models and Designs Office in The Hague. European Models and designs can be registered with the European Union Intellectual Property Office in Alicante. There is no separate Belgian models and designs regime. For European models and design, there is a separate mechanism in which no registration is required. Protection under this unregistered mechanism is, however, limited (up to a maximum of three years) and is subject to extra conditions.

Domain name registrations are not technically IP rights but are often addressed alongside IP registrations and applications. Belgian domain names can be registered with DNS Belgium. Top-level domain names can be registered with a whole range of international authorities.

In Belgium, copyright protection arises automatically as the work is created and published. No registration is required (or even possible). The same is true for trade secrets and know-how.

For IP that can be registered, the seller will usually conduct a worldwide search through appropriate databases or with the assistance of specialised IP offices. In addition, due diligence is conducted on the documents made available by the seller to the buyer, such as applications, licences and litigations. With respect to unregistered IP, such as copyright, know-how and trade secrets, buyers review all employment and third-party contractor agreements (including development contracts, confidentiality agreements and non-disclosure agreements) to make sure they include property confidentiality and invention assignment clauses. Often, IP due diligence cannot be conducted by lawyers alone, as it is not always apparent from the legal documents whether the IP protection is strong or weak, is sufficient to operate the target's technology, and if other companies use similar IP.

Liens

7 Can liens or security interests be granted on intellectual property or technology assets, and if so, how do acquirers conduct due diligence on them?

With the increasing prominence of IP as a balance sheet asset, it is common for lenders to include IP as collateral in secured debt financing. Thus, the buyer needs to determine if the target has granted any liens or security interest on specific IP assets.

The most common types of IP over which security is granted are patents, trademarks, designs and models. Such rights qualify as intangible movable assets under Belgian law.

Traditionally, it was debated among legal scholars whether it is possible to create a valid possessory pledge on IP under Belgian law.

However, following the entry into force of the new Belgian act on security interests on movable assets on 1 January 2018, it is now possible to create a non-possessory registered pledge over IP, to the extent that the pledge act is not contrary to other legal provisions in which such pledge rights are regulated specifically.

A non-possessory registered pledge will be perfected by registering the pledge in the national pledge register (which is a public, online register). Such registration remains valid for 10 years. Upon release of the pledge, it should also be removed from the pledge register.

However, if any specific law imposes additional perfection requirements for certain IP rights, it is recommended to comply with such additional requirements as well. For example, certain pledges must also be notified to, or registered with, the relevant IP authorities or registration offices to become effective against third parties.

Under the new rules, it is (in theory) also possible to create on non-possessory pledge on software and source codes (to the extent such rights are transferable). Given that the pledge register is a public register, it is not recommended to register the source code in the pledge register. A generic description (eg, 'all kind of software and source codes developed by the pledgor', or a general description of the software without revealing the source code) is also allowed, as long as the object of the pledge is sufficiently determined or determinable.

When conducting due diligence, it is recommended to perform a search in the national pledge register and the relevant IP registers.

Employee IP due diligence

8 What due diligence is typically undertaken with respect to employee-created and contractor-created intellectual property and technology?

When performing due diligence on a target company, the following documents are to be screened on specific clauses (eg, secrecy or confidentiality clauses, IP clauses, etc) to assess the ownership and assignment of the target company's IP rights:

- with respect to its employees:
  - individual employment contracts (or covenants thereto);
  - work regulations, codes of conduct, policies and any document holding unilateral instructions; and
  - guidelines, approvals or waivers pertaining to IP rights (eg, notices or brochures); and
- with respect to its contractors, service or consultancy agreements (or covenants).

Belgian employment law also provides two types of protection for company secrets (including IP):

- Workers are forbidden from divulging any company secrets that they may learn during their professional activity. This ban is imposed on workers during and after the employment contract. Violating this obligation is considered misconduct and may lead to

the immediate dismissal of the worker or to a claim for damages after the employment has terminated (article 17 (3) of the Act of 3 July 1978 on Employment Contracts).
- A worker who divulges an industrial or fabrication secret may also commit a criminal offence, which is punishable with imprisonment and a fine (article 309 of the Belgian Penal Code), although this is rarely applied.

The Belgian Code of Economic Law (articles XI.336/1 to XI.336/5) defines 'company secrets' as information that is not publicly known or not easily accessible, possesses a trade value, and has been submitted to reasonable measures to maintain its secrecy (eg, contractual clauses or physical or virtual security measures).

Depending on the nature of the activity of the employer (the principal) and the type of industry, employment contracts or service agreements customarily contain specific IP (transfer) clauses.

A distinction must be made between moral and patrimonial (economic) rights. The moral rights (eg, the right to be named as author or the right to claim or refuse the paternity of an invention) of employee-created IP or technology are not transferable, and so always belong to the employee, but patrimonial rights (eg, the right of reproduction or use of the IP or technology) can be transferred to the employer.

Patent

The employer and the employee are free to set forth any IP rights transfer clauses in an employment contract (or in a separate agreement). Except where an agreement expressly states otherwise, an invention is understood to be one of the following:
- A work invention: an invention developed within the worker's attributions, as described in his or her job description and while using the employer's resources. Such an invention is owned by the employer.
- A free invention: an invention made by the employee on his or her own, with his or her own means, and outside his or her attributions. Such an invention is owned by the employee.
- A dependent invention, such as:
  - an invention of a hybrid or mixed type; or
  - an invention made by an employee outside the performance of an employment contract, but using company resources. Inventions of this kind are mostly considered to be owned by the employee, although this is disputed in case law.

It is recommended to insert a clause in an employment contract that the employer will own such inventions and will be entitled to file for patent protection, possibly with a compensation method for the employee.

Similar language will be required in contracts with independent contractors. Failing that, any inventions made by independent contractors will be owned by them.

Trademark

Trademarks always belong to the natural person or legal entity on behalf of which the trademark is registered. Any transfer must be agreed in writing and registered with the relevant trademark office.

Computer software and databases

Under the Belgian Code of Economic Law (articles XI.187 and XI.296) there is a legal presumption of transfer of IP rights on the computer software and databases to the employer, if the software or database is created during the execution of the employee's functions or following the employer's instructions, unless otherwise agreed.

Transferring licensed intellectual property

9 Are there any requirements to enable the transfer or assignment of licensed intellectual property and technology? Are exclusive and non-exclusive licences treated differently?

In some cases, the technology or IP assets to be acquired in a technology M&A transaction will be subject to certain contractual provisions that either limit the buyer's ability to exploit those assets or the IP as expected, or prevent any transfer of the technology assets or IP altogether. The following are the most common examples of scenarios leading to these unfortunate results:
- the target company has granted a third party a licence to use its IP and:
  - the licence is exclusive with respect to a particular field of use or territory, precluding the buyer from exploiting the IP in overlapping fields of use or territories that may be key to the buyer's business; or
  - the licence is non-exclusive, but grants the licensee either an option to convert to an exclusive licence or a right of first refusal in the event of a pending acquisition; or
  - the target company has licensed certain IP assets from a third party; and
  - the licence grants only non-exclusive rights to the target, leaving open the possibility that competitors will hold or be able to obtain a licence to the same IP, which the buyer may deem critical to the ongoing business;
- the third-party licensor has retained the exclusive right to use the IP within a particular field or territory;
- the licensed rights do not include the right to any improvements or enhancements of the licensed IP that would permit the licensor or third-party licensees of the licensor to develop new versions of the IP and compete with the buyer;
- the governing agreement requires continued payment of licence fees or royalties that will be the buyer's obligation post-acquisition;
- the licence terms do not allow for sublicensing of the IP, which may be critical to the buyer's intended business model; or
- the licence terms expressly prohibit assignment of the licence to the buyer.

It is, therefore, important to scrutinise all of the target company's agreements pursuant to which an IP licence is granted to or from a third party, focusing, in particular, on terms governing assignability and exclusivity, and to determine if any third-party consents or waivers must be requested as pre-closing conditions.

With respect to transferability, the IP or technology licence agreements can either contain a no-assignment or a change-of-control clause. A no-assignment clause usually prohibits the licensee from assigning any of its rights under the licence agreement except with the prior written consent of the licensor. This is usually triggered when there is an asset deal but not when there is a share deal. A change-of-control clause usually gives the licensor the right to terminate the licence agreement in the case of a change of control. This is usually triggered by a share deal but not by an asset deal. Usually, the buyer will require a written waiver or consent of the licensor as a pre-closing condition.

When there is a share deal and nothing is foreseen in the licence agreement, the licence agreement usually remains valid and no formalities must be fulfilled.

When there is an asset deal and a no-assignment clause is seen in the licence agreement, the licensed IP or technology can, in principle, be transferred by means of a written assignment agreement. Except in the case of copyright and know-how, the assignment must also be registered with the relevant agency, these being:

- trademarks:
  - the Benelux Trade Mark Office in the Hague; or
  - the Trade Marks Section of the Intellectual Property Office of the Ministry of Economic Affairs;
- patents:
  - the Patent Section of the Intellectual Property Office of the Ministry of Economic Affairs; or
  - the European Patent Office; and
- models and designs:
  - the Benelux Models and Designs Office in the Hague; or
  - the Models and Designs Section of the Intellectual Property Office of the Belgian Ministry of Economic Affairs.

Whether a licence agreement is exclusive should not change the treatment except that exclusive licences will more likely include no-assignment or change-of-control clauses and almost always require consent of the licensor with the assignment (asset deal) or change of control (share deal).

Software due diligence

10 What types of software due diligence is typically undertaken in your jurisdiction? Do targets customarily provide code scans for third-party or open source code?

First of all, the buyer should investigate the seller's rights in any proprietary software included in the purchased technology assets, particularly if the purchased software includes software that the seller licenses or distributes to customers, and software licensed from third parties that is not readily replaceable or is costly to replace.

For software created by or for the seller and included in the purchased assets, the buyer should confirm that all relevant rights have been assigned to the seller and can be conveyed to the buyer. In particular, if the software is created by a non-employee, it is important that all rights are expressly assigned to the seller.

For software licensed to the seller by third parties and included in the purchased assets, the buyer should ensure that the rights licensed to the seller are consistent with the rights the seller has licensed to its customers or other third parties. In particular, the buyer should confirm that, if the licensed rights are terminated, the applicable licences permit the buyer's customers to continue using the licensed software and the buyer continues to have the right to provide its customers with maintenance and support.

Further, for material third-party software licensed to the seller and included in the purchased assets, the buyer should determine whether the seller is either in possession of a copy of the source code or is party to a source code escrow agreement.

A source code escrow agreement gives the licensee access to and the right to modify the licensor's source code on the occurrence of certain conditions (eg, if the licensor enters bankruptcy or ceases operation and cannot continue providing maintenance and support).

Finally, it is customary for the buyer to ask the seller to show that the company understands the open-source applications it uses and to ask to document how open source code is used within the target and its products. Relevant due diligence information could include:

- policies and procedures;
- code reviews;
- searches for 'copyleft' and similar open source code use; and
- attribution and notice requirements.

Best practices for a growing amount of companies involved in a technology M&A transaction include an independent code audit whenever software is a significant part of the deal. Indeed, more and more firms are realising that an open source code audit also should be part of their overall due diligence process, as modern software development code is rarely written from scratch. Custom code now often comprises only 10 to 20 per cent of many applications, with the remainder being previously developed code, third-party code and, increasingly, open source code as the core foundation for applications. In fact, it appears that about 95 per cent of code bases contain undisclosed open source. Open source material may come with legal obligations in its licence agreements that go with the usage of that code. There also may be security vulnerabilities within the code as well as operational risks, such as versioning and duplications. Software audits identify open-source code and third-party components and licences, and may mitigate legal, operational and security issues. The software audit is mostly undertaken by the buyer, but can also be undertaken by the seller as part of its vendor due diligence to give assurance that it can give the strict IP representations and warranties that are usually required or mitigate certain risks.

So, buyers must carefully review whether the target has combined open-source code with proprietary software in a way that requires the software to be made publicly available under the open-source licence and evaluate the third-party code. Indeed, open-source software licences can be important in a proposed transaction as they may dictate the terms on which software derived from such open-source software is licensed to third parties. If the buyer is expecting to use the target company's technology exclusively, then discovering that the technology incorporates software that is subject to free-use rights could be a deal-breaker.

Other due diligence

11 What are the additional areas of due diligence undertaken or unique legal considerations in your jurisdiction with respect to special or emerging technologies?

The focus of the due diligence approach set out above is on a traditional IT environment. IT is increasingly being acquired as 'software as a service' or in the context of cloud computing. Where a target engages or makes use of such services, this category of agreements will require separate and careful consideration. When acquiring or merging with a provider of cloud applications, platforms or infrastructure in the cloud, special attention should be paid to issues such as the ownership of the data or applications run in the cloud, compliance with mandatory rules with respect to international data transfers and exit possibilities.

Machine learning, deep learning, neural networks and other forms of artificial intelligence (AI) are often already an integral part of a target's business operations when conducting technology M&A. When conducting the due diligence and drafting M&A documentation in relation to an AI company, buyers should give special attention to:

- the IP protection of data sets and algorithms (eg, copyright, trade secrets and patents);
- ownership of IP developed by AI;
- ownership of content generated by AI;
- licensing, liability and regulatory issues;
- privacy; and
- cybersecurity.

Attention should be paid to the developments in the European Commission, which has created a Coordinated EU Plan on Artificial Intelligence and published the White Paper on Artificial Intelligence in February 2020, so that Europe can become a world leader in this technology, but with AI based on ethics and European values.

Internet of things (IoT) devices often contain components of different manufacturers. They are often low-price devices with low levels of security. So, when acquiring manufacturers or operators of IoT devices buyers should properly review liability, IP, privacy, IT security and consumer protection (such as the new digital sales rules) issues. However, IoT could also raise additional environmental (eg, waste management) or health and safety issues.

Key technologies relating to autonomous or semi-autonomous driving include automated automotive technologies, collision avoidance technologies, artificial intelligence and machine learning, and others. When acquiring companies in this field, sellers should focus on the ownership of these technologies (eg, patents and trade secrets), ownership of data, regulatory issues (eg, government authorisations and test results) and insurance.

If a target is involved with big data, the seller should, during its due diligence, prioritise the following areas of the target's business operations related to information and its related risks and liabilities:

- data privacy;
- data security;
- information governance;
- regulatory inquiries; and
- insurance policies covering information-related topics (including data breach and infected system issues).

PURCHASE AGREEMENT

Representations and warranties

12 In technology M&A transactions, is it customary to include representations and warranties for intellectual property, technology, cybersecurity or data privacy?

Buyers will want to confirm that the seller is the sole and exclusive owner of the IP it is selling and that the IP is not limited or subject to any encumbrances. The buyer will also want to ensure that the seller has the appropriate licences for any third-party IP and that the seller is not subject to any pending or threatened legal proceedings challenging its IP rights.

Examples of matters that may limit a buyer's ability to exploit any IP it acquires and for which buyers typically require representations and warranties include:

- claims by third parties that patents are invalid or infringe on their patent rights;
- liens on the IP;
- invalid evidence that contractors or third parties have assigned their rights to any property they helped create;
- rights of first refusal or exclusivity in favour of third parties;
- failure to obtain consents of third parties;
- failure to properly register the IP;
- restrictions in inbound or outbound licences; and
- issues with open source material where the IP is in the public domain.

Buyers typically want a warranty that the seller's business does not infringe, misappropriate or violate any other party's IP rights and that no other party is infringing the seller's rights. They will also want a warranty that there is no litigation or claims pending or threatened that may happen post-closing.

To the extent that it is not possible to eliminate data protection risks in the due diligence phase before signing, adequate data protection warranties should be included in the purchase agreement. These representations vary, but often cover:

- compliance with privacy laws (eg, due respect for the rights of data subjects and the effective possibility for the data subjects to exercise those rights), industry-specific security standards and contractual requirements, and terms of use relating to personal data;
- implementation of security measures in relation to information technology assets (eg, industry-standard security measures);
- detection of data-related claims or complaints and compliance investigations;
- disaster recovery plans and back-up procedures;
- disclosure of arrangements under which data is placed with or by third parties (eg, data processing agreements);
- absences of loss or unauthorised access of personal data in the past (whether or not constituting a violation of the law at the time); and
- a security assessment and remediation of any gaps.

One consideration could be to treat data protection similarly to environmental risks in the share-purchase agreement, including a potential audit to establish a baseline and remediation process.

Data protection representations and warranties referring to the knowledge of the target should only be accepted by the purchaser if a sufficient level of data protection organisation at the level of the target can be verified in the due diligence phase. The characteristics of a sufficient data protection organisation should include, in particular, appropriate technical and organisational measures to reduce the likelihood of protection violations right from the start.

The definitive agreement should contain representations and warranties that take into account all IP-related and data-related risks discovered during the due diligence and the seller's or the target's indemnification obligations for any breach of those representations and warranties. The definitive agreement should also contain carefully drafted disclosure schedules that list the IP assets or data assets being acquired and any exceptions to or encumbrances on that IP or those data.

Sellers from their side will try to limit the scope of these representations and warranties by including materiality qualifiers and knowledge qualifiers, by limiting representations and by limiting any ambiguous representations.

Customary ancillary agreements

13 What types of ancillary agreements are customary in a carveout or asset sale?

In a technology M&A transaction where the buyer is acquiring less than all of the seller's business, it may be necessary for the seller to provide the buyer with a transitional trademark licence to allow the buyer to use some of the seller's retained IP for a limited period of time and a specified use. This situation often arises where the seller has sold a part of its business, such as a business unit or division, and the buyer seeks use of the seller's retained trademarks until the buyer can transition the related products or services to new trademarks.

A cross-licensing agreement is a contractual arrangement between two or more parties in which each party is granted rights to a piece of technology, product, research or other subject. Cross-licences generally occur between companies that hold patents over different aspects of the same product or when different aspects of a technology are protected by different forms of IP (eg, when the copyright of the software is owned by one party and the patent rights with respect to the hardware are owned by the party that developed the hardware). Cross-licences allow the buyer and the seller of a technology to use a particular technology even if they do not own all the IP ownership relating to that technology (eg, when only part of a business is sold).

When a company is sold in an M&A transaction and the seller is expected to continue to provide services to support the post-closing company, the parties to the transaction enter into a transition services agreement (TSA), which governs the provision of such services to the post-closing company. Depending upon the complexity of the transition services arrangement and the criticality of the services being provided, TSAs can range from short, back-office administration services agreements with an agreement to set fees in the future and no formal performance standards, to comprehensive service agreements with defined scopes, service levels, variable fee arrangements, and detailed

data security and privacy provisions. The transitional services might include finance and accounting, human resources, information technology and procurement. The objective is to ensure business continuity while the new company establishes its own internal capabilities or to transition these services to a third-party vendor.

A technology M&A transaction may also require various ancillary agreements dealing with personal data including:

- a transitional services agreement dealing with post-closing data integration and services;
- a data-sharing agreement to govern data transfers pre-closing; and
- where appropriate, other licensing and data processing agreements for the operation of the business post-closing.

Conditions and covenants

14 What kinds of intellectual property or tech-related pre- or post-closing conditions or covenants do acquirers typically require?

If there is a time gap between signing and closing, the definitive agreement typically foresees that the seller covenants that it must conduct its or, where the seller itself is not the target company, the target company's business as usual until closing. Known as the 'interim operating covenant', this assures the buyer that the target business is operated in the ordinary course of business and is in the same condition and of the same value at closing as when the buyer conducted its due diligence and appraisal of the target business. The interim operating covenant may include a list of specific actions before closing that the seller must take, not take or not take without the buyer's consent. This list depends on the industry of the target company and deal-specific factors.

Common interim operating covenants relating to IP include not licensing, encumbering, assigning or otherwise disposing of any IP assets of the target business; and making necessary filings and payments to maintain the status of the target business's registered IP.

Other common IP-related pre-closing covenants include making necessary filings to record the release of security interests or update the chain-of-title of registered IP; executing and delivering IP assignment documents, including assignments suitable for recording with the applicable government authorities; and authorising the transfer of domain names with the applicable registrars.

Management of the seller, together with IP counsel, will need to consider the extent to which the company can comply with these covenants without harming the company and its business. If possible, the definitive agreement should provide that if the seller determines that it must deviate from any of these covenants, the consent of the buyer to such deviation should not be unreasonably withheld, delayed or conditioned. A lengthy pre-closing period is more likely to invoke these issues than a relatively shorter pre-closing period.

The parties may also include post-closing covenants in the definitive agreement to cover the licence or transfer of specific IP or IT rights or the performance of specified services after the closing. In a carveout transaction, these covenants may address the following.

Licences to retained or shared IP

the buyer may seek a licence or covenant from the seller to not sue relating to the buyer's use of IP used in the target business that the seller intends to retain after closing.

A transfer of know-how

If certain key employees with knowledge of IP or IT matters are not being transferred with the acquired business, the buyer may require the seller to make the retained employees available for consultation or training for a limited time after the closing to ensure that all know-how associated with the purchased assets is actually transferred to the buyer.

Separation or replacement of shared IT contracts

In addition to any transitional assistance that the seller may provide, or cause to be provided to the buyer under a separate transition services agreement, the buyer may seek to include a post-closing covenant in the purchase agreement requiring the seller to provide assistance in negotiating replacement licences or support agreements for enterprise systems and other software or IT services that are retained by the target company for continued use in its business and may not be covered under the transition services agreement.

Survival period

15 Are intellectual property representations and warranties typically subject to longer survival periods than other representations and warranties?

Buyers typically prefer to lengthen the period in which they may bring claims against the seller post-closing relating to breaches of warranties relating to IP because, in their view, the acquisition of a technology company is substantially an acquisition of the company's IP.

Deal studies show that in 5 to 10 per cent of Belgian transactions there is a longer survival period for IP representations and warranties. However, in technology M&A transactions, this percentage is probably substantially higher.

Breach of representations and warranties

16 Are liabilities for breach of intellectual property representations and warranties typically subject to a cap that is higher than the liability cap for breach of other representations and warranties?

In general, we see maximum cap carveouts in respect of liabilities for breaches of IP representations and warranties in 5 to 15 per cent of all M&A transactions. In technology M&A transactions, this percentage is substantially higher, sometimes 30 to 50 per cent. Whereas, usually, the general maximum liability cap is in the range of 30 to 40 per cent, for breaches of IP representations and warranties, the maximum liability cap is set at 100 per cent of the purchase price. In most cases, the sellers will not want to sell if there is no cap on their liability.

Often there is no general maximum cap carveout with respect to liabilities for breaches of IP representations and warranties, but specific indemnities are foreseen for specific IP risks established during the due diligence. Certainly, if there are financial investors among the sellers, a compromise may be to foresee warranty and indemnity insurance as these financial investors are usually not prepared to accept the high maximum liability caps and lengthy survival periods that technology investors sometimes require. However, warranty and indemnity insurance is not a substitution for due diligence or disclosure schedules and, in most cases, risks identified through these processes will be excluded from standard warranty and indemnity insurance.

17 Are liabilities for breach of intellectual property representations subject to, or carved out from, de minimis thresholds, baskets, or deductibles or other limitations on recovery?

Usually, liabilities for breach of IP representations are not carved out from, and thus are not subject to, de minimis thresholds, baskets or deductibles, unless a specific IP risk is established during the due diligence and a specific indemnity is included in the definitive agreement. In that case, the buyer will be indemnified euro-by-euro if this risk materialises.

Owing to potentially high fines arising from the General Data Protection Regulation (GDPR), reputational issues and claims from data subjects, from the perspective of the buyer, no financial caps, or, at least,

higher financial caps, should be agreed with regard to the data representations and warranties. Experience shows that Belgian sellers usually require some form of maximum cap. If there are specific data-related risks, ideally they should be remedied before closing or alternatively covered by specific indemnities. Breaches of specific indemnities are generally excluded from the calculation of de minimis and basket thresholds or deductibles.

Indemnities

18 Does the definitive agreement customarily include specific indemnities related to intellectual property, data security or privacy matters?

Ongoing IP litigation is a classic example of a situation where it may be reasonable for the seller to offer a specific indemnity. Identified IP risks where there is a certain likelihood of costs for the company at some point in time after closing the deal, are also often subject to specific indemnities. Often a definitive agreement in a transaction where IP constitutes a company's core value will contain a general indemnity against third-party infringements of the IP that is at the heart of the technology sold, as no limitations and disclosures can be accepted against the warranty that the use of this technology does not infringe third-party IP.

Special indemnities may be foreseen for specific data-related liabilities established during the due diligence (eg, infringements of the GDPR or data breaches).

The buyers may also consider, based on their diligence, how the privacy and cybersecurity representations should be treated related to other representations. For example, for unknown privacy and cybersecurity problems, buyers can push for the privacy and cybersecurity representations to be treated as 'fundamental representations' so that they are not subject to the same survival, caps and baskets limitations as non-fundamental representations. And for either known or unknown cyber risks, buyers could negotiate for a 'specific indemnity', subject to a separate set of limitations and methods of recovery.

Walk rights

19 As a closing condition, are intellectual property representations and warranties required to be true in all respects, in all material respects, or except as would not cause a material adverse effect?

As IP is usually one of the core assets in a technology M&A transaction, buyers usually require, as a closing condition, that the IP representations and warranties are true in all respects and do not accept any materiality qualifier or material adverse effect-clause with respect to such representations and warranties. Buyers will usually want a 'walk-away right' with respect to breaches on the IP representations occurring between signing and closing that does not preclude that they may waive this 'walk right' if, after due diligence of the breach, it only appears to be a minor breach.

UPDATES AND TRENDS

Key developments of the past year

20 What were the key cases, decisions, judgments and policy and legislative developments of the past year?

We see the most developments taking place in the field of data protection, where the last year has brought many important decisions from the national data protection authorities in the European Union member states with regard to the General Data Protection Regulation (GDPR). These make it possible for practitioners to better understand the privacy risks in targets, together with the guidance of the European Data Protection Board.

astrea

Steven De Schrijver
sds@astrealaw.be

Rudi Desmet
rds@astrealaw.be

Louizalaan 235
1050 Brussels
Belgium
Tel: +32 2 215 97 58
Fax: +32 2 216 50 91

Posthofbrug 6
2600 Antwerp
Belgium
Tel: +32 3 287 11 11
Fax: +32 3 287 11 12

www.astrealaw.be

In addition, a recent decision of the European Court of Justice invalidated the EU–US Privacy Shield, under which data could be transferred to the US, but maintained the validity of standard corporate clauses under certain circumstances. This decision may create raise many practical questions on EU–US data transfers in the coming months.

With regard to IP, the most important changes will take place in copyright law, pursuant to Directive 2019/79 on copyright and related rights in the Digital Single Market, which must be transposed into the national law of the member states by 7 June 2021.

Coronavirus

21 What emergency legislation, relief programmes and other initiatives specific to your practice area has your state implemented to address the pandemic? Have any existing government programs, laws or regulations been amended to address these concerns? What best practices are advisable for clients?

There are no specific relief programmes or other initiatives with regard to technology M&A in Belgium, but various general measures (such as the implementation of economic unemployment (during which the employee receives unemployment benefits due to a lack of work at the employer), forced closure of certain businesses, etc) must be taken into account in the due diligence process. The purchaser should carefully assess whether the target complies with covid-19 measures (such as social distancing rules), whether the target and its counterparties can perform their obligations under material contracts, the effectiveness of contingency and crisis management procedures and whether there are potential breaches of material contracts (including financial agreements), etc.

The transaction documents may also include specific provisions due to covid-19, such as:

- a more frequent use of deferred purchase price mechanisms;
- material adverse change clauses (it is important to expressly include covid-19 as a material adverse change);

- interim operating covenants applying between signing and closing;
- specific representations and warranties on covid-19; and
- specific termination rights.