Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

Outsourcing

Second Edition

Belgium
Crowell & Moring LLP

chambers.com

2019

Law and Practice

Contributed by Crowell & Moring LLP

Contents

Crowell & Moring LLP is an international firm of approximately 550 lawyers with offices in Washington, DC, New York, Los Angeles, San Francisco, Orange County, London and Brussels. The Brussels office has 30 lawyers in its cross-disciplinary team and relies on EU and US colleagues for international matters. Crowell & Moring Brussels combines experience in drafting and negotiating complex agreements with employment, M&A and GDPR capabilities. Representative matters include complex contract drafting and negotiating for a US multinational's Belgian operation that outsourced all but its core activities to a facility services provider, as well as advice on the HR and GDPR consequences of outsourcing. The firm also handles transition service arrangements, supply, distribution, manufacturing, group purchasing and e-commerce agreements. The authors are very grateful to the Brussels cross-disciplinary team for their help in compiling this chapter. They extend special thanks to two other members of the team whose contribution has been invaluable: Stephanie Michiels (associate) and Evelien Jamaels (associate).

Authors

Emmanuel Plasschaert is a partner, and co-head of the Crowell & Moring Brussels' corporate, commercial and employment practice. Emmanuel's primary focus is on international employment law, but he also regularly advises on corporate transactions. He is highly regarded for his employment law counselling and his advice on complex restructurings, corporate transactions and HR data protection issues. Emmanuel has significant experience in commercial matters and has represented clients in complex litigation for more than 25 years. Emmanuel has published widely. He is currently preparing a book regarding Transfer of Undertakings.

Frederik Van Remoortel is a partner at Crowell & Moring Brussels and co-heads the corporate, commercial and employment practice, and the data protection practice. He handles corporate transactional matters including acquisitions, mergers, joint ventures, and other collaborative arrangements. He drafts and negotiates a wide variety of commercial contracts, including outsourcing, shareholders, asset transfer, licensing and distribution, agency, software and cloud computing, telecommunications, supply, independent contractors and lease agreements. Frederik advises on data protection legislation, including GDPR. He is a Certified Information Privacy Professional/Europe (CIPP/E) and former member of the IAPP European Advisory Board (2015-2016). Frederik has published widely.

Karl Stas is a counsel in the Crowell & Moring Brussels' office. He focuses on EU and Belgian competition law and on the regulation of network industries (eg, telecommunications, postal and energy). He is an experienced litigator and has represented clients before the European Commission and national regulatory bodies, as well as before all the Belgian courts and the Court of Justice of the European Union. Karl has particular knowledge of industry specific restrictions and compliance issues related to outsourcing, for example in the banking and insurance sectors. Karl publishes frequently on Competition and Regulatory Law.

Heidi Waem is a counsel in Crowell & Moring's Brussels office. She focuses on privacy and data protection (eg, GDPR), contract law, market practices and consumer law, and IP/IT. Heidi advises clients on the establishment of a comprehensive data protection framework, on data transfers and, in the case of data breach, on pre-litigation issues involving data subject complaints and requests. She also represents clients in proceedings before the data protection authority. She also reviews, drafts, and negotiates a wide variety of contracts, including agreements for consultancy, collaboration, maintenance and supply, software development and licenses, funded research projects and R&D. Heidi has published widely.

1. Outsourcing Market

1.1 IT Outsourcing
The key market developments in IT outsourcing are as follows:

- The IT outsourcing market continues to grow. According to the 2019 BeLux IT Sourcing Study by Whitelane Research, the BeLux region has the highest growth in comparison to the rest of Europe and is 12% above the European average of 38%.
- Although, globally, Asia remains a strong market for IT outsourcing, this market is steadily growing in Europe, and in particular in countries such as Romania and Ukraine.

1.2 BP Outsourcing
The key market developments in Business Process (BP) outsourcing are as follows:

- Customer services offered by BP outsourcing companies are extended to include social media management. In general, there is a further diversification of the services.
- For BP outsourcing companies, the introduction of new technologies (see **1.3 New Technology**) directly affects their business model where software is replacing manual tasks outsourced by their clients.
- There is a continuous increase in the adoption of cloud and Service as a Service (SaaS) by BP outsourcing companies.
- Certain vendors are now offering Business Process as a Service (BPaaS) solutions for analytical services.

1.3 New Technology
New technologies such as robotics and artificial intelligence will help outsourcing providers to further automate processes and to achieve cost reduction and quality improvement at the same time.

The adoption of new technologies may lead to a new form of digital outsourcing whereby the services are mainly performed by machines instead of humans.

1.4 Other Key Market Trends
The 2019 BeLux IT Sourcing Study by Whitelane Research shows that the agile approach (ie, an innovative approach to software development project management) is the preferred working model in the BeLux with more than 50% of organisations using it and 33% planning to do so.

The General Data Protection Regulation (GDPR) has an impact on outsourcing contracts. Suppliers that qualify as processors must enter into data processing agreements with their customers. Such agreements must include a number of mandatory clauses.

Given the continuous stream of cybersecurity incidents and data breaches worldwide, cybersecurity is one of the main concerns of customers.

For repetitive tasks such as indexing of images, companies are resorting to crowdsourcing platforms.

2. Regulatory and Legal Environment

2.1 Legal and Regulatory Restrictions on Outsourcing
There are no legal or regulatory restrictions which apply specifically to outsourcing, except in certain sectors (see **2.2 Industry Specific Restrictions**).

Outsourcing agreements in the public sector are subject to public procurement law (ie, the Public Procurement Law of 17 June 2016 and its implementing regulations). Note that some private entities (eg, utilities, hospitals, and educational institutions) may also be subject to public procurement rules.

If an outsourcing transaction is structured as a joint venture (JV) between the outsourcing customer and the supplier, with the outsourcing customer contributing personnel and assets to the JV, this may under certain conditions trigger an obligation to make a merger filing to the relevant competition authority (ie, either the Belgian Competition Authority or the European Commission, depending on whether the Belgian or the European notification thresholds are met) and to refrain from implementing the transaction while it is being reviewed by this authority. This may, in particular, be the case if the JV partners, for example, for reasons of economies of scale, intend the JV to have significant non-captive sales and the JV therefore qualifies as a "full-function" JV with independent market access. However, typically the JV is set up to exclusively supply the outsourcing customer and therefore does not qualify as full-function, so no merger filing is required.

In addition to any applicable legal and regulatory restrictions, outsourcing customers may of course contractually stipulate that the supplier must comply with additional requirements, such as industry standards (eg, ISO standards).

2.2 Industry Specific Restrictions
There are specific restrictions on outsourcing in the banking and insurance sectors. In both cases, the general principle is that the financial institution or insurance company remains fully responsible for all its activities at all times, including activities outsourced to third parties. Outsourcing must not impair the quality of internal controls or the supervision by the competent authorities. The investigative powers of the supervising authorities also extend to third-party outsourcing providers of the institutions within their purview.

We should also mention that in the area of settlement and clearing services, similar requirements regarding outsourcing also apply to central securities depositories (CSDs) pursuant to Regulation 909/2014 on improving securities settlement in the European Union and on central securities depositories, as well as to central counterparties (CCPs) pursuant to Regulation 648/2012 on OTC derivatives, central counterparties and trade repositories. These Regulations are directly applicable in Belgium.

Banking

The Belgian regulation of the banking sector is largely driven by EU legislation, in particular Directive 2013/35/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms (the Capital Requirements Directive or CRD); Directive 2014/65/EU on markets and financial instruments (MiFID II); Directive 2105/2366/EU on payment services in the internal market (the revised Payment Services Directive or PSD2) and Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions (the e-Money Directive). MiFID II contains specific provisions regarding the outsourcing of functions in the field of investment services and activities, whereas the PSD2 sets out requirements for the outsourcing of functions by payment institutions.

Note that Belgium has adopted a so-called "Twin Peaks" model of supervision over the financial sector, with two supervising authorities, the Belgian National Bank and the Financial Services and Markets Authority (FSMA). The Belgian National Bank is responsible for the micro-prudential, macro-prudential and systemic supervision, whereas the FSMA is responsible for the supervision over the rules of conduct of financial intermediaries in their relationship with clients.

Article 66 of the Law on the Legal Status and the Supervision of Credit Institutions and Listed Companies (the Banking Act) provides that when a credit institution outsources tasks to a third party which are of critical importance for a continuous and satisfactory provision of services – in particular as regards investment services and activities – it shall take appropriate measures to limit the operational risks this entails. Outsourcing must not impair the appropriate nature of the internal supervision procedures of the institution or the ability of the supervising authority, ie, the FSMA, to verify whether the credit institution complies with its legal and regulatory obligations (see also Article 16.5 MiFID II). After obtaining the advice of the FSMA, the bank shall publish a declaration setting out its policy in relation to outsourcing of portfolio management services for non-professional clients. Furthermore, Article 39/1 of the Banking Act provides that every credit institution must guarantee in an audit charter at a minimum that the internal audit function is independent and that its purview extends to all activities and entities of the institution, even in case of outsourcing.

Articles 38 and 195 of the Law of 11 March 2018 concerning the legal status of and supervision of payment institutions and electronic money institutions, which transposes the PSD2 and the e-Money Directive, provide that payment institutions and electronic money institutions which outsource functions, activities or operational tasks, remain fully responsible for the compliance with the Law as well as with the implementing measures of PSD2 and the e-Money Directive. Outsourcing of operational tasks, in particular if they are important, must not:

- impair the quality of the organisation and in particular the quality of the internal control mechanisms of the institution;
- lead to an unnecessary increase of the operational risk;
- impair the ability of the supervising authority, in this case the Belgian National Bank, to monitor the institutions' compliance with its legal and regulatory obligations; or
- undermine the continuity and adequacy of the service provision to the payment service users.

Prior to outsourcing any "important" or "critical" functions, activities or operational tasks, the institutions must inform the National Bank. The Bank can make the contemplated outsourcing subject to conditions or restrictions.

On 25 February 2019, the European Banking Authority (EBA) published revised Guidelines on outsourcing arrangements. The deadline for compliance is 5 September 2019 and the Guidelines enter into force on 30 September 2019. At the same time, the EBA's 2006 guidelines on outsourcing and its recommendation on outsourcing to cloud service providers will be repealed. The Guidelines cover credit institutions and investment firms subject to the CRD, payment institutions subject to PSD2 and electronic money institutions subject to the e-Money Directive. They set out which arrangements with third parties are to be considered as outsourcing and provide criteria for the identification of critical or important functions that have a strong impact on the financial institution's risk profile or on its internal control framework. If such critical or important functions are outsourced, stricter requirements apply to these outsourcing arrangements than to other outsourcing arrangements. In order to allow the competent authorities to effectively supervise financial institutions' outsourcing arrangements, they are required to extensively document such arrangements. Additional safeguards are required for outsourcing to third countries (outside of the EU), to ensure compliance with EU rules and effective supervision over the outsourced activities by the competent authorities.

The FSMA, its predecessor the CBFA (Commission for the Banking, Finance and Insurance Sectors) as well as the

Belgian National Bank have issued several Circulars and other guidance documents that are relevant to outsourcing arrangements, including outsourcing of IT services (eg, CBFA Circular PPB 2004/5 on sound management practices in case of outsourcing by credit institutions and investment companies; NBB Circular 2018/20 on outsourcing to providers of cloud services, etc).

Insurance

Directive 2009/138/EC on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II Directive) contains specific provisions on outsourcing of functions by insurers. These were transposed into Belgian Law by the Law of 4 April 2014 on Insurance (the Insurance Act), and the Law of 13 March 2016 on the legal status and supervision of insurance or reinsurance undertakings (the Solvency II Law).

The Insurance Act transposes the consumer protection provisions of the Solvency II Directive, whereas the Solvency II Law transposes the provisions regarding the governance of insurance undertakings. In the "Twin Peaks" model of supervision over the financial and insurance sectors, the FSMA is the competent authority for the former, whereas the National Bank is the competent authority for the latter.

Article 16/2 of the Insurance Act provides that, where an insurance company outsources functions, activities or operational tasks, it remains fully responsible for the compliance with all its legal and regulatory obligations. The outsourcing must not impair the continuity and adequacy of the service provision to policyholders, insured persons and beneficiaries of insurance agreements. It must also not impair the ability of the FSMA to verify whether the insurance company complies with its legal or regulatory obligations. If the insurance company outsources functions, tasks or operational activities directly or indirectly related to its obligations under the Insurance Act or its implementing regulations, it must take the necessary measures to ensure that the following requirements are met: the outsourcing provider must co-operate with the FSMA in relation to the outsourced function or activity; the insurers, the auditors of the accounts and the FSMA must have effective access to the data concerning the outsourced functions or activities; and the FSMA must have effective access to the premises of the provider and be able to effectively exercise its inspection rights under the Act.

If the insurance company outsources the management of an investment fund linked to an insurance product, the following additional requirements must be complied with: the insurance company must be able to justify its entire delegation structure with objective arguments and the mandate may only be entrusted to institutions which are licensed or registered asset managers and subject to supervision or, if these conditions cannot be fulfilled, only with the FSMA's prior approval. In case of outsourcing to an undertaking established in a third country, the FSMA must have concluded a memorandum of understanding with the supervisory authority of that country. The insurer must be able to demonstrate that the delegate is qualified to accomplish the tasks entrusted to it, that the delegate was selected with the utmost care, that the insurer is able to supervise the delegate's activities continuously and effectively and to give it further instructions, and that the delegation can be revoked at all times if the interests of the insured persons or the beneficiaries so require. The insurer shall subject the services of each delegate to a continuous evaluation.

Article 92 of the Solvency II Law provides that any insurance or reinsurance undertaking which outsources functions, activities or operational tasks, remains fully responsible for the compliance with its obligations under the Law or any measures implementing the Solvency II Directive. The outsourcing of operational tasks must not entail:

- material impairment of the quality of the governance system of the insurance company;
- undue increase of the operational risk;
- impairment of the ability of the supervising authority (ie, the Belgian National Bank) to monitor compliance by the insurance undertaking with its obligations under or pursuant to the Solvency II Law; or
- undermining the continuous and satisfactory service to policy-holders, insured persons and beneficiaries of insurance policies or the persons concerned by the execution of reinsurance policies.

Pursuant to Article 274 of Commission Delegated Regulation 2015/35 supplementing the Solvency II Directive, any (re)insurance undertaking which outsources or proposes to outsource functions or (re)insurance activities to a service provider shall establish a written outsourcing policy which takes into account the impact of outsourcing on its business and the reporting and monitoring arrangements to be implemented in cases of outsourcing. In the case of outsourcing of "critical or important operational functions or activities", the Delegated Regulation sets out additional verifications that the management body of the insurance undertaking must perform when selecting a service provider, the minimum content of the written agreement with the service provider and additional requirements for the outsourcing (re)insurance undertaking itself.

The governance requirements regarding outsourcing by (re) insurers, including outsourcing of "critical and important operational functions or activities", are further specified in Chapter 7 of the Belgian National Bank's Overarching Governance System Circular.

An important governance rule regarding outsourcing by insurance undertakings is that the impact of outsourcing may not be of such a scale that the insurance company exhibits the characteristics of an "empty shell" that is no longer capable of complying with its conditions for authorisation and pursuit of business.

2.3 Legal or Regulatory Restrictions on Data Processing or Data Security

The European General Data Protection Regulation 2016/679 (GDPR) governs the processing of personal data and includes restrictions on data processing and data security. In addition, the Belgian Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data applies to the processing of personal data by:

- controllers or processors (both as defined below) established in Belgium; and
- entities established outside of the European Economic Area offering goods or services to data subjects in Belgium or monitoring their behaviour taking place in Belgium.

If the outsourcing entails the processing of personal data, the GDPR will need to be complied with. Customers or suppliers established in Belgium will also need to comply with the Belgian Act of 30 July 2018.

The GDPR applies to "controllers" and "processors" processing personal data.

A controller is defined as an entity that, alone or jointly with others, determines the purposes and the means of the processing of personal data.

A processor is defined as an entity that processes personal data on behalf of a controller.

The obligations vary depending on whether a company qualifies as a controller or a processor. In an outsourcing context, the supplier is typically considered a processor. However, this must always be assessed on a case-by-case basis.

Where the processing is carried out by a processor, the controller and processor must enter into a data processing agreement, which must contain a number of specific clauses.

The GDPR also contains restrictions with regard to the transfer of personal data which is particularly important in the context of outsourcing.

Under the GDPR, personal data may be freely transferred to countries within the European Economic Area and to countries for which the European Commission has issued an adequacy finding (Andorra, Argentina, Canada (entities covered by the Personal Information Protection and Electronic Documents Act), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the US (entities certified under the Privacy Shield program)).

For transfers to other countries, appropriate safeguards must be in place such as standard contractual clauses or codes of conduct.

Furthermore, the GDPR requires both controllers and processors to implement appropriate technical and organisational measures to adequately protect the personal data.

The Network and Information Security (NIS) Directive 2016/1148, which has been implemented in Belgian law by the Act of 7 April 2019 on the establishment of a framework for the protection of network and information systems of public interest for public safety, imposes security obligations on operators of essential services as defined in the Act (eg, transport, energy suppliers) regardless of whether they are processing personal data.

2.4 Penalties for Breach of Such Laws

Non-compliance with the GDPR can be punished with administrative fines of up to EUR20,000,000 or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. In addition, the Belgian Act complementing the GDPR provides for criminal fines of up to EUR160,000.

Non-compliance with the Belgian Act implementing the NIS Directive can be sanctioned with:

- criminal fines up to EUR400,000 and a prison term of maximum one year. In case of recidivism or obstruction of an investigation, the criminal fines may be increased and the prison term extended; and
- administrative fines of up to EUR200,000.

2.5 Contractual Protections on Data and Security

Where the supplier is a data processor, the GDPR requires customer and supplier to enter into a written data processing agreement setting out the details of the data processing (subject-matter, duration, nature, purpose, type of personal data and categories of data subjects). The agreement shall stipulate that the processor:

- may only process personal data upon the documented instructions of the controller;
- must ensure that persons processing personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- must take appropriate technical and organisational measures to adequately protect the personal data;
- must respect the conditions of Articles 28.2 and 28.4 of the GDPR for engaging sub-processors;
- must assist the controller in responding to data subject requests;

- must assist the controller in ensuring compliance with its obligations regarding security, data breach notification, the performance of data protection impact assessments and prior consultation;
- must return or delete the personal data after the end of the provision of the services, unless otherwise required by law; and
- must demonstrate compliance with the GDPR and contribute to audits or inspections conducted by the controller or its auditor.

In other cases, ie, where the GDPR does not apply, there is no general legal obligation to include data and security protections in contracts. However, it is highly recommended, and also standard practice, to include provisions on security, incident reporting, customer audit rights, customer data access rights, data retention and deletion and sub-contracting.

3. Contract Models

3.1 Standard Supplier Customer Model

Outsourcing is not a regulated contract under Belgian law. Except where public procurement rules apply (see below), the parties enjoy a high degree of contractual freedom. There is no standard supplier-customer model in Belgium. However, typically, the outsourcing agreement takes the form of a framework agreement or "master services agreement" (MSA), supplemented by specific agreements such as project agreements, service level agreements (SLAs) detailing key performance indicators (KPIs), etc. The most common remuneration model is based on unit prices, sometimes with fixed components or minimum fees to be paid by the customer regardless of its actual service consumption.

In most cases, a single-supplier model is applied, whereby the outsourced activities are entrusted to a single service provider. Less frequently, a multi-supplier model may be applied. In some cases, the outsourcing transaction is structured as a joint venture (JV) (see **3.2 Alternative Contract Models**).

Where the outsourcing is subject to public procurement rules, the content of the contract is to some extent regulated (in particular by the Royal Decree of 14 January 2013 on general rules for the execution of public contracts). There are general rules concerning inter alia payment terms, verification terms, sureties, revision of the contract, etc. Certain rules cannot be derogated from (and any derogations shall be considered as null and void), whereas other derogations require a specific justification (in the absence of which they are also deemed null and void). The regulations also supplement public contracts on points that they do not explicitly address.

3.2 Alternative Contract Models

Multi-supplier agreements are less common but may be a good option for the outsourcing of complex operations that require the specific know-how and competences of several specialised suppliers. In a multi-supplier model, one vendor often acts as the "integrator". This "integrator" is responsible for the integrated service offering, managing the different suppliers according to their individual contracts/SLAs and ensuring that they remain aligned with the customer's objectives. Such an arrangement also has the advantage that non-performing suppliers can be replaced without disrupting the whole outsourced operation.

In some cases, the parties choose to structure the outsourcing transaction as a joint venture (JV) agreement. The outsourcing customer then typically contributes the resources (personnel and assets) previously dedicated to the in-house performance of the outsourced operations to the JV, while the outsourcing supplier also contributes personnel and assets. This model allows the customer to keep tight(er) control over service delivery and security.

Alternative remuneration models include remuneration as a percentage share of the customer's net sales or, in the case of outsourcing structured as a joint venture agreement, remuneration as a share in the profits of the JV.

3.3 Captives and Shared Services Centres

There are no notable recent developments regarding the use of captives and shared services centres apart from the fact that this has also been affected by the general trend towards increasing digitisation, and the use of cloud-based and SaaS (software as a service) solutions.

4. Contract Terms

4.1 Customer Protections

The outsourcing contract is sui generis, there are no general customer protection measures provided for by law. As customer and supplier are in a B2B relationship, there is no pre-identified weaker party to the contract. Contractual freedom thus prevails and the customer will in principle have to see to its own protection (generally, by entering into a comprehensive, precise and clearly drafted contract, including a maximum of protective clauses).

However, the recent Act of 4 April 2019 introduces new provisions in Book IV of the Code of Economic Law relating to the abuse of economic dependence. These provisions will enter into force on 1 June 2020. Economic dependence is a position of weakness of one party (eg, because of the absence of equivalent alternatives) allowing the other party to impose performances or conditions that could not be obtained under normal market conditions. A customer finding itself in this situation can invoke the protective provision of Book

IV of the Code of Economic Law. The Act of 4 April 2019 does not prohibit economic dependence itself, but only the abuse of such position if and to the extent that this affects competition on the affected Belgian markets or an essential part thereof. The following practices may be considered as an abuse of economic dependence:

- refusing a sale or purchase;
- imposing unfair prices or other unfair trading conditions;
- limiting production, markets or technical development to the detriment of users;
- discrimination between trading parties; and
- abusive tying.

The Act also introduces provisions prohibiting certain unlawful contract terms or abusive clauses in B2B contracts, without the need to show economic dependence. These provisions, which will enter into force on 1 December 2020, exempt public procurement and financial services. A contractual clause in a B2B contract will be unfair and consequently prohibited if it creates a "significant imbalance" between the rights and obligations of the parties.

In addition to this general prohibition, the new rules also introduce two lists of specific categories of clauses: a black list and a grey list. Blacklisted clauses are considered abusive and prohibited in all circumstances without the need for any further evaluation, and include:

- potestative clauses (clauses that depend solely on the will of one party);
- clauses giving a party the unilateral right to interpret a clause;
- clauses requiring one party to waive any remedy against the other in the event of a dispute; and
- clauses which irrefutably establish the other party's knowledge or acceptance of terms that it was not familiar with prior to the conclusion of the contract.

Greylisted clauses are presumed to be unfair unless proven otherwise, ie, unless it is proven that such clauses do not create a significant imbalance. The grey list contains clauses that:

- give one party the unilateral right to modify the terms of the contract (eg, the fees) without a valid reason;
- permit the extension or renewal without a reasonable notice period;
- shift the economic risks without a proper reason;
- inappropriately limit or exclude the rights of a party in the event of contractual breach (a partial or total non-performance) by the other party;
- exclude or limit liability in the event of fraud or gross negligence;
- limit the means of evidence that a party may use; and
- provide for excessive damages in the event of non-performance or delay in the performance.

More generally, aside from this particular regime, the customer may see to its own protection by entering into a comprehensive, precise and clearly drafted contract, including a maximum of protective clauses. Protective measures and clauses include:

- *Pre-contractual agreement:* before entering into the contract, the customer is well advised to obtain a maximum of information about the supplier and the quality of services it can provide.
- *Service level agreement:* the customer can draft clauses in which minimum service quality levels or targeted service quality levels are described.
- *Intuitu personae clauses:* the customer can specify that the identity of the supplier is an essential element in the contract, preventing contract transfer.
- *Confidentiality clauses:* either during and/or after the duration of the contract, the supplier shall not disclose any confidential information received during the service performance (the clause states what constitutes confidential information).
- *Non-compete clauses:* depending on whether and how much 'know how' belonging to the customer is acquired by the supplier during the service performance, it may be useful to include a non-compete clause. This clause foresees that either during and/or after the duration of the contract, the supplier cannot provide services – comparable or similar to those provided to the customer – to competitors of the customer, within a defined area and for a limited period after the end of the contract.

The customer should stipulate in the contract the consequences of a contractual breach and the applicable remedies. Usually, the contract will foresee financial penalties or lump sum damages. The customer can also stipulate that the party suffering from non-execution or violation of a clause will withhold its own contractual obligations (eg, retain payment of supplier's fees), or be entitled to terminate the contract without prior recourse to a judge (see **4.2 Termination**).

4.2 Termination

Parties can freely stipulate termination terms. Whether it is a fixed-term or an indefinite duration contract, in practice numerous outsourcing agreements contain a reciprocal possibility to unilaterally terminate the contract without cause – or for a cause unrelated to the other party's behaviour – simply by respecting a determined notice period and/or by paying predefined indemnities.

The parties can also include a clause that would entitle the party who is the victim of a breach to terminate the contract without needing prior recourse to a judge. Often, the types of breach justifying termination will be listed non-exhaustively.

In some rarer cases, the outsourcing contract will contain an anticipatory breach clause allowing termination of the contract, where a breach has not yet occurred but is highly likely to.

A clause specific to outsourcing agreements is the "reversibility mechanism". Because the customer inevitably abandons certain powers relating to the outsourced services to the supplier, it will want the contract to end progressively (not abruptly), in order to be able to find another supplier or reinvest in the outsourced activities and regain control over them. Such a clause will contain contractual and post-contractual obligations ensuring continuity of the outsourced activities and mitigating damages to a maximum extent.

Other clauses can stipulate that a specific event will put an end to the contract: bankruptcy, force majeure, intuitu personae clauses, etc.

If the parties have not foreseen particular termination terms, Belgian contract law will apply by default, allowing the parties to terminate the contract through:

- an "amicable termination" where both parties agree on terminating the contract (Article 1134 Civil Code);
- unilateral termination without cause but with indemnities for lost profits and damages (Article 1794 Civil Code);
- termination by judicial order in case of serious breach (Article 1184 Civil Code); and
- if the contract is concluded for an indefinite period, a general principle in Belgian contract law prohibits perpetual commitments. Therefore, each party can unilaterally terminate the contract under the sole condition of giving a reasonable notice period.

If the outsourcing contract is concluded for a definite duration, the contract will end upon expiry of its term.

4.3 Liability

Violation by the parties of their respective contractual (or extra-contractual) obligations is subject to liability. Under Belgian law, parties can freely determine which damages are subject to recovery, be it for direct (directly deriving or resulting from the breach) or indirect losses.

Parties can also agree to limit their liability. Only exoneration for fraud or exoneration from the performance of essential obligations of the contract (which would deprive the contract of its purpose/essence) are prohibited. In practice, outsourcing contracts often contain quite sophisticated liability exoneration/limitation clauses, eg:

- where liability is limited to serious or intentional breaches (liability for all other "lighter" breaches is waived);
- where liability for indirect or immaterial damages is expressly excluded, ie, liability for lost profits, loss of goodwill, failure to realise expected savings, regulatory penalties, special, indirect, incidental or consequential loss; and
- in certain specific sectors, such as in IT, clauses can provide that certain specific incidents are exonerated, eg, computer, circuit, equipment or system failures.

Supplier's contractual and extra-contractual liability will also frequently be capped to a maximum amount, often with reference to the total value of the contract, or with reference to the amount of the supplier's insurance coverage.

Clauses can of course also limit both the type of damage/loss and the amounts due.

The customer will want to allow for the broadest possible supplier liability. It is not uncommon to see unlimited liability clauses, covering any loss or type of damage (included indirect or immaterial loss) burdening the supplier.

Finally, outsourcing contracts frequently contain so-called "hold harmless agreements". These are indemnity clauses through which one party commits itself to being liable for any damage the other would have to pay to third parties, as a result of an incident in relation with the contract (eg, violation of labour regulations).

4.4 Implied Terms

Belgian contract law and general principles impose implied terms or obligations applicable by default if the parties do not agree otherwise.

First, as the outsourcing contract is sui generis, doctrine and case-law will by default apply the rules pertaining to service provision contracts (Article 1710 et seq. Civil Code). For instance, Article 1794 of the Civil Code, allows each party to unilaterally terminate the contract without cause, provided the other party receives indemnities for any lost profits or damages (see **4.2 Termination**).

Also, the following general rules apply to all bilateral contracts:

- The parties must execute the contract in good faith (Article 1134, §3 Civil Code).
- Regarding contracts concluded for an indefinite period, as a general principle, no-one can be bound to a contract forever. Therefore, each party can unilaterally terminate the contract on the sole condition that it give the other party a reasonable notice period.
- A serious breach can always justify termination of the contract, through the intervention of a judge (Article 1184 Civil Code).

- The contract will always be interpreted according to the apparent common intention of the parties (Article 1156 Civil Code).
- In case of doubt regarding its interpretation, the contract is interpreted in favour of the party burdened by the obligation (Article 1162 Civil Code).

5. HR

5.1 Rules Governing Employee Transfers

When a company outsources an activity to another company, the outsourcing operation may qualify as a "transfer of an undertaking (or part of an undertaking)" as defined by the EU Directive 2001/23/EC of 12 March 2001 (hereafter, Directive 2001/23) containing rules for the safeguard of employees' rights. Belgium transposed the Directive through the Collective Bargaining Agreement n°32bis (hereafter, CBA 32bis). Typically, the transfer of (part of) an undertaking creates a triangular relationship between:

- *The transferor:* the customer deciding to outsource an activity that will cease to be the employer.
- *The transferee:* the supplier of the outsourced activity that will become the new employer.
- *The employee:* who was employed by the transferor but will become the employee of the transferee.

For the outsourcing operation to qualify as a "transfer of an undertaking (or part of an undertaking)" under Directive 2001/23 and CBA 32bis and for the employee protection rules to be triggered, a number of conditions must be met, primarily:

- there must be a change of employer (other legal entity); and
- the (part of the) undertaking being transferred, must retain its own identity.

There is, however, no condition as to the number of employees being transferred (the protection could thus apply to only one employee). The condition according to which the (part of the) undertaking must keep its identity after the outsourcing operation is difficult to define and the source of abundant, evolving and sometimes obscure or contradictory case-law from the European Court of Justice. The core question to be considered is whether the activities/operations of the (part of the) undertaking being transferred is continued as such (or in similar conditions) by the new employer (transferee), based on the following factors (the importance of each factor depending of the type of undertaking):

- whether tangible assets are being transferred;
- the value of intangible assets at the time of transfer;
- whether the majority of the transferor's employees are taken over by the new employer;
- whether or not customers are transferred;
- the degree of similarity between the activities carried out before and after the transfer; and
- the period, if any, for which those activities were suspended.

When there is a "transfer of an undertaking (or part of an undertaking)" as defined by Directive 2001/23 and CBA 32bis, the protective rules entail that all the employees confronted with the transfer will continue to benefit from all their individual and collective rights. Hence, all employment contracts, including the employment and remuneration conditions (except employees' rights to old-age, invalidity or survivor's benefits under supplementary company pension schemes) are automatically transferred from the initial employer (transferor) to the new employer (transferee). It is thus not necessary to enter into a new employment contract.

In theory, the transferee must take over all the employees occupied at the moment of the transfer, without the possibility to "select" only some of them. The transferor and the transferee can agree that some of the transferred employees will remain with the transferor, provided the employees concerned expressly agree to not being transferred.

The employees are protected against termination of their employment contract, either before or after the transfer, if the termination can be considered as being related to the transfer. The prohibition on terminating the employment agreement is lifted if either transferor or transferee can demonstrate that the dismissal is based on unrelated economic, technical or organisational reasons.

The transferor and the transferee are jointly and severally liable for the payment of debts existing at the date of the transfer and resulting from the existing employment contracts.

The transferor and transferee are required to inform and, in certain situations (see **5.2 Trade Union or Workers Council Consultation**), consult with the employees affected by the transfer or their representatives in relation to at least the following:

- the date or proposed date of the transfer;
- the reasons for the transfer;
- the legal, economic and social implications of the transfer for the employees;
- any measures envisaged in relation to the employees.

Besides the national CBA on transfer of undertakings, some employers also need to comply with sector-specific rules (for instance, in the cleaning sector (Joint Industrial Committee nr. 121)).

5.2 Trade Union or Workers Council Consultation

Under Belgian law, the transferor and the transferee could be required to inform and consult their respective Works Council (or Trade Union Delegation) about a (contemplated) outsourcing operation.

Section 11 of CBA n°9 of 9 March 1972 pertaining to Works Councils states: "In case of a merger, concentration, takeover or closure or other significant structural changes negotiated by the company, the Works Council shall be informed in good time and before disclosure. It shall be consulted effectively and in advance, notably as regards the impact on employment prospects, work organization and employment policy in general". The terms "significant structural changes" are not defined by CBA n°9. Doctrine is of the opinion that a broad interpretation is appropriate and that the question as to whether or not the envisaged structural changes are significant should be analysed case by case, taking into account all the factual circumstances.

In principle, an outsourcing operation with an impact on employment (eg, with the effect of transferring employees from the transferor to the transferee) will qualify as a "significant structural change", hence the transferor and transferee respective Works Council should be informed and consulted. If the outsourcing operation has no significant impact on the structure and employment of either company, there is in principle no need to consult the Works Council but this is nonetheless to be recommended.

In addition to this, since 2008, a transfer of a part of undertaking is also subject to a new paragraph of Article 4 of CBA n°9. The Works Council is also to be informed and consulted in advance by the employer on decisions which may cause important changes in the work organisation or the employment agreement. 'Consultation' (as opposed to 'information') means a right for the Works Council to negotiate, to open an effective dialogue between the employer and the workers' representatives. The general principle is that there should be an exchange of views and that the employees' representatives may ask for additional information, ask questions, formulate criticisms or suggestions, give their opinions, etc. The employer must follow-up on these questions, suggestions, etc, to ensure continuity of the dialogue.

Crowell & Moring LLP

7, Rue Joseph Stevens
B-1000 Brussels

Tel: +32 2 282 40 82
Fax: +32 2 230 63 99
Email: EPlasschaert@crowell.com
Web: www.crowell.com

The Works Council does not have a veto right and cannot unilaterally block the planned outsourcing operation.

If there is no Works Council within the company, the consultation shall occur at the level of the Trade Union Delegation (Article 24 CBA n°5 of 24 May 1971 pertaining to Trade Unions).

5.3 Market Practice on Employee Transfers

The transferor and the transferee will very often (and are encouraged to) include provisions in their outsourcing contract addressing employee transfer and providing inter alia for mechanisms and guarantees to determine potential liabilities arising from the (non)transfer of employees under an outsourcing project. This is of utmost importance since arrangements between transferor and transferee in the outsourcing contract (inter alia a potential selection of employees to be transferred) are not enforceable against the employees concerned. The question, for example, of which company will ultimately bear the potential costs resulting from termination or otherwise in relation with the (non) transfer, the rights and possible return of employees in the event of the termination of the outsourcing, etc, should be addressed.

The provisions regarding employee transfer will also usually foresee that the transferee will maintain sufficient staffing levels to ensure all the outsourced services are performed in accordance with the agreed work specifications and within the agreed timeframes.

It is common practice for an annex to be added to the outsourcing contract so as to clarify the terms and conditions of the transfer of employees, eg, are they respecting their employment contracts, are they respecting the remuneration and other work conditions, how and when were the employees informed about their rights and obligations, etc. Usually, the parties to the outsourcing contract will also agree on the criteria to be used to determine which employees fall within the scope of the transaction. This is in particular the case in relation to shared services and other support departments which carry out certain duties for the benefit of the part of undertaking transferred. The annex sometimes contains a list of the transferred employees (but again this list as such is not enforceable against the employees concerned).

6. Asset Transfer

6.1 Asset Transfer Terms

When assets are transferred in the context of an outsourcing or otherwise, the terms applicable to such transfer depend on the type of asset.

The transfer of immovable assets must be in writing and must be performed through a public notary. No specific formalities apply for the transfer of movable assets.

The transfer of IP rights must be in writing. For registered IP rights such as patents and trademarks the transfer will need to be registered with the patent and trademark register respectively.

The transferability of commercial contracts will depend on the contract terms. If the contract does not allow for transfer, then the party wishing to transfer the agreement must seek the consent of the other contract party. The same goes for the transfer of IP licenses.