Outsourcing in Belgium: Overview

by Bastiaan Bruyndonckx and Liese Kuyken, Lydian

Country Q&A | Law stated as at 01-Nov-2022 | Belgium

A Q&A guide to outsourcing in Belgium.

This Q&A guide gives a high-level overview of legal and regulatory requirements on different types of outsourcing; commonly used legal structures; procurement processes; formalities required for transferring or leasing assets; data protection issues; supply chain compliance; specification, service levels and escalation; flexibility in volumes purchased; charging methods; customer remedies and protections; warranties and indemnities; term and notice period; termination and its consequences; liability, exclusions and caps; dispute resolution; and the tax issues arising on an outsourcing.

Regulation and Industry Requirements

National Regulations

1. To what extent does national law specifically regulate outsourcing transactions?

There are no laws specifically regulating single jurisdiction or cross-border outsourcing transactions in Belgium. The Civil Code governs the formation of an outsourcing contract, the legality of the contract and certain warranties and liabilities (as it does for any other contract). Outsourcing contracts fall under the general regime for service contracts ("rent of work") as defined by Article 1710 of the Civil Code. The cornerstone of contract law is the principle of "freedom of contract" (Article 1134, Civil Code). The parties can agree on anything that does not conflict with mandatory law, public order or morality. Therefore, outsourcing in Belgium is mainly governed by the contract between the parties.

Sectoral Regulations

2. What additional regulations may be relevant for the following types of outsourcing?

Sector-specific Regulations

IT and cloud services. There are no specific regulations for outsourcing of IT and cloud services, therefore the principle of freedom of contract applies.

Telecoms. There are no specific regulations for telecommunications outsourcing. Providers of electronic communications networks and services (operators) providing outsourced telecom services must comply with the legislation and regulation governing electronic communications, including the Electronic Communications Act. In addition, these operators must comply with the resolutions and decisions issued by the Institute for Postal Services and Telecommunications (BIPT/IBPT), the telecom regulator.

Public sector. Depending on their values and characteristics, outsourcing transactions in the public sector can be subject to the Belgian Public Procurement Act, which entered into force on 17 June 2016 and implements the Public Contracts Directive (*2014/24/EU*), Utilities Directive (*2014/25/EU*) and E-invoicing Directive (*2014/55/EU*). When public authorities wish to contract certain services, supplies and/or works from companies, they must comply with the public procurement rules laid down in this act. The act provides the principles and rules applicable to public procurement. Public procurement regulations contain extensive obligations with regard to the prescribed tender procedure and the possibilities for negotiation.

Financial services. The financial sector, including credit institutions, must take appropriate measures to limit the risks of outsourcing. Article 66 of the Law of 25 April 2014 on the status and supervision of credit institutions and listed companies specifically regulates the outsourcing of operational tasks that are of critical importance. In addition, Circular NBB 2019/19 of the National Bank of Belgium applies to credit institutions, stockbroking firms, payment institutions, e-money institutions, and Belgian branch offices of non-EER credit institutions and investment firms.

The circular integrates the Guidelines of the European Banking Authority on outsourcing arrangements of 25 February 2019 and includes a grandfather clause for existing outsourcing agreements. A prior notification to the competent authority is necessary, including details on the planned outsourcing of critical or important functions and/or where an outsourced function has become critical or important. The notification must be made two months before the outsourcing. In addition, existing outsourcing contracts subject to material changes and/or material events, must also be notified to the competent authority.

Insurance. In the insurance sector, outsourcing is regulated by several specific laws including:

- Article 16/2 of the Insurance Act.
- The Solvency II Law.
- Article 274 of the Delegated Regulation 2015/35.
- Circular NBB 2020/18 of the National Bank of Belgium on outsourcing cloud services.
- The guidelines of European Insurance and Occupational Pension Authority (EIOPA), the European regulator of insurers and pension funds.

An insurance company intending to outsource must put in place a written outsourcing policy, which must be approved by the board (Delegated Regulation 2015/35). In addition, insurance companies must:

- Have a properly functioning IT system (that can keep records of the business) and appropriate IT control and security measures.

- Adopt the necessary measures to manage cyber risks in the context of their IT security systems.
- Notify the National Bank of Belgium in advance of planned outsourcings of critical or important functions or activities.

(Circulars NBB 2009/17 and NBB 2020/18 of the National Bank of Belgium.)

Utilities. With regard to outsourcings within the utilities sectors, Law of 1 July 2011 on security and protection of critical infrastructures governs all outsourcings in which a company operates critical infrastructure (that is, an installation or system, or part of such installation/system, that is of national importance and essential to the maintenance of vital societal functions, health, safety, security, economic prosperity, or social welfare). As utilities are considered critical infrastructure, these companies must comply with general safety obligations.

Other Legal or Regulatory Requirements

There are no specific regulations for:

- Professional services outsourcing.
- Legal process outsourcing.
- Knowledge process outsourcing.
- Manufacturing outsourcing.

3. What industry sectors require (formally or informally) regulatory notification or approval for outsourcing transactions?

Financial Services

Before outsourcing a function, a credit institution, stockbroking firm, payment institution, e-money institution, Belgian branch office of a non-European Economic Area (EEA) credit institution or investment firm should check whether the function in question is critical or important. A function is critical or important:

- Where a defect or failure in its performance would materially impair:
    - their continuing compliance with the conditions of their authorisation or their other obligations under the Capital Requirements Directive (*2013/36/EU*) (CRD IV), Capital Requirements Regulation (*(EU) No 575/2013*) (CRR), second Markets in Financial Instruments Directive (*2014/65/EU*) (MiFID II), revised Payment Services Directive (*(EU) 2015/2366*) (PSD2) and second Electronic Money Directive (*2009/110/EC*) and their regulatory obligations;
    - their financial performance; or

    - the soundness or continuity of their banking and payment services and activities.

- When operational tasks of internal control functions are outsourced, unless their assessment establishes that a failure to provide the outsourced function or the inappropriate provision of the outsourced function would not have an adverse impact on the effectiveness of the internal control function.
- When they intend to outsource functions of banking activities or payment services to an extent that would require authorisation by a competent authority. (These activities are listed in Annex I of the Capital Requirements Directive IV (*2013/36/EU*)).

If the function is critical or important the supervisory authority (the National Bank of Belgium) must be notified in due time and appropriately. In principle this must be done a minimum of six weeks before the outsourcing enters into force, barring any duly justified specific derogation. For the notification, a standard form can be used which is issued by the National Bank of Belgium. The notification file should be accompanied by a systematic opinion of the person responsible for compliance, confirming compliance with the requirements relating to the different stages of the outsourcing and the completeness of the file provided. The National Bank of Belgium can impose an administrative fine if the notification is not carried out in this way.

Insurance

Before outsourcing critical or important functions or activities or independent control functions, insurance undertakings must notify the National Bank of Belgium:

- Of their intention to do so.
- Any subsequent significant developments concerning these functions or activities (including the decision to terminate the outsourcing of any of these functions or activities).

In principle this must be done a minimum of six weeks before the outsourcing enters into force, barring any duly justified specific derogation. For the notification, a standard form can be used which is issued by the National Bank of Belgium.

An insurance company's outsourcing policy must include the approach and processes that apply to the outsourcing for the entire term of the agreement, and particularly the process to determine whether a function or activity is a critical or important function or activity. It must conduct this analysis by asking whether the function or activity concerned is crucial for the company's operation. A function or activity is crucial if the company would not be able to provide its services to policyholders without it. Examples of critical or important functions or activities include the:

- Design and pricing of insurance products.
- Conclusion of contracts.
- Investment of assets or portfolio management.
- Provision of computer data storage.

(Circular NBB 2016/31, September 2018.)

Merger Control

Certain mergers require the prior approval of the Competition Authority and, in certain cases, of the European Commission.

A merger is an operation that results in a lasting change of control of an undertaking, that is the ability to exercise decisive influence over its activity (Code of Economic Law).

The Competition Authority must be notified for mergers where both:

- The undertakings have a total turnover in Belgium of more than EUR100 million.
- At least two of the undertakings each generate a turnover in Belgium of at least EUR40 million.

Large-scale operations generally have effects that extend beyond national borders and must be notified to the European Commission. The Merger Regulation (*(EC) 139/2004*) requires undertakings to notify the European Commission of the merger if either:

- The merging firms have a combined worldwide turnover of over EUR5,000 million and each of at least two of the merging firms has an EU-wide turnover over EUR250 million.
- The merging firms have a combined worldwide turnover of over EUR2,500 million, the combined turnover of the merging firms is over EUR100 million in each of at least three EU member states, and at least two of these firms have a turnover of over EUR25 million in three EU member states and at least two of these firms have an EU-wide turnover of more than EUR100 million.

Joint Ventures

See above, *Merger Control*.

Structuring the Transaction

4. What transaction models are commonly used in an outsourcing in your jurisdiction? What are their respective advantages and disadvantages?

Direct Outsourcing

The customer and supplier contract directly. The supplier has the means and personnel to provide the services without another party. This structure of outsourcing is the most traditional form. Generally, the contractual structure includes a framework (services) agreement and one or more specific agreements (for example, services agreements, project agreements, consultancy agreements).

The framework agreement and its schedules cover the generic legal, regulatory, governance, commercial and operational arrangements, including:

- Service procedures.
- Pricing mechanisms.
- Services levels, service credits and monitoring.
- Regulatory compliance.
- Intellectual property (IP).
- Confidentiality.
- Customer data ownership.
- Liability.
- Indemnification; term and termination.
- Termination assistance (exit).
- Subcontracting.

In most cases, only one specific agreement is entered into under the framework (services) agreement. In multi-jurisdictional outsourcing, it is customary for the parties to enter into separate framework agreements on a country-by-country basis, to take into account country-specific requirements and constraints.

Where the outsourcing includes a transfer of assets, contracts and/or personnel, this is usually dealt with in a separate transfer agreement, to avoid this transfer being undone if the outsourcing agreement expires, is terminated or is declared null and void.

Direct outsourcing is a flexible and easy way to outsource services. The customer benefits from economies of scale and the expertise of the supplier. In addition, managing the supplier tends to be relatively straightforward. The main risks of direct outsourcing are supplier lock-in and a lack of flexibility on the supplier's side. The customer risks becoming very dependent on the sole supplier, putting the customer in a less favourable position compared to multi-sourcing. The negotiating possibilities (for example, those concerning deal structuring, liability or indemnification) for direct outsourcing are also more limited than in other forms of outsourcing.

Multi-sourcing

The customer concludes outsourcing agreements with multiple suppliers. To ensure smooth service delivery, the various agreements usually contain wording on the various providers' obligations to co-operate with one another. In certain situations, the various service providers are required to enter into "operating level agreements'" directly with one another.

Multi-sourcing gives the customer a lot of flexibility. However, a large number of contracts make the outsourcing activities more difficult to manage and incur higher costs. In addition, without a single supplier taking end-to-end responsibility for the service delivery, liability can be difficult to allocate.

Indirect Outsourcing

The supplier contracted by the customer subcontracts the services agreed on simultaneously to one or more third-party suppliers. In many cases, the third-party supplier (subcontractor) is a nearshore or offshore partner of the supplier.

The structure shares similar advantages and disadvantages to direct outsourcing. The main advantage is that the customer can enter into a "local" outsourcing contract with the supplier (likely to be governed by the law of the customer's main establishment) but at the same time benefit from offshore pricing. However, it is more difficult for the customer to enforce their rights against the second supplier.

Joint Venture

The customer can outsource by establishing a joint company with the supplier.

This requires a rather complex contractual relationship, and therefore is only advisable for far-reaching outsourcing partnerships. The customer has a larger degree of control over the supplier and the provision of the services and can even share in the profits of the joint venture. The main disadvantages of this structure are the costs and the management time required to set up and operate the joint venture. In addition, exiting the arrangement tends to be more complex than exiting traditional outsourcing agreements.

Procuring the Supplier/Service Provider

5. What procurement processes are used to select a service provider or supplier of outsourced services?

Various preparatory actions are necessary to conclude an outsourcing agreement.

Public or governmental bodies must follow a mandatory procurement process. The public customer must obtain offers from various suppliers and select the supplier that offers the best value (based on the supplier's price, quality and professionalism among other factors) or the best price depending on the public tender's selection criteria.

Private companies also often compare the different suppliers in the market. In the private sector, the process of selecting and contracting an outsourcing supplier will generally consist of the following steps.

Request for Information (RfI)

As the customer wishes to conclude the outsourcing agreement with the supplier offering the best value, the customer sends out a RfI to potential suppliers that are on the customer's long list. In the RfI, the customer provides a short description of the desired services. They ask the potential suppliers to submit an indication of their experience, capabilities and approach to the envisaged outsourcing and a high-level indication of pricing. The customer usually asks a number of specific questions to get a better understanding of the various options available in the market.

Shortlisting

The customer reviews the responses received from the potential suppliers in the RfI phase and reduces the pool of potential contract partners to a shortlist. The customer is often advised by business advisors (outsourcing specialists) that assist the customer in assessing the operational, governance and pricing aspects of the project.

A RfI and shortlisting are not always necessary and customers may choose to send out a Request for Proposal immediately.

Request for Proposal (RfP)

On the basis of the information gathered during the RfI phase, the customer finalises its own requirements and asks the shortlisted suppliers to submit a full and detailed proposal. The customer should be transparent about the criteria that it will use to select the supplier. Usually, the RfP contains a draft contract for the potential suppliers to comment on. The customer should inform the suppliers that the level and nature of their comments on the draft contract forms part of the selection criteria. In general, from this stage onwards, the customer and the potential outsourcing suppliers are advised by external counsel.

Due Diligence

One or more potential suppliers perform a due diligence exercise to gain a better understanding of the services to be provided, the technology involved and the personnel and assets that may be taken over.

The customer will also perform due diligence on the potential suppliers to verify certain aspects for example:

- Financial stability.
- Employee mobility.
- IP protection.
- Customer satisfaction with the potential supplier's performance of similar projects.

Best and Final Offer (BaFO)

On completion of the due diligence, the remaining potential suppliers are generally asked to submit a BaFO, on the basis of which further negotiations can take place between the parties. At this stage, it is also advisable that the customer obtain information on the potential suppliers' position on the legal terms governing the outsourcing transaction. This is factor that may be taken into account by the customer when deciding on the offer(s) to be retained.

Negotiation

After the parties have reached an agreement on the technical and organisational aspects and the pricing, they commence legal contract negotiations, where the parties are often accompanied by their external legal counsel. The aim of the negotiations is to conclude a final comprehensive agreement. The length of the negotiations is dependent on the scope and complexity of the outsourcing project and can vary from two weeks to several months for complex cross-border transactions.

Negotiations can take place with more than one potential supplier. It is important for customers to be transparent as to whether or not the negotiations are exclusive. Otherwise, a customer could be held pre-contractually liable for terminating the negotiations with one potential supplier to sign an agreement with another potential supplier. This issue is often addressed through entering into a letter of intent (LoI) or memorandum of understanding (MoU) with each of the suppliers with whom negotiations are started. Ideally, the LoI or MoU should provide for the right of the customer to terminate the negotiations at any point in time and without any indemnity being due.

Contract Execution and Verification

In most cases, the execution of the final contract is followed by a verification phase during which the supplier can verify their assumptions and measure the actual service levels (before committing to the agreed on service levels). The outcome of the verification phase can lead to further adjustments of the contract. Any changes to the contract as executed however require the approval of both the customer and the supplier.

Transferring or Leasing Assets

Formalities for Transfer

6. What formalities are required to transfer assets on an outsourcing transaction?

Immovable Property

The sale and purchase of immovable property (real estate) must be executed before a notary public. The notary public will check that the transfer is valid and register the agreement with the competent tax and land offices. Registration with the competent land office is necessary to ensure the transfer is valid in relation to third parties.

IP Rights and Licences

The transfer of IP rights generally requires a written agreement between the parties. Certain specific formal requirements can apply, for example in the transfer and assignment of copyrights or rights in software. A company transferring IP rights, for example a trade mark, copyright or patent, must ensure that it is entitled to transfer these rights. In addition, the transfer of registered IP rights can require registration of the transfer in the relevant IP registers (for example, the Benelux Intellectual Property Office or World Intellectual Property Organization). The transfer of third-party licences requires the approval of the third-party licensor, except if explicitly foreseen otherwise in the licence agreement. In many cases, it is a time-consuming process to obtain third-party approvals for the transfer and assignment of licences.

Movable Property

No specific formalities apply to the transfer of movable property. In most cases, the list of transferred assets will be attached to the outsourcing agreement or will form a schedule to a separate asset transfer agreement (see *Question 4, Direct Outsourcing*).

Key Contracts

Unless explicitly foreseen in the contract, a transfer of a contract generally requires the approval of the other contracting party. In many cases, it is a time-consuming process to obtain third-party approvals for the transfer and assignment of contracts. When a business division is transferred as a going concern, the transfer of agreements relating to the transferred business does not require the prior consent of the contracting party, unless specific contractual terms provide otherwise.

Data and Information

Transfers of data must comply with the General Data Protection Regulation (*(EU) 2016/679*) (GDPR) and with the national legislation on the transfer of personal data. Within the European Economic Area (EEA), the principle of free movement of personal data exists, therefore no specific measures need to be taken with regard to intra-EEA cross-border data transfer.

Data transfers to other jurisdictions outside the EEA can only take place if either:

- The transfer is to a country recognised by the European Commission as providing an adequate level of data protection.
- The business has implemented one of the required safeguards as specified by the GDPR (for example, standard contractual clauses or binding corporate rules).
- Derogations specified in the GDPR are applicable to the transfer.

On 25 May 2018, the European Data Protection Board set out in its Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (Derogations Guidelines) that a "layered approach" should be taken with respect to these transfer mechanisms. If no adequacy decision is applicable, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the GDPR before relying on a derogation.

To comply with the GDPR's transparency obligation, the data subjects may need to be notified. For example, notification is necessary when there is a change of the data controller's identity.

Formalities for Leasing or Licensing

7. What formalities are required to lease or license assets on an outsourcing?

Immovable Property

Specific legislation governs leasing real estate. Parties can deviate from most of this legislation but should do so in writing. Leases of real estate must be registered with the competent land office.

IP Rights and Licences

The customer can sub-license IP rights if this is foreseen in the licence agreement or with explicit consent of the licensor.

Movable Property

There are no specific formalities required for leasing movable property. The lease does not need to be registered. However, it is advisable to have written arrangements in place.

Key Contracts

It is not possible to lease or licence a contract. Contracts can only be transferred/assigned to the supplier (see *Question 6, Key Contracts*). In certain cases, where the parties do not wish to or cannot transfer/assign the contract, the customer mandates the supplier to manage the contract. (This is referred to as third-party management of managed contractors.) In certain cases, this even includes paying the invoices due under the managed contract. There is no change of contracting party and the customer and supplier therefore formally remain the contracting parties and responsible for performing their respective obligations under the contract.

The above formalities apply if a business function is offshored from Belgium.

Transferring Employees on an Outsourcing

8. Are employees transferred by operation of law?

For information on transferring employees in an outsourcing transaction in [jurisdiction], including structuring employee arrangements (including any notice, information and consultation obligations) and calculating redundancy pay, see *Country Q&A: Transferring Employees on an Outsourcing in Belgium: Overview*.

Data Protection and Secrecy

9. What legal or regulatory requirements and issues may arise on an outsourcing concerning data protection?

For all EU member states, General Data Protection Regulation (*(EU) 2016/679*) (GDPR) applies to the processing of personal data wholly or partly by automated means, or other than by automated means, if the data forms part, or is intended to form part, of a filing system (Article 2(1)). The GDPR defines personal data as "any information relating to a data subject" (Article 4(1)). For more details on the GDPR, see *Practice Note, Overview of EU General Data Protection Regulation*.

The GDPR was adopted in May 2016 and applied directly in all European Union (EU) member states without the need for transposition from 25 May 2018. The reform was intended to respond to new challenges brought by rapid technological developments and globalisation and to put in place a coherent framework for the protection of personal data within the EU. The GDPR applies to all processing of personal data wholly or partly by automated means, or other than by automated means, if the data forms part, or is intended to form part, of a filing system (Article 2(1), GDPR). The GDPR defines personal data as any information relating to a data subject (Article 4(1), GDPR). (For more details on the GDPR, see, *Practice Note, Overview of EU General Data Protection Regulation*.) Therefore, outsourcing requires compliance with the GDPR.

Data Protection and Data Security

Use of processors and sub-processors. To the extent that a supplier processes personal data on behalf of the customer (controller), the supplier is a processor. Controllers and processors must enter into a data processing agreement, where the different responsibilities of the parties are listed.

Liability for breaches of personal data processing requirements (for both the customer and the supplier). As the processor merely acts on behalf of the controller, it is only liable for damage caused by the processing where it has not complied with processors' GDPR obligations or where it has acted outside of or contrary to the controller's lawful instructions.

The controller, who determines the purposes and the means of the processing activities, is liable for damage caused by processing which violates the GDPR.

Transfer of personal data to third countries. Within the EU, the principle of free movement of personal data exists, therefore no specific measures need to be taken for cross-border data transfers.

Transfers to "third countries" are only permitted in any of the following circumstances:

- If the transfer is to a country the European Commission recognises as providing an adequate level of data protection. Currently, Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland and Uruguay are white-listed. Moreover, as regards to the UK, the European Commission has recognised that it is providing adequate protection under the GDPR and the Law Enforcement Directive (*(EU) 2016/680*). No general finding of adequacy has been made in relation to the US. In 2016 the European Commission adopted an adequacy decision approving a new framework for transatlantic data flows, the EU-US Privacy Shield. The organisations that joined the Privacy Shield had to adhere to the privacy rules established by the US Department of Commerce and the European Commission. The ECJ ruled the Privacy Shield invalid on 16 July 2020 (*Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Case C-311/18) EU:C:2020:559* (Schrems II)). For further information on the impact of this judgment see *https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf*.
- Where there are appropriate safeguards in place, for example standard contractual clauses (SCCs) or binding corporate rules and on the condition that data subjects have enforceable rights and effective legal remedies (Articles 46 and 47, GDPR). In relation to to SCCs, the *Schrems II* decision has questioned the validity of this transfer mechanism. Organisations are therefore required to re-evaluate all their data transfers to third countries if based on SCCs and should perform a transfer impact assessment (TIA). On 4 June 2021, the EU Commission published a new set of SCCs for the transfer of personal data to countries outside the EEA, including the UK. From 27 September 2021, any new transfers based on SCCs are required to have adopted the new SCCs, and current data transfer agreements must adopt the new SCCs by 27 December 2022.
- A derogation for a specific situation applies, for example the data subject has given their explicit consent (Article 49, GDPR).

On 25 May 2018, the European Data Protection Board set out in its Derogations Guidelines that a "layered approach" should be taken with respect to these transfer mechanisms. If no adequacy decision is applicable, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the GDPR before relying on a derogation.

Security requirements. Personal data must be processed in a way that ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have put in place appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risks, this may include:

- The encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity and resilience of processing systems.
- The ability to restore access to data following a technical or physical incident.
- A process for regularly testing and evaluating the technical and organisational measures for ensuring the security of processing.

Mechanisms to ensure compliance. See above, *Transfer of personal data to third countries* and *Security requirements*.

Sanctions for non-compliance. The Data Protection Authority has a wide range of powers, including to:

- Issue warnings or reprimands for non-compliance.
- Order the controller to disclose a personal data breach to the data subject.
- Impose a permanent or temporary restriction, including a ban on processing. The Inspection Service of the Data Protection Authority can order a temporary suspension, restriction or freezing of the processing under review, if the data concerned could cause damage which is serious, immediate and difficult to repair. Subsequently, the Litigation Chamber of the Data Protection Authority can order the temporary or definitive freezing, restriction or prohibition of the processing (Law of 3 December 2017 on the establishment of the Data Protection Authority).
- Withdraw a certification.
- Impose an administrative fine. The GDPR provides for administrative fines which can be EUR20 million or up to 4% of the business's worldwide annual turnover in the proceeding financial year, whichever is higher.

Banking Secrecy

Banking secrecy is generally recognised as a practice adopted by banks. In addition, it is assumed that the agreement between a bank and its client includes a non-written obligation of confidentiality. However, under Belgian law, there is no statutory definition or any specific regulation on banking secrecy. In addition, specific legislation sets out numerous exceptions to the application of the banking secrecy practices. Banking secrecy is also not regarded as a criminally sanctioned professional secrecy or confidentiality obligation (unlike for example, attorneys' or physicians' professional secrecy obligations).

Confidentiality of Customer Data

General requirements. In addition to being subject to the GDPR and other applicable data protection legislation, most suppliers handling data on their customers' behalf are likely to be subject to a contractual non-disclosure obligation towards their customers and potentially also to third parties. The outsourcing contract should expressly set out the obligation of confidentiality with respect to customer data. In addition, although strictly speaking ownership of data is not a recognised legal concept, outsourcing customers are well-advised to provide that they retain "title and ownership" of any and all customer data.

Security requirements. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data. See above, *Data Protection and Data Security: Security requirements*. Non-personal customer data should also be adequately secured.

Mechanisms to ensure compliance. See above, *Data Protection and Data Security: Transfer of personal data to third countries* and *Security requirements*.

International standards. See above, *Data Protection and Data Security: International standards.*

Sanctions for non-compliance. See above, *Data Protection and Data Security*: *Sanctions for non-compliance*.

International Standards

The International Organization for Standardization's ISO 27001 is the most common data security standard. The international standard ISO 27701 is also increasingly referred to with regard to GDPR compliance.

Supply Chain Compliance

10. What (if any) compliance provisions should an outsourcing customer include in the contract?

A customer may include compliance related provisions in the outsourcing agreement to ensure compliance throughout the entire supply chain for various reasons, including mandatory legal obligations. Typically, outsourcing agreements contain mandatory legal obligations ranging from data protection compliance, EU anti-money laundering and anti-bribery obligations and export control. Customers that form part of US multinationals also tend to include US-inspired compliance obligations (for example, Foreign Account Tax Compliance Act obligations).

It has become market standard for an outsourcing customer to make its code of conduct an integral part of the contract and require the supplier and any sub-suppliers to comply with that code of conduct. Typically, these codes of conduct include reference to UN resolutions on for example, human rights, the use of child labor and health and safety in the workplace. It is also becoming market standard to include requirements for environmental and sustainability awareness in these codes of conduct.

Services: Specification, Service Levels and Escalation

11. How is the service specification typically drawn up and by whom?

The service specification describes the outsourced services that are to be provided. Often, the customer clearly identifies its specific needs and draws up the service specification. Based on the customer's previous experience of the supplier, the service specification is adapted and described in detail. The service specification can be part of the RfP or can be agreed on by the parties after negotiation (see *Question 5*). The description of services is a fundamental part of the outsourcing contract and is often attached as a separate schedule. In more standardised outsourcing environments (for example, managed IT services), the service specification is often drawn up by the supplier, taking into account the multi-tenant nature of the service.

12. How are the service levels and the service credits scheme typically dealt with in the contract?

Often, parties enter into detailed service level agreements (SLAs) which can measure the performance of the supplier. SLAs must contain clearly defined levels of service, described in an objective and precise way and indicate the expected results and how those results are reported to the customer.

If there is no SLA, service levels are often included in a separate schedule of the outsourcing agreement due to the high level of detail required.

The service levels are often designed and defined by the customer's commercial teams. The parties can distinguish between service levels that are critical and others that are less critical. This can have an influence on the reporting period and the compensation. In many outsourcing transactions, use is made of a "grace period" of three to six months during which service credits do not apply and the parties measure the service levels and agree on a baseline for the service levels.

If the agreed service level is not reached, parties often use service credit mechanisms, where a price reduction is applied to the next month's invoice. Service credits must be clearly defined to ensure that they are not regarded as unlawful private penalties. It is also important to clearly specify whether or not the service credits are the outsourcing customer's sole and exclusive remedy for breach.

Multi-sourcing often entails contractual incentives for the different suppliers to collaborate, for example, collaboration targets that can trigger service credits. In a multi-sourcing context, operational level agreements between the various suppliers are often used. These regulate the interaction between the suppliers and may contain sanctions (penalties) for non-compliance. Many customers also seek to appoint one supplier that acts as a single point of contact and takes overall responsibility for end-to-end service delivery.

13. Are there any service escalation mechanisms that are usually included in the contract? How often are these exercised and how effective are they in restoring the services to the required levels?

There are no standard contractual escalation mechanism terms. However, the parties often include escalation mechanisms in the outsourcing contract as a result of their contractual negotiations. Parties often agree on the customer's:

- Increased monitoring rights when the supplier performs poorly. This enables the customer to investigate the origin of the poor performance.
- Step-in rights when the supplier's poor performance continues. The customer can take over the provision of services using its own personnel or a third party. These step-in rights are used in outsourcing contracts to ensure the performance of the agreed services for a limited time (until the specific issue has been addressed). In practice, customers do not often exercise their step-in rights (as stepping in is frequently very difficult because the customer

often lacks the required capabilities, manpower and/or know-how), but it is very common to have these rights in the contract. Step-in rights are often regarded as the penultimate remedy before termination of the outsourcing contract.

Transaction Management

Organisational Structures and Change Management

14. What types of organisational structures are commonly used to govern outsourcing transactions?

The amount of levels within the organisation involved in the decision-making process largely depends on the size of the organisation.

Companies can therefore establish organisational and/or strategic committees to simplify this process and assign powers to a specific focus or steering group, which will be familiar with the complexity of the outsourcing relationship and the specific needs of the organisation.

15. What change management models are commonly used to govern outsourcing transactions?

The description of services is a fundamental part of the outsourcing contract and is often attached as a separate schedule. Using this approach, the contracting parties retain a high degree of flexibility and will not be forced to modify the entire contract in the event of a change to these services. With this method, only the schedule would need to be replaced.

It is also possible to work with specific work orders for certain services, so that a change to a particular service does not entail a change to all the services.

Most, if not all, outsourcing agreements will include a change management process, which will set out how changes to the outsourcing agreement (including any related schedules or timings) will be initiated, reviewed, assess and approved. It is common for an outsourcing agreement to foresee the setting-up of a change management board, with representatives from both parties to oversee the change management process.

Flexibility in Volumes Purchased

16. What mechanisms are commonly used to manage adjustments in the volume of services?

There is no specific legislation governing customers' flexibility to adjust the volumes purchased. Parties can agree it during contractual negotiations. The level of flexibility to adjust the volumes customers purchase is generally dependent on the type of services and the charging method.

Often, where the changes in volumes stay within an agreed bandwidth, the customer is free to change the volume on a monthly basis. If higher or lower volumes outside the agreed bandwidth are required because the customer's needs change, this is usually addressed by making a request under the contractual change control provisions. More sophisticated IT outsourcing contracts provide for both:

- A bandwidth in which the volume can vary without effect on the price.
- Separate pricing for volumes below and above the bandwidth.

Parties can also agree on thresholds at which a reduction of the volume of services is a termination event or triggers the customer's obligation to pay a termination fee or indemnity.

Charging Methods and Key Terms

17. What charging methods are commonly used on an outsourcing?

The parties are free to negotiate charging methods. The charging method depends on the specific circumstances and the type of services required.

Common charging models are the:

- Fixed price model, which is based on the described services.
- Variable price model that is based on the defined deliverables, for example unit or service pricing.

There are other methods, for example "pay as you use" that can be agreed if the supplier is facing uncertainties.

Fixed Pricing

In is rather unusual for parties to agree on a fixed price. However, if the volumes required are foreseeable, it is possible for parties to agree a predetermined price. In long-term agreements, a provision for indexation can be added.

Variable Pricing

For ongoing services, parties can agree on a usage pricing or effort-based pricing. This pricing can be defined by the deliverables or the time spent.

18. What other key terms are used in relation to costs, including auditing and benchmarking mechanisms?

In outsourcing contracts, as the agreement is solely dependent on the parties' requirements, various terms can be provided for including:

- Indexation.
- Charge variation mechanisms.
- Benchmarking provisions.
- Payment terms.
- Late payment interest.
- Invoice dispute resolution.
- Service credits.
- Audit rights (as regards the invoices and charges).

With the exception of the indexation and the late payment interest clauses, the parties are free to agree whatever they want. Indexation clauses between Belgian companies are limited to 80% of the total price. In addition, they cannot be linked to the consumer price index but must be linked to a relevant index, for example a labour cost index. In late payment interest clauses, the parties should stay away from excessively high interest rates as these interest rates can be lowered by the courts or declared null and void.

Customer Remedies and Protections

19. If the service provider fails to perform its obligations, what remedies and relief are available to the customer under general law?

There are no specific statutory remedies or relief available to the customer if the supplier fails to perform its obligations, but contract law based on court practice and general principles provides a range of remedies and reliefs. For example, the customer can:

- Withhold payments for services that are not delivered.
- Claim damages that are directly or indirectly caused by a breach of contract by the supplier.
- Terminate the agreement because of the supplier's breach where the parties are unable to continue their cooperation because the supplier's failure to perform is crucial.

20. What customer protections are typically included in the contract to supplement relief available under general law?

Typical outsourcing arrangements allow for various customer protections, many of which are easier to exercise in comparison with general contract law remedies and reliefs. Service levels and service credits are often included in a contract. These provisions can include a contractual guarantee and assure a certain minimum level of service. The customer can also be granted a step-in right, to quickly remedy any failures. The parties can also agree on an audit right for the customer. Where audit rights are included, these are generally limited (for example, no more than once every contract year). However, in regulated sectors, exceptions must be foreseen for audits carried out by or on behalf of the supervisory authorities. Parties also often agree that audits can only be carried out by external auditors that are agreeable to both parties.

The supplier can be subject to contractual penalties for failure to perform its services or reach the minimum level of performance. However, courts are very hesitant to impose these penalties and can reduce the amount of the penalty.

Moreover, benchmarking provisions could be included in a contract, meaning that the process by which the services of an existing outsourcing supplier are compared to the same or similar services of other suppliers or with an estimation of the market price. With benchmarking, the customer will be able to examine whether the supplier is still the most adequate contractual party by taking into account the prices and quality compared to the market generally and to check that it is still receiving value for money. It is often foreseen in the outsourcing agreement that the ability to benchmark will be limited in frequency. Also, most agreements containing benchmarking clauses clearly set out precisely how the parties will be involved in the benchmarking process.

Warranties and Indemnities

21. What express warranties and/or indemnities are typically included in the contract documentation?

Outsourcing contracts typically include indemnities and warranties that the:

- Parties acknowledge that the pre-contractual documentation and information given was complete and accurate.
- Parties are entitled to enter into the agreement (both customer and supplier).
- Parties will comply with all applicable laws, including their GDPR obligations.
- Parties can license the IP rights and indemnify the other party against third-party claims for IP infringement.
- Supplier must provide the services with reasonable skill and care and in accordance with best industry practice.

The customer will generally seek (unlimited) indemnities in the areas that are most critical, for example:

- IP.
- Confidentiality.
- Regulatory compliance.
- Compliance with anti-bribery and anti-money laundering legislation.

In addition, since the GDPR entered into force on 25 May 2018, there is a clear trend among customers to ask for unlimited indemnities, specific indemnities or a higher liability cap for violations of personal data legislation.

22. What requirements are imposed by national or local law on fitness for purpose and quality of service, or similar implied warranties?

The parties are bound by the contract and the supplier must meet its obligations. As outsourcing contracts do not involve consumers, who are given additional legal protections, the parties are free to contract. There are no implied service warranties or warranties of fitness for purpose of a service. The parties can therefore exclude or limit warranties in relation to the services provided. However, where the outsourcing also involves the supply of certain products (for example, hardware), the Civil Code rules governing sale-purchase contracts implies warranties of absence of latent defects and fitness for purpose.

23. What types of insurance are available in your jurisdiction concerning outsourcing? Are there any types of insurance required by law?

Insurance policies can cover several types of risks including:

- Business liability.
- Professional liability (professional errors and omissions).
- Third-party liability.
- Property damage.
- Cyber-risk liability.
- Employee liability.

Termination and Termination Consequences

Events Justifying Termination

24. What events justify termination of an outsourcing without giving rise to a claim in damages against the terminating party?

Material Breach

For the termination to be valid, the breach must be serious and render the agreement irreparably broken. Where there is a material breach, the parties must be unable to continue their contractual relationship. A material breach of an outsourcing contract can, for example, consist of non-compliance with important contractual provisions including the:

- Customer's financial obligations.
- Supplier's non-compliance with key performance indicators.

Termination for material breach can be foreseen in the contract or decided by a court or tribunal. To avoid discussion of the nature of a breach, customers should define instances that qualify as a material breach in the contract (for example, non-achievement of a particular service level for three consecutive months).

Insolvency Events

The parties can include unilateral termination in the outsourcing agreement if any party goes bankrupt or is subject to an insolvency procedure.

Termination for Convenience

Where the contract is for an indefinite term, it is illegal to bind a party in perpetuity. Parties must always be able to terminate the agreement without reason. The parties can, however, make this possibility conditional on a notice period and a termination fee.

In principle, it is not possible to terminate a contract of a definite term prematurely without paying damages. However, the possibility can be included in the contract. Again, this is usually made conditional on the payment of termination fees. Outsourcing agreements that provide for early termination for convenience rights generally set out the method or model for calculating termination fees. These fees are aimed at compensating the supplier for the initial investments at the start of the contract and loss of profits. The most common model consists of an amount that decreases over time (that is, the later the termination occurs, the lower the termination fees). Termination fees are usually a function of the service fees paid in the past or the projected service fees if the agreement had continued.

25. What remedies are available to the contracting parties?

Where the termination is because of material breach, the terminating party can claim damages from the terminated party. Many agreements include other remedies, for example, early termination for breach, the right to require remediation or payment or withhold (part of the) payment. In addition, many outsourcing contracts include the following remedies:

- The right for the customer to terminate the provision of some specific services (partial termination).
- Liquidated damages and service credits.
- Indemnities for specific types of loss (for example, data protection, confidentiality, regulatory non-compliance or IP).
- The customer's right to require the supplier to re-provide the relevant services to the appropriate service standard or a step-in right, enabling the customer to take over the services itself or appoint a third party to manage the service on its behalf.

Exit Arrangements

26. What mechanisms are commonly used to address exit and post-termination transition issues?

Outsourcing agreements often include provisions on the transition of services to another supplier. The customer might require some services to overlap with the new service provider's services, to avoid any disruptions in their business activities.

In principle, if the parties have not included a clause in the outsourcing agreement, the supplier has no implied rights to continue to use licensed IP rights following the termination of the agreement. If the supplier wishes to continue to use of the licensed IP rights, it should negotiate a separate licensing agreement.

Confidentiality clauses will in most cases have effect even after the termination of the outsourcing agreement.

27. To what extent can the customer (or if applicable, its new service provider) gain access to the service provider's know-how post-termination and what use can it make of it?

If the parties have not included a clause in the outsourcing agreement, the customer has no right to gain access to the supplier's know-how after termination. If the customer wishes to continue to use the supplier's know-how, it should negotiate a separate licensing agreement.

Liability, Exclusions and Caps

28. What liability can be excluded?

Exclusions and limitations of liability are, in principle, permitted under the doctrine of freedom of contract. For example, it is very common to exclude liability for indirect and consequential loss. However, the extent to which contractual liability can be excluded or limited is subject to limitations:

- A limitation or exclusion of contractual liability cannot result in the erosion of the obligations of a contracting party.
- A party cannot exclude their own:
    - intentional fault;
    - fraud; or
    - fraudulent misrepresentation.
- The clause must not be contrary to mandatory law or public order and morality.
- Exclusion or limitation of liability must not lead to an imbalance in the relationship between the contracting parties.

A party cannot be released from its liability for the non-execution of the essential obligations that are the subject matter of the agreement for its wilful misconduct, its gross negligence or that of its agents, except in cases of force majeure (*Act of 4 April 2019*).

29. Are the parties free to agree a cap on liability and, if desirable, a cap on indemnities? If so, how is this usually fixed?

Limitation and exclusion of liability clauses cannot completely erode the meaning of the agreement to render the obligations of the parties under the agreement meaningless (because insufficient liability is attached to them). Often, a liability cap is foreseen to limit the liability to a determined period of service fees. If an excessively low liability cap is stipulated in the contract, this may undermine the agreement and a court can consider the limitation or exclusion of liability clause null and void.

It is common practice in outsourcing contracts to provide for a total and aggregate liability cap that is a function of the total contract value and/or a yearly liability cap that is a function of the yearly contract value. Exceptions to the liability cap are made for:

- Intentional fault.
- Fraud.
- Fraudulent misrepresentation.
- Gross negligence (see *Question 28*).

In addition, it is common for outsourcing agreements to exclude all or certain indemnities from the liability cap. Finally, in more complex outsourcing arrangements, specific (higher) liability caps may be agreed for certain matters (for example, data protection) or specific, capped indemnities may be agreed for certain matters.

30. What other provisions may be included in the contract to protect the customer or service provider regarding any liabilities and obligations arising in connection with outsourcing?

Other protection mechanisms to protect the customer or service provider are, in principle, permitted under the doctrine of freedom of contract.

The parties are therefore free to stipulate any particular safety mechanisms as considered appropriate in the context of the outsourcing relationship. For example, to further limit liability, outsourcing contracts sometimes include time limitations for contractual claims (for example, claims must be made within one year as of the claim arising). Furthermore, liability for loss of data is sometimes limited to the cost of putting back the last available backup.

Dispute Resolution

31. What are the main methods of dispute resolution used?

It is important to consider the preferred method of dispute resolution during contract negotiations and not only when a dispute arises. Therefore, the dispute resolution procedure is often defined in the agreement. Given the complexity of outsourcing contracts, the disputes that can arise are various, including those concerning the respective obligations of the parties, termination or transfer of the contract. Many agreements provide for amicable solutions for example, negotiation or mediation before formal proceedings in the courts of arbitration. Where arbitration is preferred, the matter is often referred to arbitration under the rules of arbitration of the Belgian Centre for Arbitration and Mediation (*Het Belgisch Centrum voor Arbitrage en Mediatie*) (CEPANI/CEPINA).

In technical or commercial disputes (for example, benchmarking of the price or price adjustments during the term of the contract), parties often rely on mini-arbitration or a third-party decider (for example, an expert). These alternative dispute resolution mechanisms are frequently chosen as the proceedings are confidential and faster than regular proceedings. However, parties also often revert to legal proceedings before courts and tribunals.

Disputes in respect of exit of services and transition from one vendor to another are not very common in Belgium.

Tax

32. What are the main tax issues that arise on an outsourcing?

Transfers of Assets to the Supplier

Value added tax (VAT) may be due for the assets transferred. However, in most cases, the book value or market value of the assets involved are low and do not drive the structure of the deal.

The transfer, for consideration or free of charge, of a totality of goods or of a division of a business, where the transferee is a taxable person who could deduct all or part of the tax due as a result of the transfer is exempt from VAT (Article 11, VAT Code). Therefore, certain transactions may be exempt from VAT where transferee is deemed to continue the person of the transferor.

Transfers of Employees to the Supplier

No specific taxes apply. The parties must ensure that from the date of the transfer, the supplier is liable for wage taxes and social security contributions. The transfer itself may create some operational discussions with the tax and social security authorities. For example, discussions may arise as regards to measures to harmonise the employment conditions of the transferring employees with those of the existing employees of the supplier.

VAT or Sales Tax

VAT may apply to the services depending on the location of the vendor. VAT applies in accordance with the general rules, and there are no specific exceptions for outsourcing.

Service Taxes

No specific taxes apply.

Stamp Duty

No stamp duty applies.

Corporation Tax

No specific taxes apply in the event of outsourcing. The supplier pays corporate income taxes on the income generated from the provision of outsourcing services.

Contributor Profiles

Bastiaan Bruyndonckx, Partner

Lydian
T +32 2 787 90 93
F +32 2 787 90 99
E *bastiaan.bruyndonckx@lydian.be*
W *www.lydian.be*

Professional and academic qualifications. Attorney at law, Brussels Bar, Belgium; Law degree, Catholic University of Leuven,1994, (*magna cum laude*); LLM, University of Chicago Law School,1996

Areas of practice. Information and communication technology law, with a particular focus on information governance; technology procurement and outsourcing contracts; electronic communications and e-commerce. Heads the Information and Communication Technology (ICT) and the Information Governance and Data Protection (Privacy) teams.

Recent transactions

- Companies in a broad range of industry sectors on data protection (privacy) matters. Extensive experience in ICT-related transactions, including large software licensing, development and implementation projects.
- Advising customers and suppliers on various types of outsourcing projects.

- Advising telecom-sector and other clients on electronic communications regulatory issues.
- Drafting and negotiating agreements in the field of electronic communications.
- Assisting clients on various e-commerce (B2B, B2C and C2C) and internet projects as well as on long-term, technology-driven strategic agreements, including in the framework of M&A transactions.
- Cybersecurity, cybercrime and contentious ICT matters.

Professional associations/memberships. Fellow of the Belgian American Educational Foundation (BAEF); member of the International Association of Privacy Professionals (IAPP); Certified Information Privacy Professional – Europe (CIPP/E).

Publications

- *World Data Protection Report.*
- *Data Guidance.*
- *Computerrecht (Computer Law).*
- *Privacy & Informatie (Privacy & Information).*

Liese Kuyken, Associate

Lydian
T +32 2 787 91 34
F +32 2 787 90 99
E *liese.kuyken@lydian.be*
W *www.lydian.be*

Professional qualifications. Attorney at law, Brussels Bar, Belgium

Areas of practice. Contractual and commercial law, particularly data protection (privacy) and information and communication technology (ICT); data protection law, including processing agreements, privacy and cookie policies and the rights of data subjects; and complex telecom-related (service) agreements.

END OF DOCUMENT