Chambers
Global Practice
Guides

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Outsourcing 2021

Netherlands: Law & Practice
and
Netherlands: Trends & Developments

Herald Jongen, Nienke Bernard,
Eduard Stein and Thomas Timmermans
Greenberg Traurig, LLP

practiceguides.chambers.com

NETHERLANDS

Law and Practice

Contributed by:
Herald Jongen, Nienke Bernard, Eduard Stein and Thomas Timmermans
Greenberg Traurig, LLP see p.8

CONTENTS

Contributed by: *Herald Jongen, Nienke Bernard, Eduard Stein and Thomas Timmermans,*
Greenberg Traurig, LLP

1. OUTSOURCING MARKET

1.1 IT Outsourcing

As a result of COVID-19, hyperscalers and other vendors of colo and hosting services, as well as suppliers of videoconferencing (VC) solutions and webinar systems have seen their business grow exponentially.

The key market developments in IT outsourcing are:

- significantly heightened awareness of, and focus on privacy and data security;
- an increasing focus on "as-a-service" contracts to replace traditional models;
- transition to the cloud, including service providers themselves moving to IAAS;
- service integration and architecture integration are of increasing importance, since customers work with a larger number of vendors; and
- the role of IT departments is under pressure; service providers often work directly with the business within the customer.

COVID-19 has had a huge impact on the use of technology. During the lockdowns at least 70% of the workforce worked from home, almost always using remote access systems, VC and phone. VC has replaced phone conversations at least for 75%. The expectation is that working from home will be the new normal for 20% of the time. Furthermore, online shopping has seen dramatic growth figures, that will last. In many ways, what was expected to take five years has happened in five weeks. People realise that life can be organised and led differently.

1.2 Business Process (BP) Outsourcing

As a result of COVID-19, BP outsourcing (BPO) is expected to grow, since management has seen that many business processes can be performed remotely. It is just one step further to outsource such processes.

The key market developments in BPO are:

- in BPO it is less about labour arbitration and costs savings, and more about technology transformation and automation;
- TUPE staff transfers under the Acquired Rights Directive become less common because the parties (including the employees) arrange otherwise (which quite often means that the employees are offered an attractive redundancy package); and
- companies are implementing Robotic Processing Automation (RPA) as an alternative for BPO, but most programs are not yet yielding the intended results.

1.3 New Technology

As a result of COVID-19, relatively new technologies have been rapidly accepted and enjoy widespread use; VC is maybe the best example. The quality of VC has substantially improved as a result of more efficient use of bandwidth.

The impact of new technology is as follows:

- customers are increasingly struggling to build up internal capabilities to address new technologies and are therefore relying more on IT providers;
- AI and robotics heavily impact suppliers in their delivery centres that were traditionally built around labour arbitration; and
- blockchain/smart contracts are typically applied in a larger ecosystem which requires a different mode of cooperation from traditional client-supplier relationships. The importance of these technologies is currently negligible, but it is believed this may change soon due to an increase in professional offerings from reputable service providers.

2. REGULATORY AND LEGAL ENVIRONMENT

2.1 Legal and Regulatory Restrictions on Outsourcing

Rules and restrictions on outsourcing apply only in some regulated markets, primarily the financial, insurance, asset management and pensions industries. In other markets, freedom of contract rules.

2.2 Industry-Specific Restrictions

Industry specific restrictions mainly exist in the financial, insurance, asset management and pensions industries and the regulations are, mostly, based on EU legislation. The regulations concerned include the Dutch Financial Supervision Act (FSA) and a number of directives and resolutions under that Act, the Solvency II Directive and the Solvency II Regulations, the AIFMD, the Pension Act, the Dutch Central Bank's (DNB) Good Practices for insurers and (separate) for other sectors, the EBA guidelines on outsourcing to cloud service providers. The main principles of these regulations boil down to the following:

- responsibility cannot be outsourced;
- the requirement of a written agreement that contains sufficient means for the customer to monitor performance;
- mandatory disclosure by the supplier of circumstances that may affect continuity;
- sufficient audit rights for the customer;
- requirement of a risk analysis;
- in some sectors the customer must be able to terminate at will (against a termination fee); and
- giving notice of the intended outsourcing to the supervisors is often required.

2.3 Legal or Regulatory Restrictions on Data Processing or Data Security

The restrictions on data processing and data security are based on the EU General Data Protection Regulation (GDPR), meaning that export from personal data outside the EU is not allowed unless proper contractual documentation and technical measures are in place. Furthermore, specific, highly sensitive data held by the Dutch government may not be stored in the cloud.

Data security is mainly governed by the law on the security of network and information systems (the "Cyber Security Act"), which implements the EU Directive on the security of network and information systems (the "NIS Directive") and consolidates other relevant legislation into one act. The Cyber Security Act establishes a certification framework for IT digital products, services and processes. The NIS Directive identifies sectors which are vital for the aspects of economy and society which rely heavily on IT, such as energy, transport, banking and health care. These sectors have to take appropriate security measures and ensure swift notification of any incidents to the relevant authorities. In addition, in keeping with the NIS Directive, the Cybersecurity Act also obliges providers of digital services (other than small enterprises) under Dutch jurisdiction to notify material data breaches in respect of its services to the National Computer Security Incident Response Team and the Minister of Economic and Environmental Affairs.

After the 2020 Schrems II ruling, in which the European Court of Justice decided that the transfer of personal data from the EEA to the United States could – with immediate effect – no longer be based on the so-called Privacy Shield, the permissibility of transfers of personal data to outside the EEA and in particular the USA was a topic of debate. The European Data Protection Board published much anticipated guidance in their "Recommendations on supplementary measures" in June 2021, that include additional measures that need to be applied to data transfers under "Standard Contractual Clauses".

2.4 Penalties for Breach of Such Laws

In accordance with the GDPR, the penalty for a breach is a maximum of 4% of the worldwide turnover of the group belonging to the company that breached the legislation.

Under the Cybersecurity Act, the maximum penalty amounts to EUR5 million.

2.5 Contractual Protections on Data and Security

Contracts usually contains the following contractual protections regarding data protection:

- an obligation for the supplier to give notice to the customer of a data breach within 24-48 hours;
- a detailed data processing agreement between the customer as controller and the supplier as processor;
- in the case of a data export from the EU, the Standard Contractual Clauses can be used; and
- very specific and concrete purpose limitations (see Article 6, paragraph 1 (a) of the GDPR).

If parties wish to avoid Cambridge Analytica type of risks, they shall include more limitations than covered by the GDPR, mainly on profiling and advertising.

Regarding security contracts mainly contain the following contractual protections:

- an obligation on the supplier to implement market standard physical technical and procedural security measures;
- an obligation to maintain and report on certain certifications (eg, ISO27001, ISAE3000, ISAE3402, etc);
- an obligation to comply with the customer's security policies;
- a right for the customer to undertake penetration testing via a third party;
- an obligation on the supplier to report actual or potential security breaches; and
- an obligation to have a business continuity plan and disaster recovery plan in place, concurrent with frequent testing.

3. CONTRACT MODELS

3.1 Standard Supplier Customer Model

There is no standard outsourcing agreement in the Netherlands.

The association of IT suppliers NL Digital has standard terms, but these do not, generally, apply to outsourcing. Sourcing Netherlands, the association for outsourcing, has developed a balanced standard form for an outsourcing agreement, which is sometimes implemented. Sophisticated customers will contract on the basis of their own tailored agreement. These agreements are similar to the market standard agreements in the UK and USA. They are very detailed and contain approximately 20 schedules.

The usual model consists of an asset transfer agreement and a separate services agreement. For large cross border projects, a framework structure is used, comprising a framework asset transfer agreement and a separate framework services agreement, under which local-to-local asset transfer agreements and services agreements are concluded.

3.2 Alternative Contract Models

Although alternative models are sometimes used, 95% of outsourcing will be contracted, one-on-one, with an asset transfer agreement and a separate services agreement. Multi-vendor agreements (between the customer and a number of suppliers) are also common. Joint ventures (JVs) are rare, mainly because a JV structure is rather complicated and expensive.

It will only be used where the customer and suppliers wish jointly to set up a new business.

3.3 Captives and Shared Services Centres

Originally, SSCs were set up to centralise and rationalise the IT environments. Later, labour arbitrage (ie, the reduction of the costs of labour) became a factor and, as a result there of, many SSCs were moved to nearshore and offshore locations. Lately, a number of captive SSCs have been transferred to suppliers. Also being seen is captive SSCs co-operating more closely with suppliers in order to benefit from the newest technologies and innovation.

4. CONTRACT TERMS

4.1 Customer Protections

The main customer protections are the following:

- no exclusivity for the supplier;
- no volume commitment on the customer;
- a detailed service description;
- appropriate service levels;
- tailored service credits;
- an appropriate governance and contract change structure;
- a benchmarking clause (like-for-like comparison of pricing and service levels);
- a step-in right;
- GDPR compliance; and
- an audit clause.

4.2 Termination

The customer can terminate the contract for cause. Serious breaches of services levels and severe data security and privacy incidents are often specifically mentioned as providing cause for termination. Sometimes, outsourcing or services agreements provide a termination right to the customer where there has been a change of control in the supplier, especially in contracts relating to mission critical services or services provided to regulated financial institutions.

Customers can also, almost always, terminate for convenience. In the case of termination for convenience, the customer must pay termination compensation. There is no fixed formula for calculating this compensation as this is a matter of freedom of contract. In general, the compensation consists of unrecovered costs and a small lost-margin component. Furthermore, in the financial industry the customer may terminate the agreement if a regulator requires a termination.

The supplier can usually only terminate for material breach (most notably, prolonged non-payment of invoices). It is highly unusual to allow a supplier to terminate for convenience.

4.3 Liability

Dutch statutory law does not define the difference between direct loss and indirect loss. Under the influence of Anglo-American contracts and terms, the concept is often used in Dutch law agreements. In such an event, it is wise to define exactly the damages considered direct and those considered indirect. However, it can be hard to reach agreement on these distinctions as the customer will try to include as much as possible under the definition of direct damages while the supplier wishes to exclude as much as possible from this definition.

It may, therefore, be better practice to refer to the statutory definition of damages and leave the decision to the courts. This means that damages that are reasonably attributable to the event that caused the damages, and to the party that caused the damages, must be paid. In addition, pure loss of profit and turnover can be excluded.

The liability of both parties must always be capped. The market standard caps vary between 12 and 36 months of fees.

4.4 Implied Terms

Dutch law provides for certain implied terms in relation to inter alia the quality of goods sold and the provision of services. However, these implied terms are typically not mandatory in B2B contracts and are usually explicitly excluded or superseded by the contents of the contract.

5. HR

5.1 Rules Governing Employee Transfers

The rules governing employee transfers in outsourcing are based on the EU Acquired Rights Directive (ARD). Under the ARD, employees who are predominantly working on the activities that are to be transferred will, where the ARD (as implemented in the Netherlands) applies, transfer to the supplier together with their applicable employment terms and conditions, by operation of law. In general, the ARD will apply if significant assets are to be transferred to continue the economic activity or, in case of labour-intensive activities, the majority of the employees (considering number and/or skills) are offered employment by the new service provider. The EU and Dutch case law on ARD/TUPE is numerous and granular, but at essence is based on an ever-increasing protection of employees, which should ensure that employees "follow their work".

5.2 Trade Union or Workers Council Consultation

Works council consultation (ie, a right of advice prior to implementing the proposed decision) is almost always required (under Article 25 of the Dutch Works Councils Act).

Trade union consultation is required if control in (part of) the "undertaking" is transferred or if this requirement follows from the applicable collective labour agreement.

Trade union consultation is also required where 20 or more employees are made redundant within a timeframe of three months.

5.3 Market Practice on Employee Transfers

Market practice on employee transfers in the Netherlands is:

- application of the principles of the ARD, as described in **5.1 Rules Governing Employee Transfers**; and
- staff transfers under the ARD become less common because the parties (including the employees) arrange otherwise, which quite often means that the employees are offered an attractive redundancy package.

6. ASSET TRANSFER

6.1 Asset Transfer Terms

There are no specific rules that apply to asset transfer agreements and freedom of contract prevails. Typical terms include:

- the description of the assets that transfer, usually concerning hardware, software, licence agreements and people;
- the price of the assets, typically being the book value or the fair market value;
- an "as is, where is" guarantee; and
- terms regarding the transfer of employees, including indemnities for unintended transfers.

Contributed by: *Herald Jongen, Nienke Bernard, Eduard Stein and Thomas Timmermans,* ***Greenberg Traurig, LLP***

Greenberg Traurig, LLP is an international law firm with approximately 2,200 attorneys serving clients from 40 offices in the United States, Latin America, Europe, Asia, and the Middle East. The firm's dedicated technology and outsourcing team advises on a full range of legal issues impacting outsourcing situations, including tax implications, employment, real property and intellectual property issues. The global team consists of more than 75 lawyers, six of which are located in Amsterdam. The team structures and negotiates the full spectrum of services for clients, from standard transactions to highly complex multinational transactions. Recent transactions include cross-border BPO projects for multinational banks, insurance companies and asset managers.

AUTHORS

Herald Jongen is a shareholder at Greenberg Traurig. He has more than 30 years of experience and focuses his practice on outsourcing, technology transactions and strategic relationships. He has particular expertise in leading complex multi-jurisdictional projects, in technology and in the financial industry. He has led projects in many different countries. Recently he negotiated for the Dutch and other governments and public institutions with Microsoft and Google. He published a loose leaf on International Outsourcing Law and Practice and he frequently lectures on outsourcing.

Nienke Bernard has worked on a large variety of technology transactions, including outsourcing, licensing and joint ventures. She has particular expertise in privacy law and contract law.

Eduard Stein is a senior technology lawyer at Greenberg Traurig with extensive experience across many industries. He has broad and deep knowledge of IT, IP, privacy and contract law. He combines legal experience with commercial acumen and technical knowledge, holding an MBA from INSEAD and having worked as a strategy consultant at the Boston Consulting Group and as a Digital and IT Strategy Consultant at Royal Dutch Shell.

Contributed by: *Herald Jongen, Nienke Bernard, Eduard Stein and Thomas Timmermans,*
Greenberg Traurig, LLP

Thomas Timmermans is a shareholder at Greenberg Traurig. He advises and represents national and international clients across a broad range of employment and employee benefits issues. His experience includes high-level exits, large restructurings, employee representation, employee benefits, strategic employment issues and cross-border corporate law-related employment matters. Within these areas of law, Thomas has particular knowledge and experience in the field of outsourcing, transfer of undertakings in light of the EU Acquired Rights Directive (ARD) and works council consultation procedures.

Greenberg Traurig, LLP

Leidseplein 29
1017 PS Amsterdam
The Netherlands

Tel: +31 651289 224
Email: Jongenh@gtlaw.com
Web: www.gtlaw.com

Trends and Developments

Contributed by:
Herald Jongen, Nienke Bernard, Eduard Stein and Thomas Timmermans
Greenberg Traurig, LLP see p.13

Life after Schrems II and COVID-19

Schrems II

In its 2020 Schrems II ruling, the European Court of Justice (the "Court") decided that the transfer of personal data from the European Union to the United States could no longer be based on the so-called Privacy Shield. The standard contractual clauses (SCCs) for the transfer of personal data to processors in third countries as adopted by the European Commission remained valid. However, the Court emphasised the responsibility of data controllers to assess on a case-by-case basis whether the SCCs provide an adequate level of protection for a specific transfer.

Because this assessment needs to be based on the same elements that led to the invalidation of Privacy Shield, Schrems II caused widespread uncertainty about the permissibility of transfers based on SCC in specific circumstances, in particular for transfers to third countries where authorities have broad powers for mass surveillance, such as the USA.

So far, 2021 has shown that the SCCs are "here to stay", and can continue to be used for transfers to outside of the EEA provided that additional measures are taken where required. In this respect, the European Data Protection Board published important guidance in its "Recommendations on supplementary measures" that provides guardrails on how to carry out so-called "data transfer impact assessments". In addition, the European Commission published a new set of modernised SCCs that replace the previous SCCs. The previous SCCs can no longer be used for new contracts as of 27 September 2021. Contracts entered into on the basis of the "old" SCCs before that date remain valid until December 2022.

Although 2021 has taken away some uncertainty about data transfers in the post-Schrems II era, the debate about the permissibility of and safeguards surrounding data transfers is far from over. Controllers and processors transferring personal data to outside of the EEA are advised to closely monitor developments and adjust their data practices accordingly.

COVID-19

COVID-19 has had a huge impact on the way people in the Netherlands work, shop and live. Since the first lockdown there have been hardly any traffic jams, no overcrowded public transport, 75% of people work from home, and online shopping has seen a growth that was expected to take at least three years, among others. It is clear that this will have a structural effect: these developments will be the new normal.

As a result, retail food shops and suppliers and providers of IT cloud services have seen their turnover and profits rise dramatically. Dutch employers and the big cities are encouraging people to work more flexible (start later, etc, to avoid traffic and transport jams) and to work from home also after COVID-19. And it is expected that business process outsourcing will grow because management has seen that it works remotely.

Judgments during COVID-19

There have been a multitude of judgments in Dutch courts, relating to the extent in which COVID-19 can be used as a grounds to excuse

Contributed by: *Herald Jongen, Nienke Bernard, Eduard Stein and Thomas Timmermans,*
Greenberg Traurig, LLP

performance of an obligation, often relating to lease agreements.

In general, Dutch courts have not found COVID-19 to provide grounds for force majeure as COVID-19 is not normally the proximate cause of the inability to perform, rather, it acts indirectly by causing economic or social circumstances resulting in an inability to perform (eg, the inability to pay rent). However, Dutch courts have often found grounds to alter parties' agreements based on unforeseen circumstances. This is regularly used as the grounds to, eg, reduce the lease obligations of tenants.

This appeal to unforeseen circumstances is often, but not always, successful. In particular, where a party has explicitly chosen to accept a certain risk, and that risk is augmented by COVID, courts may leave the apportionment of risk intact between the parties nonetheless, eg, in a real estate transaction where a party had intentionally not included the customary condition precedent of obtaining adequate funding, the courts did not find cause to alter the agreement or excuse performance when that party was unable to obtain funding under the more stringent criteria applied due to COVID-19.

Transition to the cloud

In 2021, the trend to transition to as-a-service solutions and cloud-based models continues. From a legal perspective, classic waterfall contracts and SLAs are less popular as parties have moved towards agile working and DevOps methodologies.

The shift to the cloud continues to the spark debate in Dutch media and politics, particularly about alleged abused of market power by big tech and the use of foreign cloud providers in sectors such as healthcare, education and government. Overall, government and thought leaders remain pro-innovation and pro-tech, but practices are being contested and tested against the key principles underlying existing regulation.

Digitalisation remains on the agenda of Dutch regulators such as the Dutch Central Bank (*De Nederlansche Bank* or DNB) and the Authority for Consumer and Market (*Autoriteit Consument en Markt* or ACM). In May 2021, the ACM started an investigation into the cloud services market in the Netherlands aimed at identifying whether the market works adequately for businesses and consumers. In this context, the ACM will analyse how the cloud services work at a technical level, as well as investigate whether any market imperfections (eg, vendor lock-in, information asymmetry) exist. If necessary, based on these findings, the ACM will conduct more in-depth investigations.

Outsourcing in the financial sector

Outsourcing in the financial sector is subject to strict regulations, and continues to be an important point of focus of the Dutch regulators. In June 2021, following an investigation into outsourcing by financial services providers (eg, customer lenders (non-banks), intermediaries and financial advisors), the AFM published a "good practices" document to address areas of non-compliance in the sector, particularly relating to the requirement to enter into agreements with contractors.

GDPR compliance

The Dutch State is a trail blazer in Europe regarding the GDPR compliance of cloud products. The Ministry of Justice created a dedicated procurement department of top specialists to negotiate with Microsoft, Google, AWS and IT suppliers. This led to a landmark agreement with Microsoft on the basis of which Microsoft agreed to make changes in the code of a number of core cloud offerings (including Office 365 and Azure) so that these now comply with the GDPR. Furthermore,

Microsoft agreed to changes of their Online Service terms, also to comply with the GDPR.

As a result, the 350,000 civil servants of the Dutch State as well as some 100,000 civil servants of lower (semi) public entities can now use these services in a compliant manner. It is widely believed that Google will soon agree to similar changes. Details and the data protection impact assessments that formed the basis for the negotiations can be found on the website of the Ministry of Justice.

Class Actions Act

An interesting development is the entry into force of the Collective Damages in Class Actions Act (the Act) in January 2020. This Act paves the way for class actions through Dutch courts, including for breaches of data protection legislation. Under the Act, an organisation may claim monetary damages for its members, provided that the action has a sufficiently close connection with the Netherlands.

In August 2020, the organisation Privacy Collective launched the first GDPR-related class action against Oracle and Salesforce for the alleged unlawful processing of personal data of Dutch internet users. This has since been followed-up by clams brought against Facebook and TikTok by the Dutch Consumer Association and the Data Privacy Foundation (Facebook only). These claims are all still mid-proceeding. However, in respect of Facebook Dutch courts have already thrown out Facebook's preliminary defense that Dutch courts do not have jurisdiction.

It is widely believed that ever more GDPR related class actions will follow in the coming years, especially relating to data security breaches. These cases will be brought by consumer watchdogs, but there is also a very real expectation that lawyers will view these types of class actions as an attractive business model and will set-up foundations specifically to pursue them. Note that the cases brought thus far generally relate to unlawful processing due to lack of an adequate grounds. Both customers and suppliers should therefor expect that where they process significant amounts of personal data and their business has a high media profile there is a real risk suits will be brought if bend and stretch the rules.

Contributed by: *Herald Jongen, Nienke Bernard, Eduard Stein and Thomas Timmermans,*
Greenberg Traurig, LLP

Greenberg Traurig, LLP is an international law firm with approximately 2,200 attorneys serving clients from 40 offices in the United States, Latin America, Europe, Asia, and the Middle East. The firm's dedicated technology and outsourcing team advises on a full range of legal issues impacting outsourcing situations, including tax implications, employment, real property and intellectual property issues. The global team consists of more than 75 lawyers, six of which are located in Amsterdam. The team structures and negotiates the full spectrum of services for clients, from standard transactions to highly complex multinational transactions. Recent transactions include cross-border BPO projects for multinational banks, insurance companies and asset managers.

AUTHORS

Herald Jongen is a shareholder at Greenberg Traurig. He has more than 30 years of experience and focuses his practice on outsourcing, technology transactions and strategic relationships. He has particular expertise in leading complex multi-jurisdictional projects, in technology and in the financial industry. He has led projects in many different countries. Recently he negotiated for the Dutch and other governments and public institutions with Microsoft and Google. He published a loose leaf on International Outsourcing Law and Practice and he frequently lectures on outsourcing.

Nienke Bernard has worked on a large variety of technology transactions, including outsourcing, licensing and joint ventures. She has particular expertise in privacy law and contract law.

Eduard Stein is a senior technology lawyer at Greenberg Traurig with extensive experience across many industries. He has broad and deep knowledge of IT, IP, privacy and contract law. He combines legal experience with commercial acumen and technical knowledge, holding an MBA from INSEAD and having worked as a strategy consultant at the Boston Consulting Group and as a Digital and IT Strategy Consultant at Royal Dutch Shell.

Contributed by: *Herald Jongen, Nienke Bernard, Eduard Stein and Thomas Timmermans,*
Greenberg Traurig, LLP

Thomas Timmermans is a shareholder at Greenberg Traurig. He advises and represents national and international clients across a broad range of employment and employee benefits issues. His experience includes high-level exits, large restructurings, employee representation, employee benefits, strategic employment issues and cross-border corporate law-related employment matters. Within these areas of law, Thomas has particular knowledge and experience in the field of outsourcing, transfer of undertakings in light of the EU Acquired Rights Directive (ARD) and works council consultation procedures.

Greenberg Traurig, LLP

Leidseplein 29
1017 PS Amsterdam
The Netherlands

Tel: +31 651289 224
Email: Jongenh@gtlaw.com
Web: www.gtlaw.com