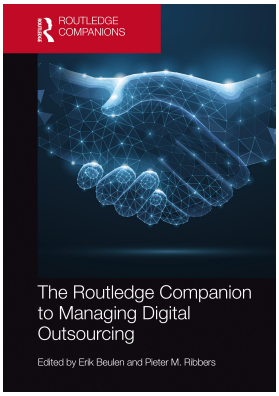

The Routledge Companion to Managing Digital Outsourcing

Erik Beulen, Pieter M. Ribbers

Parties, partners and the law. Some contractual and compliance issues in digital outsourcing

Publication details
https://test.routledgehandbooks.com/doi/10.4324/9781351037785-15
Kees (C.) Stuurman
Published online on: 28 Jul 2020

13

PARTIES, PARTNERS AND THE LAW. SOME CONTRACTUAL AND COMPLIANCE ISSUES IN DIGITAL OUTSOURCING

Kees (C.) Stuurman

13.1 Introduction

In this chapter, we will focus on a number of trends that need attention when designing and implementing contracting structures to successfully support digital outsourcing transactions. Specifically, we will focus on: (1) partnerships requiring a shift of focus on relationships rather than delivery per se, (2) the consequences of the proliferation of parties involved (networks vs. single suppliers) and finally (3) the impact of growing compliance pressure on the chain of parties involved in the delivery of outsourcing services.

"Partnership" has been a buzzword in the IT scene long before an actual realization thereof was seemingly aimed at. Nowadays, the approach to successful technology-driven cooperation has become more mature. This however has consequences for outsourcing contracts[1] as well; real partnerships require a significant focus on the actual process of communication and cooperation, including dealing with disputes, rather than "only" KPI-driven service delivery.

Outsourcing as a tool for transforming organizations usually requires input from a range of capabilities. In the IT industry, the process of specialization has been ongoing for a long time already. In practice, this implies a growing range of subcontractors is being involved in the delivery of outsourcing services. In the contractual architecture, this is however often not reflected as the customer usually only enters into a contract with a single (main) supplier. Typically, the main contractor is responsible for its subcontractors. The main contractor is hence the single entry point. In this approach, the customer is fully dependent on the extent to which the main contractor effectively enforces the performance of its subcontractors since the customer has in general no legal basis for directly safeguarding his interests in relation to subcontractors providing vital services. Multi-party arrangements can provide a solution for these vulnerabilities.

Digital driven organizations have become subject to an increasing compliance pressure over the last few years. Data protection and cyber security are leading themes in this respect. Other, more sectoral driven legislation adds to the picture. Cooperation with a network of suppliers/partners implies that compliance becomes a multi-party issues in which the suppliers/partners have to work very closely with their customer in order to allow the customer to meet increasingly strict legal obligations. Very significant penalties, such as

those applicable under the recent EU General Data Protection Regulation (GDPR) and increased reputation risks, are strong incentives for drafting adequately protective contractual arrangements supporting advanced compliance procedures (including auditing down the chain).

In the next paragraphs, we will first focus on the contractual basis for communication duties and then turn to multi-party contracting followed by a paragraph on the impact of compliance issues on the content of outsourcing contracts.

13.2 Partnerships: the contractual approach to communication

13.2.1 Introduction

Creating a "partnership" is often depicted as the holy grail for successful technology projects. As the word "partnership" is (very) multi-interpretable, everybody can have its own take, as can be seen often in marketing-driven communications involving complex technology transactions, like outsourcing. Both rather one-sided supply relationships as well true risk and benefit sharing forms of cooperation are labeled as "partnerships."

The legal side of partnerships potentially covers a wide array of issues, including the form in which the partnership operates (contractual, legal entity, etc.), the division of risks and responsibilities, potential competition law issues, etc.

In this paragraph, we will focus on a very specific aspect of partnerships: communication. In our view and experience from legal practice, this is one of the key factors setting (true) partnerships apart from more traditional customer-supplier relationships and the single most important factor for achieving success in complex outsourcing relationships.

In the next paragraph(s), we will discuss the way communication is structured as part of the contract, the potential supplementary effects of applicable statutes and some specific requirements that might apply.

13.2.2 Communication clauses

When analyzing outsourcing contracts from a communication perspective, it can be observed that usually the parties include a specific "communication clause" in their contract.

In such clause, various aspects are being covered, including:

- the obligation to inform each other, e.g. on "matters or circumstances that preclude proper performance"[2] or, even broader, "(…) keep each other informed of developments and changes that are or may be of importance to the performance of the Contract";[3]
- the channels or levels of communication, e.g. strategic, tactical operational, including a matrix linking types of issues and levels of communication;
- the format for communication, e.g. written reports, email, meetings, etc.;
- the language for communication;
- the process flow for the communication, in particular timelines for submission, decision-making (adoption, rejection, amendments), feedback and (other forms of) follow-up.

Commonly, this type of clauses is supported by one or more schedules setting out further procedural details, persons or functions involved, contact details and other operational aspects.

The incorporation of a specific communication clause might, when analyzing a contract, easily detract from the fact that such usually more "sweeping statements" are supplementing more specific communication duties that are "written all over" an outsourcing contract. Key examples include clauses on governance, service level evaluation, change procedures, acceptance procedures, contract management, reporting, audits, benchmarking as well as dispute resolution. All these clauses describe a certain process with an important communication component.

When analyzing the overall effect of commercial contracts in terms of communication obligations, one can in general distinguish several sources for such duties. In relation to outsourcing contracts, the following sources for communication duties are most relevant: (1) the text of the relevant clauses in the contract, (2) statutory obligations, (3) legal principles (e.g. good faith) and (4) the interpretation of the contract. The latter being in practice, although clearly relevant, often of somewhat less significance than the other sources. We will discuss the first three sources in more detail below.

13.2.2.1 The text of the contract

Above we gave a number of examples of key contract clauses with a major communication component, such as clauses on governance, service level evaluation, change procedures, acceptance procedures, contract management, reporting, audits, benchmarking and dispute resolution. These types of clauses can be categorized in several ways including:

- pre-defined reporting duties, like on KPI's, test results (…), etc. Basically, this concerns communications of which the content is delineated on forehand with "tangible" parameters. With providing the report, the party involved (usually the supplier) shows complying with a specific contractual obligation;
- open reporting duties, like these focusing on signaling risks or other (potentially) adverse consequences. The content of this type of clauses ("provide all relevant information," etc.; see for other examples above) often approaches the content of the supplementary obligations stemming from general contract law principles (see below);
- formal notifications, including those aimed at:
  - establishing elements of non-performance, including late payments, late approval/discharge, non-compliance with specifications, etc.;
  - compliance with a specific obligation, like sending an audit report, proof of acceptance or proof of approval;
  - formally establishing the existence of a dispute;
  - establishing/conforming a specific legal effect, including notifications relating to audits, notices of default, etc.;
- cooperation clauses obliging the parties to actively exchange information, such as dispute-related clauses reaching beyond the mere exchange of information between the parties by imposing them to cooperate in finding an amicable solution;
- clauses reflecting commercial or technological choices and clauses mandatorily incorporated on the basis of statutes (e.g. imposing security obligations on suppliers or subcontractors as is mandatory under the European GDPR; see below) or on the basis of contracts (e.g. in software distribution related contracts).

When drafting communication-related clauses parties have to deal with various aspects thereof including the means of communication, the content thereof, sender(s), receiver(s),

identification and security. In general, a more formal approach will be chosen when the stakes get higher. It is important to realize that for various reasons, including risk management, this has a fundamental and significant value. It intends to ensure that the safeguards underlying internal hierarchy/authorizations are being applied for careful decision-making on the right level of the organization, being the level on which the impact of the decision for the organization can be weighed taking all relevant information and interests into account. Experience from conflict resolution practice shows that choosing the right communication level and format is of crucial importance for preventing and solving (potential) disputes.

As regards the category of formal communications, it is furthermore important to keep in mind that binding statutory communication requirements will apply in some cases. Often, this will include especially notices of default and notices relating to data protection legislation. Non-compliance with such statutory requirements can have severe consequences. When in the context of termination no prior notice of default is given (which is often mandatory), the court might conclude that the statement aimed at terminating the contract is void and the contractual obligations can still be enforced.

The latter could be the basis for a supplier to claim payment of service fees and damages.

Notwithstanding excellent drafting skills, a contract can never detail all communication that is relevant for giving a partnership in the fundamental sense (risk and benefit sharing). From a legal perspective, such endeavor would also not be advisable as it would (1) render the text of the contract inaccessible and (2) it might give rise to the argument that parties have intended to be exhaustive which might block flexibility being a key requirement in modern outsourcing relations

13.2.3 Statutory communication obligations

13.2.3.1 Statutory obligations to inform

Depending on the type of business process that is being outsourced and the market sector in which the customer operates, various statutory communication duties can be applicable. In principle, these concern the customer but still impact the contract as it will reflect the derived obligation for the supplier to cooperate in enabling the customer to be compliant. A current example of the above is the notification duties relating to data breaches or other cyber security-related incidents. Relevant legislation in the European Union includes the GDPR (in case of breaches in processing of personal data; see below) and the EU Network Information Security Directive (in case of cyber incidents relating to critical infrastructure). Recently, the EU Cyber Security Act[4] has been added to this European framework for cyber security legislation relating to handling of disputes generally contains mandatory reporting/notification duties.

In some cases, the outsourcing supplier will be under an independent statutory obligation to report to the customer. This obligation will supplement the contractual obligations and will hence even apply if the contract does not provide for such duty. An example is the notification obligation for the supplier in case of a data breach when processing personal data under the GDPR for a customer qualifying as controller.

13.2.3.2 Communication duties following from legal principles

Duties to inform do not only arise from explicit contractual provisions but can also be derived from legal principles underlying contract law. A key example in the context of technology projects is the set of information duties based on principles such as

"reasonableness and fairness" or "good faith." In civil law jurisdictions (continental Europe), these principles can act as a basis for supplementing contractual provisions with (unwritten) information duties. These information duties generally encompass (1) the duty to provide relevant information to the other party (on the basis of the knowledge and experience the relevant party has or should have), (2) the duty to investigate (including requesting information from the other party) and – in exceptional circumstances – (3) a duty to warn against damages or other seriously adverse effects. In the context of outsourcing, an example of the latter could for instance be that the supplier warns against the risk of planning a transition in a critical business period. In countries such as France and the Netherlands, these principles have already been applied in IT-related cases as early as the beginning of the 1980s[5] and are still an important tool for judges and arbitrators in dealing with IT disputes.

In key common law jurisdictions, such as the US and the UK, the role of these principles as a source for unwritten obligations is (far) less prominent.[6] In practice, outsourcing agreements across jurisdictions often contain explicit information duties since the parties rather rely on[7] express information duties spelled out in the contract than on the court deriving similar implicit obligations from the contract in case of a dispute.

13.3 Multi-party contracting: challenges and options

13.3.1 Introduction

Specialization is an ongoing process in the technology industry. Projected on outsourcing it implies that the outsourcing ecosystem has become more complex over time, hosting more and specialized companies. To support the growingly complex business process of customers, a range of different skills and competences needs to brought together, supported by an adequate contractual framework.

Interestingly, the legal structure of outsourcing deals seems to lag behind the developments in the industry more and more. However, complex the outsourcing solution is, and notwithstanding involvement of a range of specialized parties, ultimately the deal – with exceptions for a select group of highly complex top-level deals – usually results in a bilateral contract. On the basis thereof, the lead supplier subsequently subcontracts with the other parties involved on the supplier side.

In some cases, multivendor deals result in a "hub and spoke" structure with a series of bilateral contracts between the customer and each of the suppliers involved individually. In some cases, the contract structure is enriched with a type of "coordination agreement" between the various suppliers involved, usually in the form of an Operating Level Agreement (OLA).[8] This kind of agreement is in principle only effective between the supplier and subcontractors involved and does not constitute a binding agreement the customer can enforce when necessary.

The use of bilateral contracts in a multi-party context reduces the complex reality to a straightforward, traditional "customer"-"supplier" structure. This does not mean that the multi-party reality is not taken into account at all; subcontracting relationships are applied to connect other partners in the deal to this bilateral structure. So far, so good or not? In our view, it is time to reflect on the value of more advanced contracting models that better support the business reality and reduce risks involved in the traditional bilateral approach.

13.3.2 Why bilateral contracts are suboptimal

For several reasons, the current standard contracting model is suboptimal. First, the mismatch between the dominantly bilateral contract structure and the business reality impacts the focus of the partners (subcontractor) especially in the supplier ecosystem. Ultimately, their focus is on the supplier and not primarily – as it should be – on the other partners in the ecosystem and the customer, being the ultimate beneficiary of their services. Their contract with – only – the supplier steers them toward meeting the targets agreed with the supplier (and not the customer).[9]

Second, and even more important, the traditional bilateral contracting model introduces a significant risk for the customer. In principle, the supplier is responsible, and liable, for the selection and performance of subcontractors. However in most legal systems, the customer does not have any right of its own to secure enforcement by the subcontractors engaged by the (main) supplier. The latter implies that the customer, in case of supplier default, cannot directly secure his interest toward the relevant subcontractor on the basis of the main outsourcing contract (privity of contract). Let us take the example of a supplier that has engaged an external hosting party. In case an issue arises in their mutual cooperation (e.g. late or non-payment) on the basis whereof the hosting party suspends its performance, the customer can only exert pressure on the supplier but has in no title to act in its own legal right against the hosting party. The latter is vital for securing continuity, access to his data, access to information for meeting notification obligations toward supervisory authorities, etc. Obviously, this can have very severe consequences for the customer.

In the next paragraph, we will explore several potential solutions to deal with the challenges set out above.

13.3.3 Alternative legal frameworks supporting multi-party outsourcing relations

Bilateral contracts in principle only bind the signatories and do not have an effect on third parties. In customer-supplier-subcontractor relationships, this implies that in principle the customer cannot independently act against the subcontractor on the basis of his outsourcing contract with the supplier to ensure compliance. It should be noted that we focus on a common denominator over a range of legal systems and hence some exceptions to this rule could apply in specific jurisdictions or cases. In considering alternative approaches, we will also consider ways of improving the cooperation between the partners in the ecosystem (in terms of enhancing continuity, flexibility, etc.) and not focus on merely claiming damages when things went wrong. As discussed in the previous paragraph, we see an upside in creating a legal framework that not only provides more support for aligning the efforts of the network partners but also provides more safeguards especially for the customers in protecting his interests served by the supplier's subcontractors.

Various options can be considered to improve the quality of the contractual framework for outsourcing from the perspective set out above. In exploring these options, we will distinguish between:

1 solutions that can be qualified as "add-ons" to the current, predominantly bilateral contract structures;
2 multi-party contract solutions;
3 legal entity-based approaches.

13.3.4 Add-on solutions to bilateral contract structures

As we described above, one of the key issues in modern outsourcing relationships is that reducing network relationships to a set of bilateral contracts implies that (even) strong dependencies cannot be securely managed by (in particular) the customer without the active cooperation of the (main) supplier. This creates significant risks especially when subcontractors deliver critical services components for which the supplier cannot deliver backup solutions in case of their non-compliance. The latter is more and more common due to ongoing specialization in the IT industry as we discussed above.

Not only is the customer fully dependent on the supplier for securing his rights, the same holds for other subcontractors as they (usually) only contract with the supplier. The governance of their mutual cooperation hence always requires a triangle relationship: subcontractor 1-supplier-subcontractor 2, creating a potential burden, and hence inefficiencies for an optimal cooperation on the level of the subcontractors.[10] An effective remedy to reduce the risks for the customer is to conclude "safety net" contracts with the individual key subcontractors that contain obligations that can be relied on by the customer in case the supplier does not perform adequately or timely. It is hence to be considered as a "back-up" solution in case of (threatening) non-performance of the supplier.

Such contracts can include clauses aimed at:

- securing adequate direct communication channels between the customer and the subcontractor for specific cases;
- securing payment for the subcontractor when the supplier falls short of (timely) payments, preventing suspension of his obligations by the subcontractor;
- the obligation for the subcontractor to escalate any issues that could threaten the continuity of his service delivery timely to customer directly as well;
- the obligation for the subcontractor to act directly upon instruction of the customer in critical situations;
- the obligation for the subcontractor to cooperate with audits initiated by the customer or supervisory authorities.

Above we gave as an example of this approach a case in which a customer has concluded an independent contract with the hosting partner of his supplier to prevent suspension of performance in case of late or non-payment by the supplier. Depending on the relevant jurisdiction, different legal techniques could be used to create the "safety net" approach set out above, including – next to straightforward bilateral contracts – conditional contracts (kicking in only in specific cases) and conditional third-party beneficiary clauses inserted in the contract between the supplier and the subcontractor, etc.

Obviously, the application of such instrument requires a proper understanding of its scope and application as it might otherwise lead to an ongoing interference by the customer of the supplier's subcontractor management. The latter also not being in the interest of the customer. Clearly, suppliers will not always be comfortable with such approach as this could interfere with their way of managing the relationship with the subcontractor and it could weaken their position toward the customer, e.g. due to the improved information position of the customer.

13.3.5 Multi-party contracting solutions

Bilateral contracts also fall short in adequately supporting multi-party cooperations[11] for other reasons, including:

- A lack of provisions for joining or exiting a contract by a third party, thereby creating legal uncertainty;
- Change provisions are often inadequate to support flexibility in differentiation in roles and responsibilities between the various contracting parties;
- When using a set of individual, bilateral contracts to support multi-party cooperation, the number of contracts rapidly grows with the number of parties. Covering a cooperation between each and every of N parties requires $N \times ((N-1)/2)$ individual bilateral contracts. So for example, cooperation of 9 parties requires 36 individual bilateral contracts. This creates complexity and a significant administrative burden.

The use of multi-party contracts (hence contracts with more than two signatories[12]) can provide a solution to these and other issues. Most importantly, it can (1) provide a basis for ensuring compliance with a common set of obligations forming the basis of each and very interaction between the contracting parties but also (2) cater for distinct arrangements between a subset of the parties. As this is all encompassed in one single instrument, it can also – provided that it is adequately drafted and managed – support the entry or exit of parties and efficiently support flexibility across all arrangements. When this approach is successfully deployed, changes in the ecosystem do not require a burdensome amendment of all affected bilateral contracts.

While this is a major upside of this instrument, there are obviously also some concerns. The extent to which multi-party contracts are being addressed explicitly in contract law varies across jurisdictions. In the Netherlands, an example of a civil law jurisdiction (as most other European countries), the Civil Code enables creating multi-party contracts but does not provide detailed arrangements and to a large extent the relevant statutory provisions are not mandatory. This implies that the parties have on the one hand a significant liberty to create multi-party contract structures but on the other hand it also leaves uncertainty as to critical issues like the interpretation of the contract, suspension of obligations or dissolution of the contract. This challenge can be managed in the drafting process but requires additional skills. Some level of uncertainty will however remain since, as multi-party contracts are an exception rather than the rule, case law and jurisprudence regarding this type contracts are hence generally less developed than for traditional, bilateral contracts. On forehand this can however not be labeled as a blocking issue for exploring this approach.[13]

13.3.6 Legal entity-based approaches

More explorative might be the application of a legal entity (often referred to as a "joint venture"[14]) as a vehicle for creating rights and obligations across a spectrum of parties.

Let us explain by using the example of a sport association. In most cases, the association will be a legal entity with which individuals can enter into a membership relation. By the mere accession to the association (membership contract), the individual members are bound to all regulations declared applicable by the association. Also this could, next to the vertical relationship between the association and the individual member, result in horizontal relationships (rights and obligations) between the members mutually.[15] Now, outsourcing

is a fascinating topic but not a sport with (in principle) equal participants. How could this approach nevertheless be relevant?

First of all, the use of e.g. an association could be a relatively easy way to impose the previously described "general requirements" to each and every party involved in the outsourcing, including ensuring mutual obligations. This has as an upside that the involvement of the (main) customer and supplier is not conditional for ensuring compliance with these requirements. This can strengthen the (quality of) mutual cooperation between the subcontractors involved. Second, the diversity of the parties involved can be catered for by creating various types (categories) of membership, catering for the individual or bilateral needs of subsets of the ecosystem. It should also be noted that flexibility, in terms of accession/exit of parties or changes in general or party-specific arrangements, can in principle be accommodated efficiently in this structure.

Notwithstanding these advantages, there are obviously also some challenges that would need further exploration. These include issues like the exact consequences of default of key members, the design of a detailed governance structure, potential tax issues and maybe even competition law issues. The choice for a specific type of legal entity will have to be considered carefully taking into account local characteristics of the solutions at hand and the extent to which they can effectively serve the parties interest in creating a suitable legal framework for facilitating a successful outsourcing. Despite these challenges, there seems to be an adequate amount of upside justifying the further exploration of this option in specific cases.

13.4 Compliance pressure: the impact on contracts

13.4.1 Digitization as driver for upward compliance force

The digitization of our society has impacted the governance pressure on outsourcing suppliers along two lines: the digitization of their internal processes as well as the digitization of their customer's business. This has resulted in a string of new compliance obligations. The sources for these obligations are manifold. Independent of their business focus, organizations have been confronted with new obligations concerning data security, data protection and electronic communication in general. Additionally, sector-specific rules have become applicable depending on the sector in which they operate. Important examples include finance, retail and healthcare.[16] The increased volume of applicable rules also resulted in more supervisory focus, especially in the fields of cyber security, data protection, finance and consumer protection. Additionally, the stakes have gone up as this new legislation in some cases also came with increased supervisory capacity and more stringent sanctions (like in case of the European GDPR; see below) and, sometimes even more important, a sharply risen risk of reputational damage. Obviously, this process is still ongoing with new rules for e.g. platforms, artificial intelligence and blockchain currently being debated in circles of policy makers and supervisory authorities.

Achieving compliance in this setting is no longer something an organization can do on its own or in cooperation with single supplier. As a consequence of the shift from basic bilateral relations to coupled ecosystems (as we discussed earlier in this chapter), compliance has become a "team effort" and requires intense cooperation within the technology and business ecosystem(s) in which an organization operates.

This has become even more complex due to the time-sensitive nature of various notification duties (relating to data breaches) that have been introduced, the stringent sanctions on non-compliance and the fact that – especially in the field of data protection – independent statutory obligations have been imposed on outsourcing suppliers (next to the obligations of their customers).

In view of the interests at stake, ensuring compliance requires a solid legal basis in terms of adequate contracts. More specifically, it requires in particular contractual provisions (1) setting out adequately the duty to cooperate in achieving compliance, (2) proper auditing clauses, (3) proper sanctions to ensure effectiveness of these arrangements and (4) ensuring passing on of the relevant clauses to third parties (subcontractors). Given the interests at stake (stringent sanctions, customer claims and reputational damage) especially outsourcing customers should carefully consider whether reliance on – merely – their outsourcing partner, instead of securing a direct contractual relationship with the supplier's key subcontractors, is in the given circumstances an acceptable risk. As discussed above, we see compliance pressure, in addition to continuity-related arguments, as an important driver for deciding to enter into "safety net" contracts complementing the main outsourcing contract with the supplier.

In the next paragraph, we will illustrate the above by focusing on the developments in the field of data protection regulation and in particular on the impact of the recent European GDPR. Due to its broad geographical scope, the GDPR not only impacts outsourcing relationships in Europe but is potentially relevant for customers and suppliers around the globe.

13.4.2 Case study data protection. The impact of the GDPR

13.4.2.1 Background and scope

As of 25 May 2018, the GDPR (Regulation 2016/679) constitutes the center piece of the European approach to data protection.[17] The GDPR replaces the EU Directive 95/46 (the "Data Protection Directive").[18] By its nature, the GDPR – being an EU Regulation – equally applies in all EU Member States. The GDPR also applies in a number of countries outside the EU (Norway, Iceland and Lichtenstein), together with the EU constituting the European Economic Area (EEA).

Although the introduction of the GDPR was partially driven by the desire to create a level playing field throughout the EU, national legislation remains of importance. This on the one hand since the GDPR leaves some room for national interpretations regarding some topics but also since the full EU data protection package includes a number of directives requiring national implementation. The latter includes EU Directive 2016/680 (Law Enforcement Directive)[19] effective as of 6 May 2018 and the e-Privacy Directive (2002/58/EC)[20] which in the near future[21] will be replaced by the EU e-Privacy Regulation.[22] The latter instrument will particularize and complement (as a "lex specialis") the general rules on the protection of personal data laid down in the GDPR for electronic communications data qualifying as personal data.

From an outsourcing point of view, it is particularly important to note that the GDPR seeks to extend the reach of EU data protection law compared to Directive 95/46/EC. In many cases, the GDPR will be relevant, and likely even directly applicable, for outsourcing partners from outside the EU when entering into contracts with customers having a business focus on Europe. The establishment of the customer or outsourcing supplier in the EEA or processing of data in the EEA is not mandatory per se for the applicability of the GDPR. The territorial scope of the GDPR extends even beyond the EEA as the Regulation applies:

1 to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not (art. 3 par. 1 GDPR);

2 to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to offering goods or services to such data subjects in the Union or the monitoring of their behavior within the Union (art. 3 par. 2 GDPR).

Materially, the scope of the GDPR extends to almost all forms of processing of data since the definition of "personal data" is very broad. Under Article 4 (1) GDPR "personal data" include any information relating to an identified or identifiable natural person ("data subject") being a person who

> "can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

13.4.2.2 GDPR principles, roles and responsibilities for data processors

The GDPR is based on a number of principles/rights, mainly:[23]

- fair, lawful and transparent processing (processed lawfully, fairly and in a transparent manner in relation to the data subject);
- purpose specification and purpose limitation (collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes);
- data minimization/proportionality (adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed);
- data quality (accurate and, where necessary, kept up to date);
- storage limitation (kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed);
- data integrity and confidentiality (processed in a manner that ensures appropriate security of the personal data).

Furthermore, the principles of lawful processing,[24] data portability[25] and "data protection by design and default" are important elements in the GDPR. The "by design" principle refers to the obligation of the controller to, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures (such as pseudonymization) that are designed to effectively implement data-protection principles and to integrate the necessary safeguards for meeting the requirements of the regulation.[26] Data protection "by default" encompasses the obligation of the controller to implement appropriate technical and organizational measures to ensure, by default, only personal data which are necessary for each specific purpose of the processing are processed (in terms of amount of the personal data collected, the extent of their processing, the period of their storage and their accessibility).[27]

The very broad scope of the GDPR in terms of both types of data covered and geographically is particularly relevant for outsourcing providers as they generally qualify as "processors" under the GDPR. The qualification "processors" refers to an entity which processes personal data on behalf of the "controller" – the latter being the entity responsible for determining the purposes and means of the processing of personal data.[28] In the context of outsourcing involving processing of personal data, basically the customer will qualify as

"controller" and the supplier as "processor." When the supplier also processes (parts of) the data for its own purposes, like some Cloud providers do, they will also qualify as "controller" for the relevant data processing activities.[29] On the side of the supplier, other parties involved (subcontractors) could qualify as "sub-processors."

The extension of the applicability of the data protection framework to processors constitutes a novelty in the EU approach to data protection and creates a basis for independent obligations pertaining to processors.

Art. 28 GDPR further clarifies the obligations of the processor and its relation to the controller and other parties involved. Without prejudice to the independent obligations of the processor, the controller is obliged to engage only processors providing "sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."

For outsourcing suppliers, it is important to realize that the GDPR does introduce some direct responsibilities for processors and non-compliance might result in severe fines or other sanctions.

Under the GDPR penalties can even amount to 4% of the total global annual turnover or €20 million (whichever is higher).[30] The UK Data protection Supervisory authority (ICO) has summarized the direct responsibilities obligations for data processors under the GDPR as follows:

- not to use a sub-processor without the prior written authorization of the data controller;
- to co-operate with supervisory authorities (such as the ICO);
- to ensure the security of its processing;
- to keep records of processing activities; or to notify any personal data breaches to the data controller;
- to employ a data protection officer;
- to appoint (in writing) a representative within the European Union if needed.[31]

13.4.2.3 Contractual aspects

Processing of personal data shall only take place by a processor on the basis of a contract[32] that is binding and sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.[33]

The mandatory elements of such contract include:[34]

- processing of personal data only on documented instructions from the controller;
- confidentiality obligations for staff authorized to process the personal data;
- the obligation to take all measures required to ensure the security of processing according to art. 32 GDPR;
- providing assistance to the controller for fulfilling his obligation to respond to requests for exercising the data subject's rights including providing information, access to information, erasure ("right to be forgotten" and correction) and the controller's obligations in case of data breach (including notification to the supervisory authority and communication of a personal data breach to the data subject);
- assisting the controller in performing data protection impact assessments;
- the obligation to cooperate with audits and inspections conducted by the controller or mandated auditors.

In practice, the data processing contract is often drafted in the form of a separate contract that is added as an annex to the main outsourcing contract. The upside of such approach is that the negotiations regarding the data processing contract can be entrusted to a dedicated data protection working group with experts from both sides. The potential downside of such approach is however that the terminology and content of the data processing contract significantly deviates from the approach taken in drafting the main outsourcing contract by the commercial/legal working group. In the latter case, this can in principle be balanced by priority and interpretation clauses in the main outsourcing contract.

Subcontracting by the processor (hence engaging sub-processors) is only allowed on the basis of prior specific or general written authorization of the controller.[35] Engaging sub-processors does not relieve the processor of its obligations toward the controller.[36]

Under the GDPR, the establishment of data protection certification mechanisms (as well as data protection seals and marks) is encouraged for the purpose of demonstrating compliance by controllers and processors (art. 42 GDPR).[37] Currently, there are already a significant number of potentially relevant schemes on the market. These schemes however differ in terms of sources (legislation, standards or combined), scope (geographical, sectoral, process), single issue (e.g. privacy by design or data security[38]) or comprehensiveness (all GDPR provisions covered). Additional complications include:

- A variety of different controls. Schemes operated by public authorities/privately owned schemes and schemes accredited/monitored by public authorities vs. national accreditation bodies, DPAs;
- Uncertainty as to the legal effect of certification. Certification does not reduce the responsibility of the controller or the processor (art. 42(3)). Under art. 83 (Fines), when a fine is being issued, "due regard shall be given to the (…) adherence to (…) approved certification mechanisms pursuant to Article 42";[39]
- No clarity as to the mutual recognition of certificates between Member States (a certificate has – so far – in principle only validity in one Member State) unless it concerns a certificate issued by the EDPB.[40] This implies that the controller might, worst case will, have to obtain a range of certificates in order to cover its activities across Europe.
- Uncertainty regarding the way effective certifications can be realized in relations to non-EU-based controllers or processors.[41]

It is not unlikely that customers will put pressure on their outsourcing suppliers to obtain the relevant certificates.[42] In the near future, next to GDPR-related certifications, additional certificates might be required under the European Cybersecurity Act[43] providing for product and process-related cyber-security certifications. Although the bringing about of the Regulation was in part driven by the aim of countering the rise of local certifications (and hence barriers to trade), the current framework still contains a serious risk of substantial complications for especially cross-sectoral operating providers.

13.5 Concluding remarks

Digitization is heavily impacting the way organizations operate, innovate and connect to customers and partners. Outsourcing supporting these processes can only be successful if adapted accordingly. This not only requires innovative ways of operating and connecting

with customers but also requires adaptation to the changing landscape of the tech industry in terms of ongoing specialization, entrants and technological focus (Cloud computing, big data, cyber security, block chain, artificial intelligence, etc.).

From a contracting point of view, the increasing demand for flexibility and speed requires a strong focus on process rather than on merely fixed KPIs. However, also the contractual architecture underlying the outsourcing process needs to be adapted, calling for moving away from only deploying traditional bilateral contracts.

Bringing responsibilities close to the relevant partners can significantly enhance the customer's ability to monitor, guide and control their key delivery partners. The growing compliance pressure facing many customers of the outsourcing industry is, next to the drive for innovation, a strong second argument for substantiating such approach. Effectively realizing such approach requires the ability to consider alternative contracting structures as well.

Notes

1. In relation to outsourcing in practice both the terms "agreement" and "contract" are being used to reflect the document in which the main legal understanding between the parties is laid down. Although we consider both terms equivalent in this context, we will for the sake of clarity refer to "contract" or "contracts" unless the use of the phrase "agreement" is more common in the market, like in "service level agreement."
2. See e.g. Pon Template Sourcing Agreement v1.0, Clause 12.1 available through an internet search at: PON+outsourcing+agreement+template. For (other) notification duties, see for instance as well the recent Model Services Contract of the UK Government (see: https://www.gov.uk/government/publications/model-services-contract).
3. Art. 4.4. General Government Terms and Conditions for IT Contracts 2018 (Arbit 2018) as adopted by order of the Dutch Prime Minister, Minister of General Affairs, of 3 May 2018, no. 3219106 available at: https://www.pianoo.nl/nl/regelgeving/voorwaarden/rijksoverheid/algemene-rijksvoorwaarden-bij-it-overeenkomsten-2018-arbit-0.
4. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cyber-security certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (text with EEA relevance) PE/86/2018/REV/1 OJ L 151, 7.6.2019, p. 15–69.
5. Vandenberghe, G., *Partijenaansprakelijkheid bij softwareovereenkomsten. Een rechtsvergelijkend onderzoek*. Reeks Informatica en Recht Deel 2, Antwerpen/Deventer: Kluwer 1984 and De Lamberterie, I., *Les Contrats en informatique*, Litec, Paris, 1983.
6. Historically, there has been no established general concept of good faith in English law. In specific cases, like partnership agreements, the principle may however be considered relevant be it (considerably) less than in the European approach. In recent years, the English courts however seem more willing to consider express contractual good faith provisions to be enforceable. See: Sinanan, Andre, Good Faith in English Contract Law: A 'Contagious Disease of Alien Origin' (December 2, 2014). Available at SSRN: https://ssrn.com/abstract=2654752.
7. The level of enforceability may vary across jurisdictions.
8. In most cases OLAs are only used within the organization of the supplier to facilitate cooperation between the various internal departments involved in service delivery to the customer.
9. A similar reasoning could be developed for partners operating on the customer side of the ecosystem but this seems in general less relevant in practice.
10. Technically speaking, this could be solved by making a subcontractor a party to the customer-supplier contract. This "cure" might however be worse than the "disease" since – without major changes – such contract would not basically solve the issue of cooperation between subcontractors but does give rise to a wide range of issues (including governance, termination, liability, etc.) in the relation between (all) parties involved.
11. Stuurman, C., Wijnands, H. S. A., & Drion, C. E. (1998). *Electronic Commerce. Een privaatrechtelijk kader voor multilaterale EDI.* (ITeR; No. 12). Deventer: Kluwer, p. 10–11.
12. Or other forms of adherence, like acceptance of third-party clauses.

13. The way multilateral treaties and connected institutions function (like in the field of international trade) could also provide inspiration for further exploring multi-party approaches.
14. Although a joint venture could be purely contractual as well.
15. For instance by inserting third-party clauses in the membership contract.
16. See for an overview of the European legal framework for electronic communication in general: Lodder, A. R., & Murray, A. D. (Eds.) (2017). *EU Regulation of E-Commerce A Commentary*. Cheltenham Glos: Edward Elgar Publishing.
17. For electronic communications, additional rules will be set out in the forthcoming ePrivcay Regulation (proposal for a regulation of the European parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final – 2017/03 (COD)). This Regulation will (probably) take effect in the course of 2019.
18. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 31–50.
19. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4/5/2016, pp. 89–131.
20. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31/7/2002, pp. 37–47.
21. Probably in late 2020.
22. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final – 2017/03 (COD).
23. Art. 5 GDPR.
24. Art. 6 GDPR.
25. The right to receive the personal data in a structured, commonly used and machine-readable format with the right to transmit those data to another controller without hindrance (art. 20 GDPR).
26. Art. 25 par. 1 GDPR.
27. Art. 25 par. 2 GDPR.
28. Art. 4 GDPR.
29. See as well art. 28 par. 10 GDPR: "(…), if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing."
30. Art. 83 par. 6 GDPR.
31. ICO GDPR guidance: contracts and liabilities between controllers and processors, v 1.0 draft for consultation, 2017, p. 21.
32. Or other legal act (e.g. a permit or (other) government decision) under Union or Member State law that is binding on the processor (Art. 28 par. 3 GDPR).
33. Art. 28 par. 3 GDPR.
34. Art. 28 par. 3 GDPR.
35. Art. 28 par. 2 GDPR.
36. Art. 28 par. 4 GDPR.
37. See also Consideration 81 ("The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller.").
38. For instance covering (only) ISO/IEC 27001.
39. It should be noted that this not necessarily implies that a fine will be mitigated when a certificate has been obtained. The fact that, even where a certificate was obtained, the GDPR was violated might also be considered an aggravating circumstance. See Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (3 October 2017), p. 16: "Non-compliance with self-regulatory measures could also reveal the controller's/processor's negligence or intentional behavior of non-compliance."

40. Art. 42 par. 5 GDPR.
41. Art. 42 par. 2 GDPR provides the framework for these certifications. Implementing this provision gives rise to various questions regarding the organization and substance of these certifications (pending research of the Tilburg Institute for Law, Technology and Society, see: https://www.tilburguniversity.edu/research/institutes-and-research-groups/tilt/research/current-major-research-projects).
42. The recently introduced ISO 27701 standard (see: https://www.iso.org/standard/71670.html) could be an effective instrument in the process of achieving compliance and readiness for GDPR certification in this context.
43. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15–69.