First Lawyers

MYOBI B.V.
For the attention of Mr. A.J. Biesheuvel
Frankenslag 137
2582 HH Den Haag

Date: 31 March 2016

mr. dr. A.W. Duthler
T. 070 306 00 33
F. 070 392 22 76
E. a.w.duthler@firstlawyers.nl

Translated from Dutch:
Legal Information Regarding Robust Data Processing Agreements

Dear Mr. Biesheuvel,

MYOBI B.V. (MYOBI) develops Robust Data Processing Agreements that address the needs of its clients who act as ‘data controllers’ and ‘data processors’ in complex data processing chains. Robust Data Processing Agreements provide the means to ensure the risks and costs associated with the processing of data as it moves through a chain are correctly managed and mitigated.

Achieving these benefits requires all parties in the chain to sign up to a Robust Data Processing Agreement. Should, for whatever reason, any party in a chain be unwilling to sign a Robust Processing Agreement and thereby be disqualified from using the services of a Trusted Third Party (TTP) such as MYOBI, it effects the ability of all other parties in the chain to control potentially costly liability risk exposures, complicates the distribution of risk and has negative implications for the risk profile.

With regards to parties who are reluctant to sign a Robust Data Protection Agreement, as requested, I have provided in the attached document further details about the risks and consequences of not concluding a Robust Data Processing Agreement. In addition, I have also provided some guidance on how best to raise awareness of these risks among your clients.

It is perhaps helpful to note here that as your clients have a legal obligation to provide information, including about risks, they are duty bound to inform their customers, suppliers and partners of the risks they expose themselves to by not signing a Robust Data Processing Agreement. In their turn, their clients, suppliers and partners are bound to pass this information on to their relations. In providing this information, an ideal opportunity arises for your clients to detail why they chose a Robust Data Protection Agreement to limit or exclude liability towards their customers, suppliers and partners.

In the attached document, I describe the various benefits and limitations of the different data processing agreements MYOBI develop. In addition to the Robust Data Processing Agreement, these are:

- The Data Processing Agreement with Privacy Seal certification and maturity level assessment based either on a consultative process involving executive officers or on self-assessment
- The Standard Data Processing Agreement without Privacy Seal certification.

The information provided has been formulated in such a way as to make it suitable for general distribution. I would like to recommend you share this information among your clients to raise awareness of the advantages of using a Robust Data Processing Agreement and to highlight the importance of their decision and the subsequent consequences for their clients, suppliers and partners.

The attached document is intended to replace the document dated 26 October 2015 that was forwarded to you in your position as director of Duthler Associates .

I hope the information will be helpful to you. Should you have any questions, please do not hesitate to contact me. I would be more than happy to provide further details in person.

Yours sincerely,

Mr. dr. A.W. Duthler
Sollicitor

First Lawyers

Legal Information Regarding Robust Data Processing Agreements

Summary of capabilities and limitations

First Lawyers
The Hague, March 2016

First Lawyers

Table of contents

Introduction

1. Traditional Data Processing agreements are standard form contracts where the terms and conditions are drafted by the data controller which the data processor either accepts or rejects. The Data Processing agreement referred to under article 14 of the *Wet Bescherming Persoonsgegevens* (Wbp; the Dutch Personal Data Processing Act) is also based on these classic one-to-one contractual arrangements. Given the difficulty in today's increasingly interconnected business environment in determining which organisation in a data processing chain or network is data controller, or which is data processer[1], the traditional approach is no longer adequate.
2. The newly passed Dutch General Data Breach Notification law and the EU General Data Processing Regulation (GDPR) necessitate a new type of data processing agreement. With its Robust Data Processing Agreement, MYOBI provides for this need.
   MYOBI also offers two alternatives to the Robust Data Processing Agreement, namely:
   - The Data Processing Agreement with Privacy Seal certification and Maturity Level assessment
   - The Standard Data Processing Agreement without Privacy Seal certification.

   The Data Processing Agreement with Privacy Seal certification and Maturity Level assessment is also available in two variations: one in which the assessment is based on a consultative process involving senior management and one which is self-assessment based.
   This document describes the capabilities and limitations of these agreements in further detail.

The Robust Data Processing Agreement

3. The Robust Data Processing Agreement constitutes a mechanism for ensuring all parties in a data processing chain or network offer the same level of data protection and for establishing a basis for cooperative working relationships. The fundamental idea of the Robust Data Processing Agreement is that data controllers must have a demonstrable ability to provide data subjects with control and transparency over how their data is processed and keep full records of their personal data processing activities in an inventory (privacy accounting system). Maintaining a privacy accounting system is also one of the conditions for demonstrating compliance with the data breach notification and transparency requirements vis-à-vis the data subject and for giving effect to the rights of the data subject.

4. Parties who are signature to a Robust Data Processing Agreement subscribe to the MYOBI *Trusted Third Party* (TTP). MYOBI requires all its member organisations to hold a Privacy Seal certificate, to have consulted with the FG register to familiarise themselves with the data processing control framework and to commit to the level of privacy protection prescribed by MYOBI and laid down for each chain or network in the TTP Policy.

[1] This is exactly why the legislator introduced the Dutch Data Breach Notification Act as an amendment to article 14 of the Dutch Data Protection Act.

5. MYOBI member organisations are each assigned an Organisational Dossier in the MYOBI privacy and security accounting system, the SBC Management system. This Dossier can be used to share access to disclosure documents with third parties[2] as indisputable evidence of actual data processing practices. Alongside the Robust Data Processing Agreement and the MYOBI Contractual Agreement, disclosure documents may include other pertinent contracts as well as documentation pertaining to the contract process. The MYOBI PSA system also supports the use of sticky policies to authorise access to the Organisational Dossier.

   The Organisational Dossier can also be used together with the organisation's own privacy accounting system to create verifiable records of subject access requests and to maintain a register of data breaches including timing of notifications ('without undue delay') and description of the breach resolution. Please note that this option is not a standard part of the Robust Data Processing Agreement.

6. Data protection levels are laid down for each chain or network in the MYOBI common Legal Framework. The Legal Framework as well as the Policy Framework Privacy[3] that underpins it are governed by TTP Associates. In the event of a security incident, MYOBI can also be requested to coordinate investigations into the cause of a privacy incident, to facilitate and coordinate the resolution of data breaches and to facilitate communications directly to other data controllers, processors and sub-processors in the chain or network and indirectly to the AP and data subjects. The communications are facilitated by TTP Associates while MYOBI provides for immutable records of the moment and content of communications.

7. The TTP policy affords MYOBI the right to intervene, to impose fines or to terminate membership should a party fail to comply with the arrangements or the privacy norms laid down in the Robust Data Processing Agreement, the MYOBI Contractual Agreement and the TTP policy itself. MYOBI also has the authority to play a mediating role in the event of disputes between partners in a chain or network.

Capabilities and limitations of a Robust Data Processing agreement

8. As described above, the Robust Data Processing Agreement provides a mechanism for securing mutual agreements on data processing levels, security levels, security controls and breach communication and response procedures. The result for MYOBI member organisations is a set of common criteria that effectively enables the identification and detection of security incidents and whether they have or are likely to have a serious adverse impact on the protection of

[2]If the other party offeree accepts the Robust Data Processing Agreement, they are assigned their own Dossiers in the PSA. If the other party offeree does not accept the Robust Data Processing Agreement, they remain as related party in the Dossier of the offeror.
[3]TTP Associates is the development and management organisation that is part of Duthler Associates. See also: www.ttp.associates

personal data. In the event a security incident should occur, the Robust Data Processing Agreement protects MYOBI subscribers from unnecessary forensic assessment and notification costs by shifting those costs to the party who instigated the investigation.

9. In addition to securing agreements on technical measures, the Robust Data Processing Agreement also secures agreements with regards to terminology (a common semantic language) and privacy norms (maintaining a personal data processing inventory or privacy accounting, respecting the data subjects rights to information and giving effect to their rights to access, correction and deletion). MYOBI assumes responsibility for the oversight and control of all these agreements. In tandem with the Privacy Seal, the Robust Data Processing Agreement enables data controllers and data processors to demonstrate they comply with the fair and lawful data processing principle to the highest level, their processes are transparent and verifiable and that they have appointed and identified a Data Processing Officer. The advantage for data subjects is that they can easily ascertain what data has been collected about them and the level of protection afforded.

10. The Robust Data Processing Agreement enables member organisations to allocate risk liability equitably across all members in a chain or network. Because they are afforded visibility into each other's data protection compliance level and MYOBI has the authority to intervene to rectify any non-compliance[4], member organisations are able to control and limit their liability risk exposures.

11. The Robust Data Processing Agreement lays down concrete security standards with which every MYOBI member organisation is required to comply. In the event of an infringement of these standards, it will be assumed unless otherwise proven that there is a causal link between the infringer's act and the damage and the infringer will be held liable. This provision simplifies debate about proof and burden of proof.

12. The Robust Data Processing Agreement contains provisions for situations in which a financial penalty is imposed on a data controller by the AP (Dutch Data Protection Authorities) for failing to comply with the 'without undue delay' data breach notification ruling although responsibility for the infringement lies with another party in the chain or network and the data controller has the right to seek redress against this other party.

13. Because MYOBI member organisations demonstrate their commitment to a certain level of data protection through the Privacy Seal, they are clear towards their customers and partners about their personal data handling practices. This limits their liability risk exposure in the event a party attempt to hold them responsible for harm allegedly caused as a result of their actions or negligence.

[4] This can become apparent during the initial executive consultations or during the internal or external controls. As a last resort MYOBI can terminate the Agreement thereby ending MYOBI membership.

14. A subscription to MYOBI includes access to the expert knowledge of Data Processing Officers (DPOs). DPOs can assist member organisations in meeting the obligations imposed by the Wbp (Dutch Data Processing Act). These obligations are set out in the Legal Framework together with all other applicable privacy laws. Together with the agreed internal and external controls, the availability of DPOs provide organisations further assurance of their regulatory compliance.

15. In the event of conflict with the Regulatory Authorities or other parties in the chain or network, MYOBI will intervene to prevent or de-escalate the situation. Without mediation, organisations may run up unnecessary lawyer, security specialist and IT auditor costs or be confronted with significant financial losses stemming from reputational damage as well as the costs for civil lawsuits as both sides attempt to seek redress.

16. The Robust Data Processing Agreement contains a dispute resolution provision that requires parties to agree to attempt to resolve disputes through a mediator. Because the cost of mediation is minimal compared to traditional court litigation presided over by a judge, this can result in significant cost savings.

Capabilities and limitations for Board Members and de facto Directors

17. MYOBI identifies and maintains electronic records of all an organisation's personal data processing activities in electronic dossiers in the SBC Management system. This feature is not only available for organisations but can also be used by private individuals[5]. Although, for the purposes of this document, use by a legal entity or organisation is assumed[6], it is worth noting that there are circumstances in which Board Members and de facto Directors may be held directly liable for fines, for example, if they are deemed an 'accomplice' by the AP or public prosecutors. In such an event, the ability to show due diligence by means of a MYOBI-facilitated Personal Dossier that demonstrates their accountability with evidence will reduce the risk they will be considered as co-perpetrator and make them evidentially robust should they be involved in an administrative enforcement process or criminal investigation.

18. A Personal Dossier may also be helpful for Directors, Supervisory Directors, de facto Directors and Policymakers involved in improper performance of duties, mismanagement or tort action lawsuits.

19. According to Article 2:9 of the Dutch Civil Code (BW) Directors and de facto Directors are responsible towards the legal person for a proper performance of their assigned tasks and are liable for the full consequences of an improper performance of duties unless not gravely to blame for, nor negligent in taking measures to avert the consequences of that improper

[5] The Dossier of the legal entity and other organisations is called the Organisations Dossier. The dossier for private individuals is called the Individuals Dossier.
[6] Since it is the legal person or another organisational form that concludes the Data Processing Agreement.

performance of duties. A MYOBI Personal Dossier can provide Directors and de facto Directors with relevant evidence should they want to make use of this exculpation clause.

20. Article 2:248 BW or 2:138 BW provides that a Director or a de facto Policymaker is jointly and severally liable if the Board of Directors has performed its duties clearly improperly and this is likely a major cause of the bankruptcy. If the Board of Directors has failed to meet its obligations under article 2:10 BW (or 2:394 BW), then it is presumed that this improper performance of duties is a major cause of the bankruptcy. This presumption is a substantive rule of law and as such cannot be rebutted or contradicted by evidence to the contrary. If the Board of Directors fails to comply with its obligations under article 2:10 BW this presumption is a rebuttable legal presumption. Article 2:10 BW concerns the bookkeeping obligations of the legal person and requires that accounting records are kept of all assets and liabilities and of everything regarding the activities of the legal person in accordance with the requirements arising from these activities, and to store the books, documents and other data storage media in such a way that at all times the rights and obligations of the legal person can be known. In conjunction with article 2:391 para. 5 BW this can also be interpreted as an obligation of the legal entity to keep records of its privacy practices and to meet its obligations under the Dutch Data Breach Notification Act. Article 2:391 para. 5 BW refers namely to additional requirements to be set by Order in Council regarding the content of the Annual Report. Briefly stated, these additional requirements refer to a governance code that imposes the obligation on Directors and Supervisory Directors to disclose their strategic, operational, financial, reporting and compliance risk exposures in their Annual Report and, if necessary, to issue an in control statement that in their opinion the internal risk management and control systems provide a reasonable assurance that the financial reporting does not contain any errors of material importance and that, with due regard to the aforementioned shortcomings, the risk management and control systems performed adequately.

21. The corporate governance code that underpins article 2.391 para. 5 BW has increasingly come to resemble a materiality law. The Dutch Supreme Court, for example, has defined that the code adds substance to two sections of the Dutch Civil Code. Article 2.8 BW requires the legal person and those who pursuant to law and the articles of incorporation are involved in its organization to behave with “reasonableness and fairness” towards each other. Article 2.9 BW states every managing board member has a duty to the organisation to perform their function properly[7].

22. To conclude, Article 6.162 BW read in conjunction with article 2:9 BW provide that a Director, a Supervisory Director or a de facto Policymaker may be apportioned liability if a tortious act is committed by fault and the damage can be attributed to him personally. A tortious act can be attributed to the person committing the tortious act if there is a causality between the tortious act and the damage incurred. A further definition of a tortious provided in article 2.9 BW.

[7] HR 13 July 2007, NJ 2007/434, m.nt.J.M.M. Maeijer (ABN AMRO).

Capabilities and limitations of a Data Processing Agreement with Privacy Seal and Access to Data Protection Officers

23. The Data Processing Agreement with Privacy Seal contains an arrangement for the allocation of liability risk and the apportionment of damages including the type of damages that are recoverable, how the level of compensation is calculated and how proof of damage is apportioned. Since the Agreement requires parties to implement applicable levels of data protection, to have knowledge of the application and interpretation of the Dutch Data Processing Act and to be open and transparent with each other regarding this information, liability risk can be allocated fairly equitably. This arrangement, however, only applies to the party with whom the Agreement has been concluded. As such, the Data Processing Agreement with Privacy Seal only provides provisions for liability risk limitation and control with respect to the actual signatories to the Agreement and not with respect to other parties as would be the case with a Robust Data Processing Agreement.

24. Furthermore, the Data Processing Agreement with Privacy Seal lays down hard and fast rules for data protection which all parties are required to observe. In the event of an infringement of these rules, it will be assumed unless otherwise proven that there is a causal link between the infringer's act and the damage and the infringer will be held liable. This arrangement simplifies debate about proof and burden of proof with respect to signatories to the agreement. This arrangement does not apply to other parties in the chain or network.

25. In the event a fine is imposed on a data controller for a violation that was caused by a party in a chain other than the processor with whom the data controller has a contractual agreement, it can be very difficult for the data controller to seek reparation from the party that caused the violation. Since no prior contractual relationship has been established between the data controller and the other party, the data controller cannot base a claim on breach of contract and must seek an alternative legal basis, such as tort law or fiduciary duty. However, it is more difficult to recover damages on these bases and litigation is often expensive and prolonged.

26. Because parties commit to a level of data protection and display a Privacy Seal to demonstrate their compliance with high data protection standards, they are clear and unambiguous about the level of data protection their customers can reasonably expect. This serves to limit liability exposure to customers, partners and other third parties who claim damages allegedly caused by an infringement of data processing regulations.

27. Although provisions can be included in the Data Processing Agreement with Privacy Seal to minimise the risks and liabilities associated with a data breach, such provisions only relate to the data processing agreement the data controller or data processor has concluded with their customers. Agreements that the customers of the data controller or data processor in their capacity as data controllers or data processors and, or sub-processors conclude with other processors or data controllers also fall outside the scope of these provisions.

The Data Processing Agreement with Privacy Seal applies thus only to the contractual arrangement between the parties who are actually signatories to the Agreement. In theory, third parties cannot derive any rights from this Agreement, nor can obligations be imposed on the basis of this Agreement. There are, therefore, few if any possibilities for limiting the costs incurred in resolving a data breach.

28. Moreover, the Data Processing Agreement with Privacy Seal does not contain provisions for the coordination of security incident forensic investigations. Coordination of forensic investigations into a security incident are essential but if conducted without full cooperation from all data controllers, data processors and sub-processors in the chain or network, the costs can become exorbitant. Parties will then want to seek ways to transfer liability for these costs to the party who is ultimately responsible for generating the risk.

29. Data controllers and data processors who opt for a Data Processing Agreement with Privacy Seal should also take into account the possibility that customers may vary in how they interpret their obligation to ensure processors actually deliver on their statutory compliance responsibilities. The question arises as how to guard against excessive costs as a result of differences in the governance mechanisms adopted by individual customers.

30. The Maturity Level of the Privacy Seal reveals whether an organisation keeps records of its Data Processing practices (privacy bookkeeping), whether it complies with its information obligations and whether it supports data subjects in effecting their rights – among others to access, rectification and to object. However, because members of the chain or network collaborating under a Data Processing Agreement with Privacy Seal have not identified or established Data Processing goals common to the whole chain or network, MYOBI is unable to intervene to rectify compliance deficiencies. For data controllers and processors, the benefits of a Privacy Seal is that it allows them to demonstrate unambiguously the level of Data Processing they offer and to show an independent Data Privacy Officer is available to provide oversight and control. For data subjects, a Privacy Seal means they are informed about how their data is being handled and are in control. In this way - depending on the Maturity Level reached - a Privacy Seal goes a long way towards achieving the Data Processing goal of transparency.

Capabilities and limitations of the Simple Data Processing Agreement

31. Should a data processor for whatever reason not wish to become party to a Robust Data Processing Agreement or a Data Processing Agreement with Privacy Seal and in consequence also not join MYOBI, a data controller has good grounds for imposing all liability on the processor[8]. Ultimately, the data controller has little or no guarantee the processor has suitable security arrangements in place to comply with the DDPA.

[8] This also applies the other way around and it is the data controller who doesn't wish to become party to a Robust Data Processing Agreement.

32. The Simple Data Processing Agreement does not include concrete security standards. Without this set of hard and fast data protection rules, should damages be incurred due to a contravention of data protection laws or regulations, hefty arguments can arise as to the cause of the damage, the causality between the cause and the damage and about the allocation of the burden of proof.

33. In the event of a data breach, it is difficult to mitigate the costs of forensic investigations and other costs related to breach resolution or legal costs should one or other party be held liable for damage resulting from the breach.

34. Without predetermined data protection levels and a Legal Framework in place, it is difficult to limit the costs related to ensuring compliance with the Data Processing Agreement and the Wbp. Moreover, these costs are incurred anew for each additional contract, and that is before any actual control activities have been carried out.

35. Since neither data controller nor processor are transparent about how they comply with privacy legislation or about the level of data protection they offer, data subjects and other parties have no reason to trust that the data controller or the processor will comply with data protection legislation.

In Conclusion

36. Basic starting point is that due regard for the interests of the customer is central to both data controllers and data processors. Of course. However, the interests of the customer are not absolute; they are restricted by the extent data controllers and processers are willing to accept responsibility for complying with the provisions of the Dutch Data Processing Act, the Dutch Data Breach Notification Act and the GDPR. But the fact is, adherence to these Acts and Regulations by data controllers and data processors is conditioned by the extent their customers are willing to adhere to them. Thus, when we look for how to ensure compliance with the laws mentioned above, we arrive at a baseline - controlling the risks of non-compliance. Those risks must be controlled extremely well.

37. The Robust Data Processing Agreement offers the fewest limitations and the most advantages, including a common Legal Framework, common data protection levels and a system for reporting and compiling information for Managing Directors, Supervisory Directors and de facto Directors. Every MYOBI member organisation is accountable for complying with the common level of protection, undertakes to perform internal and external controls and, in the event of security incidents or conflict, accepts MYOBI as mediation facilitation provider. In case of a claim or fine, the Robust Data Processing Agreement enables organisations and its Directors and de facto Directors to support their position with evidence.

38. Not all contracted parties will necessarily want to be signature to a Robust Data Processing Agreement and data controllers and processors cannot oblige them to become a member of MYOBI. In such cases, the preferred alternative is that the contracted party demonstrate they meet MYOBI's high data protection standards by undergoing Privacy Seal certification and availing themselves of the expertise available in the FG register. This would clarify the level of data protection offered and enable unnecessary liability risk exposure to be avoided. If the contracted party is still reluctant, then it would be justifiable to impose strict liability against the unwilling party would be justifiable. This is on the condition that the offeror (of the Robust Data Processing Agreement) is able to prove the other party was offered the agreement and provided with information and warnings about the pros and cons and the risks of not signing such an agreement. The offeror can provide access to this information by adding the contract process to the Organisational Dossier as well as potentially the Personal Dossier that was assigned to them when they first became members of MYOBI.

Overview

	Robust Data Processing Agreement	Other Data Processing Agreements
Liability risk exposure and damages	Risk liability equitably allocated	Other party is held fully liable.
	Via TTP policy financial penalties are recoverable from party at fault.	Difficult to recover fines; procedure can be costly.
Evidence-based position	Strong in both civil, criminal and administrative procedures.	Unclear. Probably limited.
Forensic investigation costs	Coordinated investigations into security incidents.	Investigations in incidents not coordinated and probably carried out by numerous parties.
	Limits cost of investigation	No cap on costs of investigations
Legal costs	TTP policy includes mediation. This is more cost-efficient and faster than traditional court litigation.	Costs can only be recovered through court litigation.
Oversight costs	Limits oversight costs	No cap on costs of investigations.
Clear level of data protection	Parties conform to MYOBI agreed level of protection. MYOBI can differentiate between levels of protection by means of the Privacy Seal.	Parties comply with laws and regulations. No possibility to differentiate between levels of protection.
	Privacy Seal demonstrates Level of Maturity. The chain is accountable in defining expectations.	
Compliance assurance	Knowledge of application, interpretation and compliance with privacy legislation is guaranteed.	Knowledge of application, interpretation and compliance with privacy legislation is not guaranteed.
	Agreed controls provides further assurance of privacy legislation compliance	Less assurance of privacy legislation.

Summary: Capabilities and limitations of the Robust Data Processing Agreement versus the Simple Data Processing Agreement.