Dealing with a Vendor which has its own data processing terms[1]

It may be that you receive requests from a new or existing Vendor to use their Data Processing Addendum or where, in new agreements, the contract with the Vendor is created and not on your Company's standard terms. Where this occurs and the Vendor has its *own* data processing agreement / addendum, you should use the checklist below which is designed to help you ensure that the contract has everything required under GDPR and RPM's Global Protection Policy. If there are elements missing you should liaise with the Vendor to explain the position with the view to getting the contract amended accordingly. In the event of a deadlock, you should contact you general counsel who will advise you on how to proceed.

Keep a record of the amended contract and/or Addendum
When the amended contract has been agreed, make sure that you:

- Remove all highlighting and square brackets
- Check the numbering of clauses and page numbers
- Check that references to clause numbers are accurate

CHECKLIST AGAINST VENDOR'S STANDARD DATA PROCESSING AGREEMENT

CHECKLIST AGAINST VENDOR'S STANDARD DATA PROCESSING CONTRACT		
Name of person completing checklist		
Vendor name		
RPM entity / entities party to contract		
The Agreement must contain		
	Notes	**In contract?** ✓
Details about the data processing and data processing instructions:		
The subject-matter of the processing	This is required by Article 28(3) of GDPR. This information may be set out in a schedule or in the main body of the agreement.	[✓]
The duration of the processing		[✓]
The nature and purpose of the processing		[✓]
The type of personal data involved		[✓]

[1] If the contract requires RPM's or your GC's review under their contract review policies, please ensure you comply with those policies after considering and implementing the procedures described herein.

The categories of data subjects involved		[✓]
The Vendor must only process the personal data on documented instructions from our company unless required to do so by EU or EU Member state law to which the Vendor is subject, in which case, the Vendor must inform our company of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.	This is required by Article 28(3)(a) of GDPR.	[✓]
Data security		
Any individual processing the personal data must be under a duty of confidentiality.	This is required by Article 28(3)(c). Both contractual and statutory obligations of confidentiality are acceptable.	[✓]
The Vendor must implement appropriate security measures to protect Customer personal data against unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure.	This is required by Article 28(3)(c) of GDPR. The GDPR suggests various security measures to be considered, including using pseudonymisation and encryption, and having processes in place to restore and recover data quickly in case of incident; although preferable, the agreement does not need to list out the Vendor's security measures.	[✓]
The Vendor must delete or return all personal data to us after they have finished providing their services, at our choice (and provide certificate of destruction). Any copies must also be deleted unless an EU or Member State law requires that the personal data is stored.	This is required by Article 28(3)(g) of GDPR. The agreement may cross refer to similar provisions in the services agreement and / or provide clarification regarding the process / timeframes of deletion / return of data. This is acceptable provided that the essence of the clause is not substantially changed. While the GDPR does not strictly require Vendors to provide certificates of destruction, enforcement action by data authorities indicates that these should be obtained as a matter of course. You should therefore insist on this provision, or at least something similar.	[✓]
The Vendor must make sure that all information necessary to demonstrate compliance with these obligations can be made available to the company, which includes contributing to audits and inspections.	This is required by Article 28(3)(h) of GDPR. This requirement is somewhat vague and at the moment it is not clear how far parties can limit it. Instead of agreement to physical audits / inspections, Vendors may insist that receipt of their own third party audit report is sufficient to meet this obligation (the rationale is usually because this obligation is perceived by large Vendors as impractical as it could result in thousands of	[✓]

	customers conducting onsite audits). Accepting third party audit reports may fall short of the requirements of Article 28(3)(h) and therefore before accepting this risk (and you will need to obtain the approval of RPM's or your company's legal department to do so), you should attempt to come to a compromise with the Vendor; for example limiting audits rights "to once per year and on occasions where the Customer reasonably suspects that the Vendor may have breached the provisions of this Addendum" as well as the usual provisions regarding notice, that the audit will be untaken during business hours only, confidentiality undertakings, allocation of costs for the audit, etc.	
Data subjects' rights / general compliance assistance		
The Vendor must assist the company in complying with Articles 32 to 36 of the GDPR and RPM's Data Protection Principles These cover: • **Data security** • **Data breach notification** • **Data protection impact assessments** • **Consulting RPM's or your legal department prior the processing if the data protection impact assessment indicates this is required** • **Enquiries / investigations**	Required by Articles 28(3)(e) and (f) of GDPR. It is acceptable if this clause is qualified along the lines of "to the extent possible and taking into account the information available to the Vendor" – this wording is specifically permitted under Article 28(3)(e)-(f) as permissible qualifications to a processor's obligation to assist. There should also be a specific clause in the agreement relating to the Vendor notifying the Company of data breach incidents. Ideally, this should be within 24 hours of the Vendor first becoming aware of the breach but may also be 'without undue delay'. In addition it is better to obtain agreement for notification of 'actual, alleged and potential' breaches, but accepting only 'actual' breaches would be permissible under GDPR.	[✓]
The Vendor must assist the company in responding to requests from the data subject.	Required by Article 28(3)(g) of the GDPR. Again, the GDPR recognises that the Vendor will not have access to all of the Company's information, and allows them to assist with the requests "insofar as this is possible".	[✓]
Subcontracting		
The Vendor must get written authorisation from the company to contract with any sub-processor, and	Required by Article 38(4) of the GDPR. Permission can be general or specific but if general, the Vendor must inform the company	[✓]

this must be obtained before the sub-processor contract is entered into	whenever there is a change in the sub-processor; this is to give the company the opportunity to object. The agreement should cover what happens in the case of an objection as this is not covered by the legislation: a right to terminate may be appropriate.	
Any sub-processor must be bound by the obligations that the Vendor is subject to. There must be a written contract with the same requirements, and the need for security measures is particularly emphasised. This may be difficult to implement in practice, particularly if using a standardised cloud service, for example.		[✓]
International data transfers		
Personal data cannot be transferred outside of the European Economic Area (EEA) unless certain safeguarding measures are in place.	Required by various articles of GDPR. If a transfer is contemplated, you will need to obtain the approval of your Data Protection Champion or your company's legal department and additional wording must be placed in the contract.	[✓]