DATA PROCESSING ADDENDUM GUIDANCE

When a service provider has its own data processing agreement/addendum ("DPA") or other language related to information that identifies or could lead to the identity or otherwise relates to specific individuals, including names and email addresses ("Personal Data"), you may use this document to help ensure it addresses relevant topics. The information may be set forth in a schedule or in the main body of the agreement. Please note that while the majority of these requirements originate from EU or UK law, it is important to remember that other jurisdictions may have similar requirements and thus the inclusion of these terms across the board when processing Personal Data is recommended.

Remember that all software agreements and new applications must be vetted and approved by IT and any agreement or project that includes the storage, transfer (or access to) or other processing of Personal Data must also be assessed pursuant to the RPM DPIA Policy.

Guidance for EU & UK Data Processing Language		
Topic	**Notes**	**In contract?**
Data Processing and Instructions		
The subject-matter of the processing. Identify the service being provided.	The details of the processing and the nature under which it is done must be identified within the agreement.	[✓]
The duration of the processing. The term under which the service will be provided.		[✓]
The nature and purpose of the processing. Explain what the provider is doing and why they are doing it. *For example*: collecting, sorting, saving, transferring, restricting and deleting data to allow end-users to schedule appointments online.		[✓]
The type of personal data involved. Describe what types of data will be involved, i.e., contact data, health data, financial data. *Sensitive data will require higher level of protection*.		[✓]
The categories of data subjects. Describe what people are involved, i.e., employees, consumers, distributors. *Consumer data generally poses a higher risk to the company.*		[✓]
Processing only upon instruction and not for their own benefit. The service provider must only process the personal data on documented instructions from the company and state they will not sell or utilize the data for their own or any other third party's benefit, including sharing the data for a benefit.	If the service provider is required to process the data for another purpose pursuant to local law, they must inform the Company before processing, unless otherwise prohibited on important grounds of public interest.	[✓]
Confidentiality and Data Security		
Contractual or Legal Duty. Any individual processing the personal data on our behalf, directly or indirectly, must be under a duty of confidentiality.	Both contractual and statutory obligations of confidentiality are acceptable.	[✓]
Appropriate Security Measures. The service provider must implement appropriate security measures to protect Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. The agreement needs to set out the specific measures taken to protect the data and they need to be in-line with securing the types of data involved.	There are 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. Under the new SCCs it is no longer sufficient to have a blanket statement about security.	[✓]
Deletion or Return of Personal Data. The service provider must delete or return all personal data to us after they have finished providing their services, at our choice (and provide certificate of destruction) unless they have a valid reason to retain such data (to comply with law or to protect their legal rights). Any copies must also be deleted unless an EU or Member State law requires that the personal data is stored.	The agreement may cross refer to similar provisions in the services agreement and/or provide clarification regarding the process, timeframes of deletion, and return of data.	[✓]

Audit Rights. The service provider 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.	Some common limitations often proposed by third parties are limiting audits rights "to once per year and on occasions where the Customer reasonably suspects that the service provider 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. These are generally acceptable.	[✓]
Breach Notification, Compliance Assistance & DSARs		
Assist in our Compliance Efforts. The service provider must assist the company in complying with all data protection and other laws including: • Providing data breach notifications immediately • Responding to DPIAs and data transfer impact questions • Assisting with regulator inquiries and investigations • Responding to data subject access requests ("DSARs"), including the right to be forgotten.	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 service provider". There should be a specific clause in the agreement with respect to notifying the Company of data breach incidents. Ideally, this should be within 24 hours of the service provider first becoming aware of the breach but may also be 'immediately', 'promptly' or '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.	[✓]
Sub-processing/Subcontracting		
Authorization for sub-processors. The service provider must get written authorisation from the company to contract with any sub-processor.	Ideally all sub-processors should be identified either in an attachment to the main agreement or via a link to the service providers list of approved processors. Permission can be general or specific but if general, the service provider must inform the company 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.	[✓]
Sub-processors must be bound by same terms. Any sub-processor must be bound by the same or substantially similar obligations that as the service provider.		[✓]
International Data Transfers		
Personal Data Transfers must be Assessed. EU Personal data cannot be transferred outside of the European Economic Area (EEA) unless certain transfer mechanisms are in place and appropriate safeguards are available and in place to protect the data from government interception. A transfer includes accessing the Personal Data from another country. Reminder that the UK is no longer part of the European Union.	If a transfer is contemplated, you will need to complete a data transfer impact assessment to determine if additional wording is needed in the contract (assessment is done as part of the DPIA process). Any agreements referencing the SCCs must be updated to include the June 4, 2021 versions (effective September 27, 2021).	[✓]
Red Flags & Deviations		
Liability & Damages. Fines and penalties from data breaches can be significant. Be cautious if a service provider seeks to limit liability or cap data breach, or other, damages arising from violations of the DPA.	While many agreements contain limited liability language data processors should commit to adherence to the DPA and be willing to cover the company in the event they breach the DPA.	
Electronic Communications Service Providers (ECSP). ECSPs are subject to federal surveillance laws which are an area of concern under data privacy and protection laws. SCCs may not be appropriate in these circumstances. A data transfer impact assessment should be documented to ensure appropriate safeguards are possible and in place prior to the transfer.	When dealing with an electronic communications service provider, determine if they have Binding Corporate Rules or some other transfer mechanism they are relying on. If not, consider whether transferring the data is necessary (review options to segregate and/or maintain EU data within the EU instead of transferring).	
Relationships. Different relationships are governed by different SCCs. Most often the relationship will be the company as controller and the service provider as processor. If the service provider is a controller either alone or jointly with the company different terms will apply. The same will be true if company is a processor.	In the event the service provider is controlling or directly analyzing the information without our specific instruction (controller to controller relationship- i.e. a law firm) the standard DPA language won't not apply.	