GDPR | **Doing Business in a Connected World**
The Impact of Cybersecurity, Data Privacy and Social Media

GDPR Checklist for Third Party Agreements

Unlike the EU Data Protection Directive ("Directive") (where only data controllers had direct compliance obligations), the EU General Data Protection Regulation ("GDPR") will impose both direct compliance obligations on data processors as well as specific contractual requirements for the data controller to include in its data processing agreement with the data processor (see, e.g., Article 28 of the GDPR).

The following is a list of some issues to consider when reviewing your third party vendor agreements for compliance with the GDPR. This list assumes that such agreements are already compliant with the Directive (e.g., already have security requirements in place), and that the vendor is acting as a data processor rather than as a joint controller. In addition, please note this list is not meant to be a complete list of all the issues you may need to consider.

DEFINITIONS

- ☐ Consider whether the definitions in your Agreement need to be updated to reflect the revised definitions in the GDPR (e.g., definition of "sensitive personal data").

DATA BREACH

- ☐ In the event of a data breach, the vendor should be required to notify you without undue delay after becoming aware of the breach.
- ☐ In the event of a data breach, the vendor should be required to cooperate with you to investigate and remediate the breach, cooperate with any supervisory authorities and law enforcement, and assist with any notifications as required.

DATA SECURITY

- ☐ Consider whether it is appropriate to require the use of specific technical measures, such as pseudonymisation or encryption.
- ☐ Consider requiring the vendor to implement data protection by design where applicable.

PROCESSING AND RECORD KEEPING

- ☐ The vendor's data processing should be set up so that it can help you respond to and fulfill data subject requests (e.g., with respect to their right to data portability, right of access, right to rectification, right to erasure ("right to be forgotten"), right to restriction of processing, right to object to processing, and right to not be subjected to automated profiling).
- ☐ The vendor should be required to make available to you all information necessary to demonstrate the vendor's compliance with its processing obligations.
- ☐ The vendor should be required to maintain a record in writing of all categories of processing activities carried out on your behalf and make such records available to you or a supervisory authority upon request.

COOPERATION
Consider requiring the vendor to cooperate: ☐ With any data protection impact assessments (DPIAs) that you conduct. ☐ With any audits or inspections that you or another auditor may need to perform (e.g., to verify the vendor's compliance). ☐ To assist you in complying with your obligations regarding data security. ☐ With any inquiries or notices received from or with any investigations or consultations with a supervisory authority, or with a supervisory authority in the performance of its tasks, upon request.
DATA PROTECTION OFFICER
☐ Consider whether the vendor is required to have a designated data protection officer.
PRIVACY SHIELD
☐ If you are Privacy Shield certified, evaluate the agreement to ensure it is compliant with the Privacy Shield onward transfer requirements.
FINES
☐ Consider whether to modify the indemnities, limits of liability and other similar clauses to address the new risks, including the substantially increased fines (e.g., in the event of a data breach).