

For more information contact
Jon Dartley, Esq., 917-837-2909
jon@perlmanandperlman.com
www.perlmanandperlman.com



GDPR THIRD PARTY VENDORS

KEY TERMS FOR EVERY TECHNOLOGY AGREEMENT

Increasingly organizations are relying on third-party vendors to provide a wide range of services and operational support. Typically, the “default”, vendor-provided contracts are extremely one sided in favor of the vendor. Failing to appropriately – and vigorously - negotiate these contracts – will leave organizations with little recourse or means of redress should something go awry. Additionally, for those organizations collecting personal data from individuals residing in the European Union, the recent adoption of the General Data Protection Regulation requires additional obligations regarding the terms of these vendor contracts. While it’s impossible to provide an exhaustive list of issues to be considered in negotiating these vendor contracts, below is a list of key points that should always be addressed.

PROVISIONS TO BE ADDRESSED IN ALL CONTRACTS

The following provisions are strongly suggested to be addressed in every technology-related contract.

Security Obligations

Given the increasing prevalence of 3rd-party vendor breaches, documenting specific physical, administrative and logical safeguards is critical.

Limitation of Liability Cap

Vendors routinely attempt to limit all claims for losses or damages that customers might incur. Failure to negotiate will prevent any meaningful recourse/compensation.

Exclusions to the Limitation of Liability Cap

Certain damages, because they pose a greater risk to your organization and its reputation, should be excluded from any limitations.

Transition Services

When vendor relationships do not workout, smooth and seamless transitions are critical. Provisions requiring the vendor to provide ongoing services and specific transition support is essential.

Representations and Warranties

Vendor contracts are notoriously vague on deliverables, functionality, performance, etc. A variety of representations regarding security, performance metrics, deliverables and timing are essential.

Breach Notification/Credit Monitoring

Breaches are expensive, and if your vendor experiences a breach your organization will be responsible for your customers' claims, absent a negotiated provision. Drafting provisions related to notice and compensation are key.

Auto Renewal

Auto-renew term provisions are rarely a benefit, and should be addressed.

Termination for Convenience

For most engagements, the ability to terminate, at any time, is recommended.

Cap on Future Fee Increases

When making a sizable investment in technology, it's important to have an understanding – and restrictions - as to future cost increases.

Applicable Law/Venue

Ensure that should your organization need to bring a legal action, that the location and applicable law is favorable.

CONTRACT PROVISIONS REQUIRED FOR GDPR COMPLIANCE

The following items must be addressed in every contract in every vendor agreement subject to GDPR.

Contract Adequately Specifies/Addresses:

- Subject matter and duration of processing
- Nature and purpose of processing
- Type of personal data and categories of data subjects

- Obligations to follow only documented instructions from your organization
- Appropriate duty of confidentiality obligations
- Implementation of appropriate technical and security safeguards to meet obligations of Article 32.

Impose the required “sub-processing” restrictions

- Obligate the assistance of complying with “data subject” requests (e.g., right to data portability, right to erasure, etc.)
- Assistance with its obligations of Articles 32 to 36 (i.e., security, notification of data breaches, DPIAs, consultation, etc.)
- Deletion or return of data at end of contract
- Obligations related to data audits and inspections

DISCLAIMER:

These materials were prepared for informational purposes only. The information contained herein is general in nature and may not have application to particular factual or legal circumstances. These materials do not constitute legal advice or opinions and should not be relied upon as such. Transmission of the information is not intended to create, and receipt does not constitute, an attorney-client relationship. Recipients of this information should not act upon any information in this article without seeking professional counsel.

Presented By: Jon Dartley, Esq., 917-837-2909
jon@perlmanandperlman.com or www.PerlmanandPerlman.com