IMPORTANT ISSUES TO CONSIDER WHEN NEGOTIATING SOFTWARE LICENSES AND AGREEMENTS

The primary goals of the Office of General Counsel ("OGC") and Procurement ("Procurement") in reviewing Software License Agreements (and cloud-based "software as a service" agreements) are to ensure that the agreement will allow NYU to use the software, and that the software will perform, to the full extent intended by NYU’s stakeholder. Although software companies typically start from their "standard boilerplate" license agreement, virtually every vendor routinely considers requests for amendments to those standard terms. It is rare that one version of a vendor’s software license is suitable for all applications.

OGC’s approach to negotiating the terms of these agreements is consistent with national standards developed by prominent organizations, including the National Association of College and University Attorneys and the Association of Corporate Counsel. OGC has developed and uses a checklist that facilitates the undertaking of due diligence by OGC, Procurement, and the department or unit involved with the goal of ensuring that the terms of the license will suit the needs of NYU and its stakeholder. Please note that insurance and indemnification provisions are reviewed separately by the NYU Insurance and Risk management Department ("Insurance"). To minimize delays, please have Insurance review those provisions simultaneously with the OGS and Procurement review.

The OGC checklist addresses business issues, liability issues, technical issues, and what OGC characterizes as “corporate” issues. It also addresses special issues related to cloud-based "software as a service" ("SaaS") agreements. As is apparent from the issues noted below, the review of software licenses requires a dialogue between OGC and/or Procurement and the department or unit in question. All of these issues can be assessed, and the license provisions reviewed, in an expeditious fashion. With that said, OGC appreciates that negotiations with a vendor can be time consuming where the vendor is slow to respond or where there is a great deal of back-and-forth with the vendor, but OGC and Procurement strive to move the negotiations as expediently as possible and ordinarily have a good degree of success in negotiating terms that can better ensure that the stakeholder’s goals are met and that the stakeholder and NYU are properly protected. To better enable stakeholders at NYU to undertake their negotiations with vendors, some of the more significant considerations are set forth below:
Business Issues

- Are the technical specifications/performance requirements stated for the software/service sufficient to allow NYU's stakeholders (or their IT/technical representatives) to ensure the adequacy of the software?

- Once NYU has purchased the software, what are the terms for "accepting" the software, and what opportunities does NYU have to ensure that it is functional? Is "testing" needed?

- To what extent does the unit/department in question require training or support at the time of acquisition, and does the agreement include this?

- Does NYU require any additional development or customization of the software, or other implementation services from the vendor?

- Does NYU need to acquire the right to modify the software for any specific purposes? This is often prohibited under the terms of the license and needs to be carefully considered.

- Are there provisions relating to NYU's use of later enhancements in the software?

- Are there issues at the time a software license is terminated regarding access to or importing data generated by the software? These can arise with any software, but does so more frequently when there is a SaaS component.

- Is the grant of rights included in the software license adequate to suit NYU's needs (e.g., worldwide coverage, including uses by portal campuses and study away sites, right to sublicense, right to create derivative works, length of time for the license, territory of the license, exclusivity issues, etc.)?

- Does the agreement contain restrictions on how NYU may use the software, and has this been reviewed with the NYU stakeholders?

- Does the agreement contain references to documents hosted on the vendor's website, such as a Service Level Agreement, Data Security Policy, Terms of Use, or Privacy Policy? If so, does the agreement contain any limitations on how the vendor may change them? Have these documents been reviewed?

- How are license fees calculated? If on a usage or user basis, how are those numbers calculated? Does NYU self-report, or is the vendor able to measure? If the vendor can measure, do they have access to NYU's systems in order to do so? Are there limits on users/locations/"seats" that impact the flexibility to perform research in an efficient manner?
**Liability Issues**

- What warranties has the vendor made regarding performance of the software? These may include anything from the integrity of the software code to the adequacy of the documentation.

- If the software malfunctions, or software as service malfunctions, has the vendor limited NYU's ability to seek an appropriate recovery? Are these "limitation of liability" terms acceptable to the department/unit? Who is bearing the financial responsibility for such limitations? In certain cases, software failure can literally be catastrophic -- sometimes to a research program, and sometimes to an entire unit or department or school. Liability can easily be in the millions of dollars. Is the language of the license sufficient to protect NYU and its stakeholders in the event of a failure?

- Are there any issues with regard to the software infringing the rights of third parties? If NYU is prevented from using the software because of infringement issues, does NYU have any remedies against the vendor? If not, is the financial risk fully understood by the department/unit? Is there a financial liability cap for such claims?

- Does the software license subject NYU to a lawsuit in an unfavorable venue, such as California?

- Will NYU be sharing information with the vendor that is protected by HIPAA, FERPA, GDPR, or another privacy statute? If so, are the requisite provisions in the agreement to protect that information?

- In general, are there financial caps for liability arising from claims under the agreement? If so, has a determination been made that the level of the cap is sufficient? Areas where there never should be a restrictive cap include claims based upon breach of confidentiality, claims based upon infringement, and claims for security/privacy breach, especially with SaaS-based contracts.

- What insurance does the vendor have and does it protect NYU?

**Technical Issues**

- What are the specific hardware requirements and can NYU meet them? Are there "interoperability" issues NYU or the vendor must address?

- Are there any unique security risks with regard to the data generated or processed with the software (such as HIPAA or FERPA), and does the vendor have any role in that regard? This becomes more important with so many "cloud-based" software licenses.

- What are NYU's expectations with regard to debugging, patches, and upgrades during the term of the license? Is NYU satisfied with levels of response time and "severity" of performance issues?
• Are there particular technical personnel from the vendor NYU expects to be involved with the project? Does NYU wish to have control over the vendor's right to appoint or replace personnel? Can NYU insist on receiving the “A-team?”

• Is there additional documentation NYU expects to receive from the vendor and is it adequately described in the document?

• Is there a need to have source code for the software placed in escrow for any reason, such as if the vendor stops supporting the software? Sometimes, this can be essential to ensuring the integrity of a research program or a valuable NYU database.

"Corporate" Issues

• What are NYU's rights in the event of a bankruptcy? In that event, are there issues that need to be addressed in terms of: i) maintaining access to the software and its source code; ii) maintaining access to stored data; or iii) the integrity of any research or program based on or utilizing that software? Will a software escrow provide adequate protection, or should there be other means for protection, including the right to monitor the financial and business stability of a privately-held vendor?

• Does the vendor subcontract any key services to third parties? What is the reliability of those entities? Is the vendor responsible for non-performance by a subcontractor?

• Does NYU have concerns about the impact if the vendor merges with another company, or is acquired by a competitor, etc.? These issues happen frequently, and can have a significant impact on the continuity of the product, and its competitiveness. Will NYU have the right to continue to obtain the same product, which includes the same functionalities, or will the merged entity have the ability to change the product specifications and/or pricing after the merger?

“Cloud” Based SaaS Software Contracts

• Are there adequately defined service level agreements ("SLAs") appended to the contract, or incorporated within the contract that define the level of service the vendor is agreeing to. If the vendor fails to meet the SLAs, what is the nature and extent of penalties on the vendor, including financial and/or a right to terminate. There also can be "reputational penalties," which may have more "teeth" than straight financial penalties. Are there issues with regard to the location of the servers that the vendor will be using to provide the SaaS service? Are the servers in restricted countries and what are the implications?
Does NYU have the right to back up its data on its own servers (as a security precaution) as often as it wishes? Does it have the tools necessary to do so, and will the data be in a file format that is useful to NYU?

Upon termination of a SaaS contract, does NYU have software tools and other access rights necessary to migrate necessary data to a new system? Has there been an analysis done of the cost to NYU for such migration as a part of the business analysis for entering this contract?

One of the key risks from SaaS agreements is from security breach claims, where access to critical third-party information (including credit card information, Social Security numbers, etc.) is breached. Does the vendor have specific insurance coverage for "cyber risk" types of liability? This is a unique type of coverage that is necessary to cover such claims. Because the average national security breach claim is in excess of $3 million, the level of insurance for such a vendor should be commensurate with the risk of liability. Some of NYU's key SaaS vendors have at least $10 million in cyber risk insurance.

What types of audit rights will NYU have? Will the vendor agree to the industry-standard types of audits for SaaS-based computing? As of 2018, this ordinarily includes the ISO 27001 audits, SAS 70/SSAE16 audits (and related SOC1 and SOC2 reports), and similar audits; however, the standards for such audits are constantly evolving, and language should reflect that. SaaS based contracts often have a longer term, and therefore it is important to ensure that there are appropriate price caps contained within the agreement. There should be a balance between the length of time NYU is able to lock in rates, and the ability of NYU to read to renegotiate other key terms of the agreement several years after signature.

There should be a chart identifying the various functionality of the software in question, and making sure that as the vendor product evolves over years, NYU continues to receive the original functionalities as a part of updated services, for no additional price.

As noted above, there usually are issues regarding mergers and acquisitions with SaaS-based agreements, and care should be taken to ensure that NYU is adequately protected in such an event.

Further Resources

If you have legal questions about software licenses and agreements, you can find a member of the Office of General Counsel who practices in this area by visiting our practice areas page and scrolling to “Computers, Internet and Web Legal Issues”.

Replaces version dated July 25, 2012