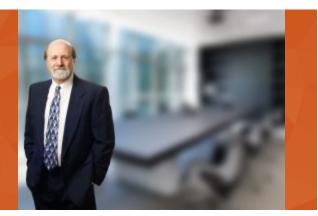# Reviewing Software License Agreements

A Licensee's Checklist

By: Howard G. Zaharoff
September 15, 2020

Often lawyers or contracts specialists are asked to give a "quick" review of an incoming software license agreement on behalf of a prospective licensee. The following is a checklist and short discussion of the main issues the reviewer should consider.

License: Scope

If this will be an on-premise installation, the license granted should be sufficiently broad to permit the licensee to *install* and *use* the software on any (one or more) computer systems, *copy* it as required (including to execute the program and for reasonable backup), and (if appropriate) *modify* it as needed. (Rights to copy and modify, if granted, should apply to the documentation, too). If the license specifies a CPU, it should be clear that the program can be run on any single back-up or replacement CPU.

If this will be a Software as a Service ("SaaS") or other internet-access license, the license or subscription agreement should permit the right level of use and access (whether it's defined by users, seats, field, etc.) and perhaps the right to download and copy documentation you will need.

If the licensee maintains a separate development/support system and/or a backup site, be sure appropriate rights of installation, reproduction, use, testing and/or adaptation are included. If the license specifies a location, it should be clear that the licensee may change the location (at least to anywhere within the United States and other predetermined locations) merely by notifying the licensor. (If they require notice to be given in advance, make sure that there is an exception for emergencies).

Deliverables

The agreement should be clear on *what* the licensor will furnish (e.g. for on-premise licenses, the licensor may be required to provide computer media containing the program in executable form or – more likely these days – a password-protected website for downloads, as well as user documentation of sufficient quality and completeness to enable a competent user to run the program). It should also be clear when these must be delivered or made available.

Source Code

If the system is very costly, or if modifications clearly will be required and the licensee wants the ability to perform them, source code must be furnished. If the licensor refuses, consider a source code escrow arrangement. Be sure it clearly defines how the source code may be used — don't assume the rights granted respecting the object code are sufficient.

Vendors of SaaS solutions are even less inclined to furnish source code than on-premise

licensors. For mission-critical SaaS applications, consider a backup resource such as Iron Mountain's SaaSProtect or, as noted above, a source code escrow agreement.

Services Furnished

If *training* is required, the licensor's obligation to provide it (when and where) must be stated. *Maintenance and support* (fixes, corrected versions, new upgrades/releases, telephone consultation, online support and/or programming services) are almost always needed. Thus, either the agreement should spell out the licensee's right to receive support, or a separate maintenance contract should be signed simultaneously, or the agreement should give the licensee the right to enter into a maintenance contract. See "Remedies" below. The availability of maintenance should be guaranteed for some minimum period, such as 3 or 5 years, with a fixed price, if possible — e.g. current prices increased no more than CPI or a fixed percentage (e.g., 3/5/7% per year).

Disclosure/Access

The licensee should have the right to disclose the software, or make it available, not only to its employees and agents, but also to independent contractors whom it retains, as well as advisors and perhaps directors, investors and acquirers (subject to confidentiality in each case). Sometimes, disclosure must be made to the licensee's accountants and, in the case of banks, its examiners and regulators. Ideally the licensee's confidentiality obligation would be limited to informing these individuals that the disclosure is confidential or, at most, requiring these individuals to observe confidentiality (without necessarily having to obtain signed agreements from all of them). If possible, avoid being expressly liable for breaches of confidentiality by third parties (particularly regulatory bodies and professionals) with whom you are permitted to share the information.

If you are required to obtain a written non-disclosure agreement from disclosees, review and approve the form in advance. (Computer professionals are often independent contractors rather than employees, and many companies must grant their auditors and the like, the opportunity to inspect their operations–in short, access by third parties may be essential, and third parties' reactions to non-disclosure obligations should be considered before agreeing in the license agreement that all third party disclosures are contingent on their accepting terms that they haven't vetted).

Make sure that certain standard exceptions from the nondisclosure obligations apply, the most common being information that: was previously known, is public (without fault), properly disclosed by third parties, independently developed, or required by law or judicial process. Consider both a time limit (e.g., 5 years) and, *provided you will not be disclosing critical data to the licensor*, a "residuals" clause (exempting from these nondisclosure obligations information learned by employees and retained unaided in memory).

If the licensor will learn or have access to confidential licensee information, the licensee must also agree to treat the information as confidential. If that information involves customer data, such as personal, financial or medical data, consider whether the licensor must agree to special rules, such as compliance with Gramm-Leach-Bliley, HIPAA or the GDPR; at a minimum, they should agree to comply with all applicable laws. (If they will have access to sensitive information, be cautious about a residuals clause that benefits the licensor).

New IP/Developments

If either party might develop new intellectual property (e.g., adapted code, new code, etc.) when customizing, installing or using the software, ownership and rights should be carefully considered. Most software licensors insist on owning modifications and add-ons to their software products, even if you pay for the development and sometimes even if *you perform* the development. At a minimum, seek the right to use freely what you pay for and/or restrict the

licensor's right to use this for third parties, particularly competitors (you'd hate to pay for the licensor to develop a tool that it can license more cheaply to your competition, particularly if its use yields a competitive advantage).

Be leery of "feedback" clauses providing that any ideas your employees share unsolicited with the vendor is freely usable by the licensor. Also, if the licensor may have access to your valuable trade secrets, beware of "residual" clauses providing that any confidential information your employees share with the licensor, which its employees retain in their unaided memory, is also freely usable (except perhaps as limited by patent or copyright laws).

Open Source

Developers increasingly use open source components in their products. A problem may arise if a licensee obtains rights to modify and sublicense portions of a program which includes open source code, particularly open source licensed under the GPL (or other similarly "viral" open source licenses). Licensors of open source who follow this model require licensees who distribute software containing such open source code to freely license the derivative product, even if it is comprised mainly of otherwise proprietary code (though there remains some debate about the enforceable breadth of such clauses). Therefore, before a licensee modifies or redistributes any licensed software, it must determine whether it contains open source code and understand what special terms may apply respecting distribution.

Acceptance/Warranties

Unless the licensee is able to determine in advance that the system works properly (for example, by discussing the matter with, and observing the operations of, other licensees), there should be an acceptance period and a right to a refund if the system is not accepted. Similarly, there should be warranties of functionality usually tied to a specific pre-disclosed specification, and a right to a refund if problems cannot be corrected during the warranty period (or beyond).

However, where the project includes substantial customization or other services, the licensor will be loath to agree to refund the service fee — negotiation may be needed. In addition, if the licensee might invest significant resources to implement the new system, the licensor should not be able to simply refund its fees and walk away from performance failures (this is discussed further in "Remedies" below).

Breaches

The licensor should not be able to terminate the license on account of the licensee's breach unless the licensee has notice and an opportunity to cure (often 30 days). For certain key applications, the licensee may deny the licensor a right to terminate (except perhaps under extreme circumstances, and then only after substantial advance notice and opportunity to cure).

Remedies

The issue of remedies must be carefully considered. Once a licensee installs a system, it may be very difficult or time consuming to exercise a right to revoke and receive a refund. (Even for an online service, the time spent investigating, negotiating, training for, migrating data to, and acquiring technology needed to implement a new system may make cancellation very damaging or impractical for the licensee/subscriber). Therefore, it is generally critical to obligate the licensor to use whatever efforts are necessary to correct problems.

In general, the licensor should be required to address problems promptly; but it is reasonable for response times to be commensurate with the severity of the problem. Thus, ideally the licensor would offer a "service level agreement" that requires the licensor to respond to, and commence efforts to remedy, a *system-down/debilitated problem* within a very short period (e.g., 1-2 hours); to remedy a *serious impediment* quickly (e.g., 4 hours); and *other material bugs and*

Morse

CityPoint, 480 Totten Pond Road, 4th Floor, Waltham, MA 02451 | 177 Huntington Ave., 17th Floor, Boston, MA 02115

defects reasonably and promptly (e.g., 8 hour response and 24-48 hour correction). If correction can't be completed within these time frames, the licensor should provide a "work around," i.e., a temporary fix that enables the licensee to continue using the software substantially as originally contemplated. The licensor should also be obliged to use its continuing best efforts to correct the problem fully thereafter (though it is fair for the licensor to correct truly minor issues with its next software release or cycle).

Consider also seeking a specific "cover" remedy: that is, if the licensed or subscription product can't be made to work properly, ideally the licensor would be obligated to pay the licensee's cost to obtain a comparable working system. However, expect an argument over this, particularly if comparable software doesn't exist or is extremely costly.

If the licensor seeks force majeure and consequential damage limitations (and often even if it doesn't), the licensee should demand similar protections. (However, if the licensor will have access to valuable confidential information, consider not waiving consequential damages for breaches of confidentiality, since significant consequential harm may be sustained when confidential or trade secret information is disclosed). If the licensor seeks a cap on damages (e.g., to the total paid, often limited to the last 3, 6, or 12 months), seek something similar *and* make exceptions for IP infringement claims, security breaches (if applicable), and damages attributable to gross negligence and willful misconduct.

Hardware: Integrating Responsibility

If hardware is included in the deal, make sure that the software and hardware warranties are coordinated and integrated with each other. If the hardware is dictated by the licensor but purchased directly from the hardware manufacturer, make sure that the licensor is obligated (at least secondarily) to correct problems or (at a minimum) to provide reasonable cooperation with the licensee, at no cost, to ensure that problems are remedied. (Beware of the finger-pointing problem and be sure that the licensee cannot get trapped between a software licensor claiming it's a hardware problem and the hardware vendor claiming it's a software problem).

Infringement

There should be a warranty against infringement and a workable remedy if infringement claims are made. Typically, this means that the licensor will notify the licensee of actual or anticipated claims made against it or its customers and agree to indemnify and defend the licensee against them. The licensee should have a right to participate in the defense at its own expense; it may also seek a right to assume control of the defense, perhaps also at its own expense unless the licensor has mishandled the defense.

In most cases, the licensor will have the right either to modify the program so that it becomes non-infringing, replace it with a non-infringing replacement (either of its own creation or furnished by a third party — thus the "cover" remedy noted above), or repossess materials and provide a refund. If such provisions are included, make sure that the modified or substituted software continues to satisfy the applicable specifications and that the refund is adequate (for example, it should not be a refund of only the amount paid for the particular software application or module involved if in fact this is an integrated system and the removal of any single component could render the whole useless or less valuable to the licensee).

Privacy

Though less likely with an on-premise license, when the software is made available as a subscription service the licensor often hosts or has access to personally identifiable information controlled by the customer. This may be information regarding its personnel, or information regarding its customers. Most US states have laws that require secure treatment of personal data, with California and Massachusetts leaders in this field. And if the personal data includes any identifiable regarding Europeans, all parties must consider and comply with the GDPR. At a

Morse
CityPoint, 480 Totten Pond Road, 4th Floor, Waltham, MA 02451 | 177 Huntington Ave., 17th Floor, Boston, MA 02115

4

minimum, the licensor should represent that it uses appropriate physical, technical and contractual measures to ensure security. *Be sure to get good legal counsel on these issues, because much (and many dollars) may be at stake!*

Transfer/Assignment

Ideally, the licensee would have the right to transfer the software in connection with its sale of the related hardware. At a minimum, it should have the right to assign the license (and maintenance contract) to any successor business.

Taxes

In some jurisdictions, the sale, license, or other transfer of a right to use software on a server hosted by a third-party (such as SaaS) is generally taxable; whereas other states view SaaS through the lens of a true service offering that may not be taxable. Further, many states tax product sales, including licenses, without taxing services; in such cases breaking out the services component of the fee may save the licensee local sales taxes. Generally, if sales and use taxes are due, they are the licensee's responsibility; however, given the complex patchwork of state sales and use tax laws, both licensors and licensees are urged to consider the myriad tax consequences that might arise when reviewing a proposed software license or subscription agreement.

For more information regarding software license issues, please contact **Howard G. Zaharoff**.