Indemnity clause in software license contract drafting and negotiation

**Introduction**: An Indemnity Clause in a software license contract is a provision that outlines the responsibilities of the parties involved in terms of protecting each other from certain claims, losses, or liabilities. This clause is especially important in software agreements due to the potential risks associated with data breaches, misuse of software, and non-compliance with data privacy laws.

Indemnity in a software license contract is a provision that addresses the legal responsibilities and liabilities of the parties involved, typically the software developer or vendor (licensor) and the software user or licensee. This provision defines who will be responsible for certain types of claims, losses, or damages that may arise in connection with the use of the software.

The indemnity is typically related to third-party claims, meaning it covers situations where a party outside of the software license agreement initiates legal action.

Let understand through simple example: Suppose a software company, ABC Software Inc., is licensing its accounting software to a small business, XYZ Services LLC. They enter into a software license agreement, and within this agreement, there is an indemnity clause.

Indemnity Clause:

ABC Software Inc. agrees to indemnify and hold harmless XYZ Services LLC from any third-party claims, losses, and damages arising out of any copyright or intellectual property infringement related to the software provided by XYZ Software Inc.

In this example, ABC Software Inc. is the indemnitor, which means they are taking on the responsibility to protect and compensate XYZ Services LLC in case of certain legal issues.

And XYZ Services LLC is the indemnitee, the party being protected by ABC Software Inc.

The indemnity clause specifies that the indemnitor (ABC Software Inc.) will provide protection to the indemnitee (XYZ Services LLC) against claims, losses, and damages resulting from copyright or intellectual property infringement related to the software. In simpler terms, if a third party, such as a copyright holder, sues XYZ Services LLC for using the software, ABC Software Inc. will take responsibility for defending ABC Services LLC and covering any financial losses.

Now suppose if third party software developer sues XYZ Services LLC for copyright infringement and data privacy breach (exposure of sensitive customer information) or due to a vulnerability in the software

In this scenario, ABC Software Inc. will step in to protect XYZ Services LLC's interests for copyright issue which is cover under indemnity clause.

This is case data privacy breach is not mention in indemnity clause. The responsibility for data breach and any associated liabilities would depend on the specific terms of the software license agreement and the wording of the indemnity clause. In this situation, the indemnity clause comes into play.

Drafting and negotiating the indemnity clause in a software license contract requires careful consideration of the interests of both the software vendor (licensor) and the software user (licensee).

Here are best practices for drafting and negotiating the indemnity clause

1. **Be Specific and Clear**: Clearly define the scope of the indemnity clause. Specify what types of claims or situations trigger the indemnity, and under what circumstances it applies.

Example: In a software license agreement for a customer relationship management (CRM) software, the indemnity clause may specify that the licensor (CRM Software, Inc.) will indemnify the licensee (XYZ Services LLC) against any third-party claims of patent infringement related to the software's core functionality.

1. Identify Responsible Parties: Clearly identify who is the indemnitor and who is the indemnitee. Be specific about their roles and responsibilities.

Example: The indemnity clause should state that CRM Software, Inc. is the indemnitor, responsible for covering legal costs, settlements, and damages, while XYZ Services LLC is the indemnitee, entitled to this protection.

1. **Define the Extent of Responsibility**: Specify the extent of the indemnitor's responsibility, including whether they are responsible for legal defines costs, settlements, or damages.

Example: The clause should detail that CRM Software, Inc. will cover all reasonable legal defense costs and any settlements or damages up to a certain financial cap.

1. **Address Limitations and Exceptions**: Include any limitations or exceptions to the indemnity, such as exclusions for claims arising from the licensee's misuse of the software or failure to comply with data protection laws.

Example: The indemnity clause should state that CRM Software, Inc. is not responsible for claims arising from XYZ Services LLC's modification of the software's source code without permission.

1. Compliance with Laws: In today's environment, data privacy and security are paramount, especially in software agreements. The clause addresses data breaches, privacy violations, and other security-related risks that could affect both parties. It ensures that these risks are adequately managed and covered.

Ensure that the indemnity clause aligns with applicable laws and regulations, such as data protection laws, intellectual property laws, and contract law.

Example: The clause should specify that both parties must comply with relevant data protection laws, and any indemnity will not apply in cases of non-compliance.

1. Legal Review:Have legal counsel review the indemnity clause to ensure it's legally sound and provides the necessary protection for both parties. Legal experts can help draft a clause that aligns with current laws and industry standards.

Example: Legal counsel for both CRM Software, Inc. and ABC Services LLC review the indemnity clause to ensure it is in compliance with relevant software licensing and intellectual property laws.

1. Revise as Necessary:Software and circumstances change over time. Periodically review and update the indemnity clause to ensure it remains relevant and effective.

Example: CRM Software, Inc. and ABC Services LLC review and update the indemnity clause annually to account for changes in the software, the industry, and legal requirements.

**Why Need Indemnity Clause in software license agreement:**

An Indemnity Clause is essential in a software license agreement for several reasons, primarily centred around risk allocation and protection of both parties involved. Here's why an Indemnity Clause is needed, with examples to illustrate its importance:

Risk Allocation: Software licenses often involve inherent risks, especially in terms of data privacy, security, and potential legal liabilities. The Indemnity Clause helps allocate these risks between the Licensor (the software provider) and the Licensee (the software user). It specifies who is responsible for handling certain types of risks and associated costs.

Example: If the Licensee (Company B) experiences a data breach due to a vulnerability in the software, the Indemnity Clause may state that the Licensee is responsible for any legal claims, financial losses, or expenses incurred as a result of the breach. This allocation of risk protects the Licensor (Company A) from being held liable for the breach.

Protection from Legal Claims: The clause safeguards the Licensor from legal claims or disputes that may arise due to actions or negligence of the Licensee during the use of the software. It outlines the specific scenarios where the Licensor is indemnified from such claims.

Example: Suppose the Licensee, while using the software, inadvertently violates data privacy regulations, leading to legal action against the Licensor. The Indemnity Clause may require the Licensee to cover the legal costs and financial losses incurred by the Licensor due to this breach.

Data Privacy and Security Concerns: In today's environment, data privacy and security are paramount, especially in software agreements. The clause addresses data breaches, privacy violations, and other security-related risks that could affect both parties. It ensures that these risks are adequately managed and covered.

Example: If a cyberattack results in a data breach affecting the Licensee's customers, the Indemnity Clause might state that the Licensee is responsible for any financial losses or legal consequences, protecting the Licensor from such claims.

Financial Responsibility: The Indemnity Clause defines the financial aspects of indemnification, including the maximum liability cap and exceptions for cases of gross negligence or willful misconduct. This ensures that the indemnifying party's financial exposure is limited.

Example: The clause might specify that the Licensee's maximum financial liability for indemnification is capped at a certain amount, which provides financial predictability for both parties and limits the Licensee's exposure in case of a significant breach.

Legal Compliance: The clause ensures that both parties adhere to relevant laws and regulations, particularly data protection laws. It allocates responsibility for compliance and any consequences of non-compliance, which is crucial in ensuring that the agreement complies with legal requirements.

Example: If a software feature is used in a way that violates a new data privacy regulation, the Indemnity Clause may outline that the Licensee is responsible for rectifying the violation and covering any associated penalties or fines. **Manage data privacy and AI-related risk clause**: Managing data privacy and AI-related risks in indemnity clauses of software license agreements is crucial in today's digital landscape. These clauses should address the potential liabilities and responsibilities of the parties regarding the handling of data and the use of artificial intelligence.

Draft of Data Privacy Risk Indemnification Clause:

This Data Privacy and AI-Related Risk Indemnification Clause (the "Clause") is an essential component of the Software License Agreement ("Agreement") between the Licensor and the Licensee.

1. Data Privacy Obligations:

a. Licensor's Obligations: The Licensor commits to handling data collected and processed through the software in compliance with all applicable data protection laws and regulations. This includes, but is not limited to, ensuring the secure storage, access, and handling of personal and sensitive data.

b. Licensee's Obligations: The Licensee shall ensure that the data collected through the software is used in strict compliance with relevant data privacy laws. The Licensee is also responsible for obtaining any necessary consents from end-users where required by law

Example: Imagine that Company A developed software, the Licensor, provides a software application to Company B, the Licensee, for managing customer data. This software collects and processes sensitive personal information, including names, addresses, and payment card details. Both companies operate in a jurisdiction subject to strict data protection laws, and the software is expected to be in full compliance.

Data Privacy Obligations:

The Licensee (Company B) is responsible for configuring and using the software in compliance with data protection laws, including obtaining proper consent from customers for data processing.

The Licensor (Company A) is responsible for developing and maintaining the software, ensuring that it is secure and complies with data protection regulations.

Now suppose, A cyberattack takes place, exploiting the software vulnerability, leading to a data breach. Personal information of numerous customers is compromised.

Unbeknownst to Company A, a software vulnerability is discovered that exposes customer data to unauthorized access. This vulnerability could be exploited by cybercriminals.

Now Legal Consequences arises after data breach, Company B faces legal consequences. Customers whose data was exposed file lawsuits against Company B, alleging negligence in protecting their personal information and non-compliance with data protection laws.

The Data Privacy Indemnification clause in the software license agreement now comes into play. It specifies that the Licensor (Company A) is responsible for any legal and financial consequences arising from data privacy breaches related to the software, provided that the Licensee (Company B) has not violated the terms of the agreement.

The indemnification clause includes provisions to indemnify Company B against third-party claims, such as those made by the affected customers, and any resulting legal and financial obligations.

Company B notifies Company A about the data breach as required by the indemnification clause, and they collaborate in addressing the issue.

Company A must bear the legal costs associated with defending Company B in the customer lawsuits. They may also be responsible for compensating affected customers for the damages they incurred as a result of the data breach.

In this scenario, the Data Privacy Indemnification clause within the software license agreement plays a crucial role in allocating responsibilities and liabilities. It helps protect Company B (the Licensee) from the legal and financial consequences of the data breach caused by a software vulnerability. Company A (the Licensor) is legally obligated to address the issue, including providing indemnification, as long as Company B is in compliance with the terms of the agreement.

**How company A include the Indemnity clause related to software license.**

**Indemnification:**

1. **Comprehensive Indemnification: Licensor shall indemnify and hold Licensee harmless from any claims, suits, or actions brought by third parties, as well as from any legal and financial consequences arising from data privacy breaches, or non-compliance with data protection laws due to the use of the software. The indemnification obligation of the Licensor extends to both claims made by third parties and to any legal and financial obligations incurred by Licensee.**
2. **b. Limitations of Liability:**

**i. Maximum Liability: The maximum aggregate liability of Licensor for any claims arising from data privacy breaches or non-compliance with data protection laws shall not exceed the total fees paid by Licensee to Licensor under this Agreement within the past twelve (12) months.**

**ii. Exclusions: The limitation of liability shall not apply to instances of gross negligence, wilful misconduct, or breaches of the Agreement related to data privacy or AI.**

1. Governing Law and Jurisdiction: a. Jurisdiction for Disputes: This Agreement shall be governed by and construed in accordance with the laws of [Applicable Jurisdiction]. Any disputes, claims, or actions arising out of or in connection with this Agreement shall be subject to the exclusive jurisdiction of the courts of [Jurisdiction].
2. Force Majeure Considerations: Force Majeure Events: Both parties acknowledge that unforeseeable events such as cyberattacks, natural disasters, or other unforeseeable events may impact data privacy and AI-related risks. Therefore, any such events shall be considered as force majeure and may be subject to separate force majeure clauses contained elsewhere in this Agreement.

**Strategy from Company A for negotiating the Indemnification clause from a commercial perspective:** When Company A (the Licensor) negotiates the Indemnification clause in terms of commercial transactions in a software license agreement, they need to balance their interests in protecting their business while ensuring a fair and mutually beneficial agreement. Here are some key considerations for negotiating the Indemnification clause from a commercial perspective:

**Define the Scope Clearly:** Company A should negotiate the scope of indemnification to ensure it's reasonably limited to issues directly related to the software's design or vulnerabilities, rather than broader issues that may arise from Licensee's actions.

Define what constitutes a covered event that triggers indemnification. For instance, specify that it covers data breaches resulting from software vulnerabilities, not from Licensee's failure to secure their systems. Financial Limitations:

**Negotiate the maximum liability cap.** Negotiate the maximum liability cap to limit Licensor’s and Licensee's financial exposure. Ensure that the cap amount aligns with the software's value and the potential risks involved.

Discuss exceptions to the limitation of liability, ensuring it doesn't cover instances of Licensor's gross negligence, wilful misconduct, or breaches of data privacy or AI obligations

**Exclusions:** Define and agree upon the specific circumstances where the limitation of liability does not apply. Ensure that exclusions are reasonable and justifiable, and discuss the threshold for gross negligence or wilful misconduct.

For instance, exclusions could apply if Licensee deliberately misuses the software or acts with gross negligence in data handling.

**Notification and Collaboration:** Specify the process and timeline for data breach notification and resolution, and negotiate this with a focus on prompt and coordinated response.

Discuss what actions both parties should take in the event of a data breach to minimize harm and potential liabilities.

Commercial Flexibility: Discuss flexibility in payment terms for indemnification, such as the ability to pay in instalments or negotiate a structured payment plan that suits both parties' cash flow.

Explore the possibility of offering additional support or services to mitigate future risks, rather than solely relying on indemnification.

**Insurance Requirements:** Consider negotiating whether the Licensee should maintain cyber liability insurance that could cover certain types of data breaches. This can be an alternative or supplement to indemnification**.**

**Audit Rights:** Negotiate the right to audit the Licensee's compliance with data protection laws and AI-related ethical considerations. This can help Company A identify and rectify potential issues before they escalate

**Dispute Resolution: Define a dispute resolution process that's commercially reasonable and efficient, such as mediation or arbitration, to resolve disagreements related to indemnification.**

**Indemnity Clause (Force Majeure Considerations, Company A's Perspective):**

1. **Force Majeure and Data Privacy Indemnification:** **A "Force Majeure Event" in the context of Data Privacy Indemnification is defined as an unforeseeable and external event beyond the reasonable control of both parties that may impact data privacy and security obligations, including but not limited to acts of nature (e.g., earthquakes, floods, hurricanes), government actions (e.g., new data privacy regulations), cyberattacks, and other events that significantly disrupt the parties' ability to fulfill their data privacy and security responsibilities under the agreement.**
2. - In the event of a Force Majeure Event affecting data privacy, the party affected by the event must promptly provide written notice to the other party, describing the event, its anticipated duration, and the expected impact on data privacy and security obligations under the agreement
3. During the suspension period caused by a Force Majeure Event, fees or other contractual obligations related to data privacy and security may be temporarily waived or adjusted as agreed upon by the parties

How to Review idenmity clauswe with example :

let's use a sample example of an indemnity clause in a software license contract and review it.

1)Sample Indemnity Clause:

Indemnification: Licensee agrees to indemnify and hold Licensor harmless from and against all claims, suits, actions, demands, liabilities, losses, damages, expenses, or costs (including reasonable attorney's fees) ("Claims") arising from or related to Licensee's use of the software. Licensee's maximum aggregate liability under this indemnity clause shall not exceed $100,000, except in cases of Licensee's gross negligence or wilful misconduct.

**Review of the Sample Indemnity Clause:**

Scope and Specificity: The clause specifies that Licensee must indemnify Licensor for all Claims related to the software's use. However, it lacks specific scenarios that would trigger indemnification, such as data privacy breaches or intellectual property disputes. A more detailed list of triggering events could enhance clarity

Revised indemnity clause that includes data privacy, data security, and AI-related risks:, Indemnification - Data Privacy, Data Security, and AI-Related Risks:

Licensee agrees to indemnify and hold Licensor harmless from and against all claims, suits, actions, demands, liabilities, losses, damages, expenses, or costs (including reasonable attorney's fees) ("Claims") arising from or related to Licensee's use of the software, including but not limited to claims related to data privacy breaches, data security vulnerabilities, or AI-related ethical violations. Licensee's maximum aggregate liability under this indemnity clause shall not exceed $100,000, except in cases of Licensee's gross negligence or wilful misconduct.

Limitations: The clause sets a maximum aggregate liability of $100,000, which provides a financial cap. It is essential to ensure that this cap is reasonable and aligns with the contract's value and risks. In this case, further context would be needed to assess the reasonableness.

**The maximum aggregate liability for Licensee under this indemnity clause, initially set at $100,000, is subject to a reasonable assessment to ensure fairness, except in cases of Licensee's gross negligence or wilful misconduct.**

Notice and Reporting: The clause doesn't include provisions regarding the notice and reporting of claims, which could lead to issues related to timely notifications.

Third-Party Claims: The clause does not specify whether it covers third-party claims or outline the responsibilities in such cases. It's essential to determine how third-party claims are handled and which party is responsible for defending against them.

Data Privacy and Compliance: The clause does not address data privacy or regulatory compliance, which is increasingly important in software license agreements. Inclusion of language to align with relevant data protection laws would be advisable.

Legal Compliance: The clause should be assessed to ensure that it complies with applicable laws and regulations. Without specific legal language, it may be necessary to seek legal guidance to confirm compliance.

Balance of Interests: The clause does not explicitly balance the interests of both parties, and it may benefit from a more equitable allocation of responsibilities.

Clear Language: The clause is relatively clear and straightforward, but it could be enhanced by providing more context regarding the specific triggering events for indemnification.

Negotiability: The clause doesn't indicate whether it is open to negotiation. If the client wishes to modify terms, it may need to be explicitly negotiated.

Consequences of Breach: The clause doesn't detail the consequences or remedial actions in case of breach. Clear language on how breaches are addressed and the associated penalties is essential.

Enforceability: It is important to ensure that the clause is legally enforceable according to the jurisdiction and relevant laws.

In a software contract, indemnity is a legal concept that addresses the responsibility for losses or damages that may arise from the use of the software. It is a clause in the contract that specifies who will bear the financial burden if the software causes harm or infringes on the rights of a third party. The indemnity clause typically outlines the terms under which one party agrees to compensate the other for any legal claims, losses, or liabilities related to the software.

Let's consider an example involving AI software:

Imagine a company purchases AI software for managing customer data, and the software provider includes an indemnity clause in the contract. If the software turns out to have a bug that leads to a data breach, and this breach results in legal claims or financial losses for the company, the indemnity clause will come into play.

The scope of indemnity clause is playing vital role in software licence contract.

There are two common types of indemnity clauses in software contracts:

Broad Indemnity: This type of indemnity clause often states that the software provider (typically the developer or vendor) will indemnify and hold harmless the customer from any claims, losses, or damages arising out of the use of the software, regardless of whether the issue is due to the software's defects or the customer's actions.

Broad Indemnity clause example :

**The Software Provider shall indemnify the Customer against claims by third parties that the Software infringes any valid intellectual property rights, provided that the Customer promptly notifies the Software Provider in writing of such claims, gives the Software Provider sole control of the defense and settlement of such claims, and cooperates with the Software Provider in defending or settling such claims."**

In the example of Broad Indemnity, the software provider is assuming a broader and more significant burden by agreeing to indemnify the customer for any issues related to the software, even if the provider is not directly at fault. This could include issues such as software defects, security breaches, and more. The provider is essentially taking on a high level of responsibility for the software's performance.

Limited Indemnity: This clause is more restrictive and may state that the software provider will only indemnify the customer if the claims or damages result from the software's defects or breaches of intellectual property rights. It limits the scope of indemnity to certain specific scenarios.

Limited indemnity clause example :

"The Software Provider shall indemnify the Customer against claims by third parties that the Software infringes any valid intellectual property rights, provided that the Customer promptly notifies the Software Provider in writing of such claims, gives the Software Provider sole control of the defense and settlement of such claims, and cooperates with the Software Provider in defending or settling such claims."

If the contract has a limited indemnity clause, the software provider would only be responsible for covering the legal costs, damages, and losses if they were directly caused by the software's defect. If the data breach was due to the company's mishandling or other factors not related to the software's design or functionality, the provider might not be liable.