Professional Certificate in Contract Law in Technology (Germany)

Contract Termination and Remedies

Contract termination in the context of technology agreements in Germany is a multifaceted concept that incorporates statutory provisions of the Bürgerliches Gesetzbuch (BGB), case law, and the specific clauses drafted by the parties. Understanding the vocabulary surrounding termination and the subsequent remedies is essential for any practitioner who advises on software licences, cloud-computing services, or hardware procurement contracts. The following exposition presents the most important terms, explains their legal significance, illustrates their application with practical examples, and highlights typical challenges that arise in technology-focused contracts.

Termination for cause – also known as termination for breach – occurs when one party fails to fulfil a fundamental contractual obligation, giving the other party the right to end the agreement. In German law the key notion is material breach (wesentliche Pflichtverletzung). A material breach is a violation that deprives the injured party of the essential benefit of the contract, and it must be serious enough to justify termination. For example, a SaaS provider that repeatedly delivers a platform with critical security vulnerabilities, despite repeated notices, may be in material breach of its duty to provide a “secure and reliable service”. The customer may therefore invoke termination for cause.

Anticipatory repudiation (vorweggenommene Vertragsverletzung) is a related concept. It occurs when a party clearly indicates, before the performance date, that it will not perform its contractual duties. The injured party may treat the contract as terminated immediately, rather than waiting for the performance date to pass. In a cloud-infrastructure contract, if the provider sends a notice stating that it will discontinue the service within three months, the client can invoke anticipatory repudiation and terminate the contract now, securing the right to seek remedies.

Termination for convenience (Kündigung aus wichtigem Grund) is a unilateral right to end the contract without assigning fault to the other party. Under German law, a party may only rely on a contractual clause that expressly provides for termination for convenience. The clause must specify the notice period and any compensation that the terminating party must pay. In practice, many technology contracts include a “termination for convenience” clause that allows the purchaser to end the agreement after a defined period, often in exchange for a termination fee that reflects the provider’s sunk costs.

Termination by mutual agreement (Aufhebungsvertrag) is the simplest method: The parties agree to bring the contract to an end. This approach is frequently used when a software development project fails to meet expectations, and both sides wish to avoid protracted litigation. The agreement should clearly state the date of termination, any outstanding payments, and the handling of intellectual-property rights that have been created during the collaboration.

Notice period (Kündigungsfrist) – The notice period is the time interval between the communication of termination and the effective date of termination. German law distinguishes between statutory notice

periods (e.G., § 622 BGB for employment contracts) and contractual notice periods agreed by the parties. In technology contracts, notice periods are often tailored to the nature of the service. A short-term cloud service may have a 30-day notice, whereas a long-term enterprise software licence may require a 90-day notice to give the provider sufficient time to reallocate resources.

Unilateral termination clause – This clause grants one party the right to terminate unilaterally under certain conditions, such as a change in applicable law, a merger, or a breach of a confidentiality provision. The clause must be drafted with precision; otherwise, it may be deemed an unfair term under the German Civil Code, especially if it creates a significant imbalance in the parties' rights and obligations.

Force majeure (höhere Gewalt) – Force-majeure events are extraordinary circumstances beyond the control of the parties, such as natural disasters, wars, or major cyber-attacks that render performance impossible. A force-majeure clause typically allows suspension of performance for the duration of the event and, if the event persists beyond a certain time, permits termination without liability. The challenge in technology contracts is defining the scope of force majeure, as many cyber incidents may be considered "ordinary risks" unless expressly excluded.

Impossibility of performance (Unmöglichkeit) – Impossibility is a legal doctrine that releases a party from its contractual obligations when performance becomes objectively impossible. Under § 275 BGB, if a software component that was promised cannot be delivered because the underlying technology has been discontinued, the provider may invoke impossibility. However, the doctrine is applied narrowly; a temporary technical difficulty usually does not constitute impossibility.

Change of circumstances (Störung der Geschäftsgrundlage) – This principle allows a contract to be adjusted or terminated when an unforeseen event fundamentally alters the equilibrium of the contract. In technology contracts, a sudden regulatory change that bans the export of encryption software to a particular jurisdiction may trigger a change-of-circumstances claim. The injured party must demonstrate that the change was not anticipated and that it renders performance excessively burdensome.

Termination for breach of warranty – Warranty (Gewährleistung) in German law refers to the statutory guarantee that the seller must deliver goods free from defects. In technology contracts, warranties may also cover software functionality, compliance with specifications, and the absence of hidden defects. If the delivered software contains a defect that makes it unsuitable for its intended purpose (e.G., A critical bug that prevents data synchronization), the buyer may issue a notice of defect (Mängelrüge) and demand remediation. Failure to remedy within a reasonable time can lead to termination for breach of warranty.

Right to cure (Nachfrist) – Before terminating for breach, the injured party generally must grant the breaching party a reasonable period to cure the defect. This is the "nachfrist". In practice, the injured party sends a written notice specifying the defect and the deadline for cure. If the provider does not remedy the defect within the stipulated period, the buyer can terminate and claim damages. The length of the nachfrist depends on the nature of the breach; a minor bug may require a short cure period, whereas a systemic failure may justify a longer period.

Damages (Schadensersatz) – Once a contract is terminated, the injured party may claim monetary

compensation for the losses suffered. German law distinguishes between compensatory damages (Schadensersatz) and liquidated damages (Vertragsstrafe). Compensatory damages aim to put the injured party in the position it would have occupied had the contract been performed. In a technology licence, if the licensor's breach forces the licensee to purchase an alternative solution at a higher price, the licensee can claim the price difference as compensatory damages.

Liquidated damages – These are pre-agreed amounts stipulated in the contract to be payable upon breach. Liquidated damages clauses are common in high-value IT projects to provide certainty and avoid disputes over the amount of loss. Under § 309 Nr. 2 BGB, such clauses must be "reasonable" and cannot create an "excessive penalty". Courts will assess whether the amount is proportionate to the anticipated damage. For example, a contract may stipulate a €100,000 penalty for each week of delay in delivering a custom ERP system. If the actual loss per week is substantially lower, a court may reduce the amount.

Mitigation of loss (Schadensminderungspflicht) – The injured party has a duty to mitigate its losses. In technology contracts, this means that a client who terminates a service must take reasonable steps to obtain an alternative solution, rather than simply sitting idle. Failure to mitigate can result in a reduction of awarded damages. For instance, if a client terminates a cloud-hosting agreement and does not seek a comparable service, the court may deem the client's inaction as unreasonable and limit the damages.

Retention of title (Eigentumsvorbehalt) – This clause allows the seller to retain ownership of hardware until the buyer has paid the full purchase price. In the event of termination for cause, the seller may invoke the retention of title to reclaim the equipment. The buyer, however, must return the hardware in a condition consistent with normal use. The clause is particularly relevant for hardware-as-a-service (HaaS) arrangements where the provider supplies servers that remain its property.

Set-off (Aufrechnung) – Set-off permits a party to offset a claim it holds against the other party with a counter-claim. In termination scenarios, a provider may set-off unpaid fees against the client's claim for damages. The right to set-off is subject to contractual conditions and must be exercised in good faith. In practice, a provider might withhold a portion of the termination fee until the client returns all proprietary software and data.

Termination fees – These are payments that the terminating party must make to the other party, often reflecting the costs incurred in preparing for performance. In technology contracts, termination fees are common when the provider has invested heavily in custom development. The fee must be reasonable and proportionate; otherwise, it may be deemed a penalty. For instance, a contract may require a terminating party to pay 20 % of the total contract value if termination occurs before the first delivery milestone.

Refund of prepaid amounts – When a contract is terminated, any prepaid fees for services not yet rendered must be refunded. The calculation of the refund can be complex in subscription-based models where the fee covers a period of service. The parties may agree on a pro-rata refund, deducting any usage costs incurred up to the termination date.

Intellectual-property rights – Termination often raises questions about the ownership and licensing of IP created during the contract. In a software development agreement, the client may own the source code, but

the provider may retain a licence to use certain reusable components. Upon termination, the agreement should specify whether the client must return the provider's IP, destroy copies, or continue to use it under a licence. Failure to address this can lead to infringement claims.

Confidentiality obligations – Confidentiality clauses survive termination in most contracts. The parties remain bound to protect each other's confidential information even after the contractual relationship ends. In technology contracts, where trade secrets and source code are involved, robust confidentiality provisions are essential. Breach of confidentiality after termination can give rise to damages and injunctive relief.

Data protection and privacy – The General Data Protection Regulation (GDPR) imposes specific duties on data controllers and processors. When a contract is terminated, the parties must ensure the lawful transfer or deletion of personal data. For example, a cloud-service provider must delete or return all customer data within a stipulated period after termination, unless a separate data-processing agreement provides otherwise. Non-compliance can result in regulatory fines in addition to contractual damages.

Escrow arrangements – In critical software projects, the parties may agree to place the source code in escrow with a third-party agent. The escrow agreement typically defines trigger events, such as the provider's insolvency or breach, that allow the client to obtain the source code. Upon termination for cause, the client may activate the escrow and obtain the code to continue the project with another provider, thereby mitigating disruption.

Termination for insolvency – German insolvency law (Insolvenzordnung) provides that a contract can be terminated automatically upon the filing of insolvency for the other party, unless the contract is of a type that must be continued (e.G., A lease). In technology contracts, a provider's insolvency may trigger automatic termination, but the parties often negotiate "continuity clauses" that allow the client to continue using the service under the same terms while the provider's assets are administered by an insolvency practitioner.

Assignment and sub-licensing – The ability to assign rights or sub-license software can be affected by termination. A clause may prohibit assignment without consent, or it may allow assignment upon termination, provided that the assignee meets certain qualifications. This is particularly relevant in SaaS contracts where the provider wishes to transfer the service to a successor entity.

Termination of maintenance and support – Maintenance clauses often survive the termination of the primary licence for a limited period. For example, a software vendor may agree to provide bug-fixes for 12 months after the licence ends. The contract should clearly delineate the scope and duration of post-termination support, as well as any fees that may apply.

Force-majeure vs. Contractual termination rights – While force-majeure can excuse performance, it does not automatically confer a right to terminate unless the contract expressly provides for it. Practitioners must therefore draft termination clauses that reference force-majeure events, specifying when such events give rise to termination rights and the required notice.

Termination notice content – The notice of termination must contain certain elements to be effective under

German law: Identification of the parties, reference to the contractual provision being invoked, a clear statement of intent to terminate, the effective date, and any required cure period. The notice must be delivered in a manner prescribed by the contract (e.G., Registered mail, electronic transmission) and must reach the recipient.

Electronic notice – Modern technology contracts often allow termination notices to be sent electronically, provided that the method ensures receipt and authenticity. Parties may agree to use qualified electronic signatures (QES) to satisfy the legal requirement for written form under § 126 BGB. Failure to comply with the agreed method can render the termination ineffective, leading to disputes.

Effect of termination on warranties – Termination does not automatically extinguish warranties that were in force before termination. For instance, a hardware supplier's warranty for defects may continue for the statutory period after the contract ends, unless the contract expressly limits it. The client must be aware of any surviving warranty obligations to avoid unexpected liability.

Partial termination – A contract may be partially terminated, meaning that only certain obligations or parts of the agreement are ended. This is common in multi-module SaaS contracts where a client may discontinue a specific module while retaining the rest of the service. The contract should specify the mechanism for partial termination, including the allocation of fees and the handling of data associated with the terminated module.

Termination and third-party rights – In technology contracts, third parties such as subcontractors, resellers, or end-users may be affected by termination. The contract should address the impact on these parties, for example by granting the client a licence to use the software for the benefit of its customers after termination. Ignoring third-party rights can lead to infringement claims or breach of contract actions by downstream users.

Termination and regulatory compliance – Certain technology contracts are subject to sector-specific regulations (e.G., Financial services, healthcare). Termination may trigger obligations to maintain compliance, such as preserving audit logs for a defined period. The parties must allocate responsibility for post-termination compliance activities, otherwise regulatory authorities may impose sanctions.

Remedies for wrongful termination – If a party terminates a contract without valid cause, the other party may seek remedies for wrongful termination. Under German law, the injured party can demand rescission (Rücktritt) of the termination, reinstatement of the contract, or damages for the loss incurred. In practice, wrongful termination claims often focus on the breach of a termination clause that required a specific cause or notice period.

Rescission (Rücktritt) – Rescission restores the parties to their pre-contractual positions. It is available when the termination was wrongful, but the injured party wishes to continue the contractual relationship. The injured party must return any benefits received (e.G., Software licences) and may be required to pay a reasonable compensation for the services already performed.

Specific performance – In some technology contracts, the injured party may request specific performance

(Erfüllung) as a remedy, compelling the breaching party to fulfil its obligations. Courts are generally reluctant to order specific performance for personal services, but they may order it for the delivery of software or hardware, especially where monetary damages are inadequate. However, specific performance is often impractical in fast-moving tech environments, leading parties to rely on damages.

Injunctions – An injunction (Einstweilige Verfügung) can be sought to prevent a party from continuing a breach, such as the unauthorised use of proprietary code after termination. Injunctive relief is common in intellectual-property disputes arising from termination, where the injured party wants to stop the counterpart from exploiting confidential or protected material.

Damages calculation – direct vs. Consequential losses – German law distinguishes between direct damages (Schaden) and consequential damages (Folgeschäden). Direct damages are the immediate loss caused by the breach (e.G., The cost of a replacement system). Consequential damages include lost profits, loss of opportunity, and other indirect effects. The contract may limit or exclude consequential damages; such exclusions must be clear, understandable, and not unreasonably disadvantageous to the injured party.

Limitation periods – Claims for damages arising from termination are subject to limitation periods. Under § 195 BGB, the general limitation period is three years from the date the claim became known. However, specific provisions may shorten or extend this period. Practitioners must advise clients to act promptly, especially in rapidly evolving tech sectors where the damage may be discovered long after termination.

Choice of law and jurisdiction – International technology contracts often involve parties from different jurisdictions. The contract should specify the governing law (usually German law for contracts performed in Germany) and the competent courts. The choice of law clause influences the interpretation of termination provisions and the available remedies. For cross-border disputes, parties may also agree on arbitration, which can provide a faster and more specialised forum for technology-related issues.

Arbitration awards and enforcement – Arbitration clauses are common in technology contracts to ensure expertise and confidentiality. An arbitration award that orders termination fees or damages can be enforced in German courts under the New York Convention. However, the enforceability of termination clauses that are deemed “unfair” under German law may be challenged even in arbitration, so the drafting must align with German public policy.

Termination and transition services – To minimise disruption, many contracts include a transition services clause that obliges the provider to cooperate in transferring data, knowledge, and operations to a new provider after termination. The clause typically defines the scope, duration, and fees for transition services. Failure to provide adequate transition assistance can give rise to a claim for damages resulting from the interruption of critical services.

Termination and data migration – In cloud-migration projects, termination may occur before data migration is complete. The contract should specify the responsibilities for data extraction, format conversion, and verification. The provider may charge a “data-extraction fee” proportional to the volume of data and the effort required. The client must ensure that the contract includes warranties that the data will be transferred securely and without loss.

Termination and intellectual-property licensing – A licence may be granted “solely for the duration of the contract”. Upon termination, the licence may automatically expire, requiring the client to cease use of the software. Some licences, however, include a “survival clause” that permits continued use for a defined period after termination, often for the purpose of transitioning to alternate software.

Termination and open-source obligations – When a contract involves open-source components, termination may affect the obligations to provide source code or comply with licences such as GPL. The contract should clarify whether the open-source obligations survive termination and how the parties will handle the distribution of source code after the agreement ends.

Termination and service-level agreements (SLAs) – SLAs define performance metrics (e.G., Uptime, response time). Persistent failure to meet SLAs may constitute a material breach, giving rise to termination rights. The contract should articulate the remedies for SLA breaches, such as service credits, the right to terminate after a specified number of violations, and the calculation of damages based on the severity of the breach.

Termination and penalty clauses – Penalty clauses (Strafklauseln) impose a monetary penalty for breach, independent of actual loss. Under German law, penalty clauses are enforceable unless they are “excessive”. The court may reduce an excessive penalty to a reasonable amount. In technology contracts, penalty clauses are frequently tied to deadlines for delivery of software modules, with predefined sums for each day of delay.

Termination and confidentiality of source code – The source code of a bespoke software solution is often considered a trade secret. Upon termination, the provider may require the client to return or destroy copies of the source code, or may grant a limited licence to use the code for maintenance purposes only. The contract must specify the method of verification (e.G., A third-party audit) to ensure compliance.

Termination and export controls – Export control regulations (e.G., The EU Dual-Use Regulation) can affect termination. If a contract involves the transfer of encryption technology subject to export restrictions, termination may be required if the parties cannot obtain the necessary licences. The contract should allocate responsibility for obtaining export licences and outline the consequences of non-compliance, including the right to terminate.

Termination and anti-corruption compliance – Many technology contracts contain anti-corruption clauses that require the parties to comply with the German Act on Combating Corruption (Gesetz zur Bekämpfung von Korruption). A breach of such a clause can be a ground for immediate termination. The contract may also provide for damages resulting from any fines or reputational harm caused by the breach.

Termination and change-order processes – In development contracts, change orders (Änderungsaufträge) modify the scope, cost, or schedule. Repeated or unilateral change orders that significantly alter the original agreement may constitute a material breach, giving rise to termination rights. The contract should define a clear change-order procedure and the consequences of non-conformant changes.

Termination and performance bonds – A performance bond (Bürgschaft) may be required from the provider to secure performance. Upon termination for cause, the client can claim on the bond to recover losses. The

bond terms must specify the conditions under which a claim can be made, the amount of the bond, and the procedure for invoking it.

Termination and escrow release conditions – Escrow agreements typically list specific events that trigger the release of source code. Termination for cause may be one such trigger, but the contract must be clear whether the client can access the escrowed code immediately upon termination or only after a cure period. The escrow provider may also require proof of the breach before releasing the code.

Termination and subcontractor obligations – If the provider relies on subcontractors for parts of the service (e.G., Data centre hosting), termination of the primary contract may affect the subcontractors' rights and obligations. The primary contract should contain provisions that require the provider to ensure that subcontractors honor confidentiality, data-protection, and IP obligations even after termination.

Termination and documentation handover – A comprehensive handover of documentation (technical specifications, user manuals, configuration files) is critical to avoid disputes. The contract should obligate the provider to deliver complete and up-to-date documentation before termination takes effect. Incomplete handover can lead to claims for additional costs incurred by the client in reconstructing the system.

Termination and insurance – Professional liability insurance (Berufshaftpflichtversicherung) can cover damages arising from breach of contract. The contract may require the provider to maintain insurance throughout the term and to provide certificates of insurance upon request. In the event of termination, the insurance may be invoked to compensate the client for losses, provided that the claim falls within the policy limits.

Termination and force-majeure clause drafting tips – To avoid ambiguity, the clause should list specific events (e.G., Natural disasters, war, cyber-attack deemed "act of God"), define the notice requirements, and state the effect on the contract (suspension vs. Termination). Including a "materiality test" (i.E., The event must materially affect performance) helps prevent parties from invoking force-majeure for minor setbacks.

Termination and governing law interaction with EU regulations – Even if German law governs the contract, EU directives (e.G., The Consumer Rights Directive) may impose additional obligations on termination, particularly when the client is a consumer. The contract must reconcile these higher-order rules, ensuring that any termination clause does not infringe consumer protection standards.

Termination and data-processing agreements (DPAs) – A DPA attached to a cloud-service contract outlines the responsibilities for personal data. Upon termination, the DPA typically requires the provider to delete or return the data within a specified timeframe. Failure to comply can result in regulatory penalties and civil claims for breach of data-protection obligations.

Termination and audit rights – Many technology contracts grant the client audit rights to verify compliance with security standards or licensing terms. After termination, the client may retain a limited audit right to confirm that the provider has properly destroyed or returned all confidential data and IP. The audit clause should define the scope, timing, and cost allocation for post-termination audits.

Termination and warranty periods – Warranty periods may survive termination for a defined term. For

example, a hardware supplier may provide a two-year warranty on equipment even after the purchase contract ends. The contract must state whether the warranty is tied to the original purchase price or to a separate service agreement.

Termination and maintenance contracts – Maintenance contracts are often separate from the main licence. When the main contract terminates, the maintenance contract may continue independently, or it may be automatically terminated. The parties should decide whether maintenance fees will continue to be payable and whether the provider will still deliver updates.

Termination and “no-shop” clauses – In acquisition scenarios, a “no-shop” clause may restrict the seller from negotiating with other potential buyers for a set period. If the buyer terminates the agreement, the clause may still bind the seller, preventing it from seeking alternative purchasers for the technology. The clause must be carefully drafted to avoid antitrust concerns.

Termination and “right of first refusal” (Vorkaufsrecht) – Some contracts grant the client a right of first refusal on additional modules or upgrades. Termination may extinguish this right, unless the contract explicitly preserves it. The parties should clarify whether the right survives termination and under what conditions it may be exercised.

Termination and “change of control” provisions – A change-of-control clause allows a party to terminate if the other party undergoes a merger or acquisition. In technology contracts, a provider’s acquisition by a competitor may raise concerns about data security or continuity of service. The clause should define the notice period, any termination fees, and the obligations for data protection during the transition.

Termination and “force-majeure” in the context of cyber-attacks – Increasingly, parties consider major cyber-incidents as force-majeure events. However, German courts tend to treat cyber-attacks as business risks unless the contract expressly categorises them as force-majeure. To secure a termination right in such cases, the clause must specifically list “significant cyber-attack” or “large-scale data breach” as qualifying events.

Termination and “liquidated damages” schedule – A detailed schedule of liquidated damages can provide certainty. For instance, a schedule may specify a €10,000 penalty for each week of delay in delivering a core module, a €5,000 penalty for each missed milestone, and a €2,000 penalty for each failure to meet a performance metric. The schedule must be proportional to the anticipated loss and must avoid being punitive.

Termination and “cumulative remedies” – Contracts may allow the injured party to pursue multiple remedies (e.G., Damages plus specific performance). German law permits cumulative remedies unless the contract expressly limits them. Practitioners should advise clients on the strategic choice of remedies, balancing the need for compensation against the desire to maintain the relationship or protect reputation.

Termination and “mitigation costs” – When a client terminates a contract and engages a replacement provider, the costs incurred for the transition (e.G., Consulting fees, data migration expenses) are considered mitigation costs. The client can claim these costs as damages, provided they are reasonable and directly

attributable to the breach. Documentation of all mitigation expenses is essential for successful recovery.

Termination and “conflict of laws” in cross-border technology projects – If a German company terminates a contract with a foreign partner, the conflict-of-laws rules may determine which jurisdiction’s law governs the interpretation of termination clauses. The Rome I Regulation generally applies to contractual obligations within the EU, designating the law chosen by the parties. However, mandatory provisions of German law (e.G., Consumer protection) may still apply, limiting the parties’ freedom to contract out of certain protections.

Termination and “good faith” (Treu und Glauben) – The principle of good faith under § 242 BGB permeates all contractual relations, including termination. A party must not terminate in a manner that is abusive or that exploits a loophole in the contract. For example, invoking a termination clause solely to avoid paying a performance bonus, while continuing to benefit from the service, may be deemed a breach of good faith, exposing the terminating party to liability.

Termination and “contractual penalties for early termination” – Early-termination penalties are common in long-term licences. The penalty is usually expressed as a percentage of the remaining contract value. The clause must be clear about the calculation method, the events that trigger the penalty, and any caps on the amount. Courts will enforce such penalties if they are proportionate to the anticipated loss.

Termination and “data-migration assistance” – When a client terminates a SaaS agreement, the provider may be obligated to assist with data migration to a new platform. The contract should define the format, scope, and timeline for migration assistance, as well as any additional fees. Failure to provide adequate migration support can give rise to a claim for consequential damages, especially if the client suffers business interruption.

Termination and “continuity of service” provisions – Some contracts contain a continuity clause that obliges the provider to maintain service levels for a short period after termination to allow the client to transition smoothly. This “post-termination service period” is often limited to 30 days and may be provided at a reduced fee. The clause helps mitigate the risk of abrupt service loss and can be a negotiating point in termination discussions.

Termination and “security incident reporting” – In the event of termination, the provider may be required to disclose any security incidents that occurred during the contract term. The contract should stipulate the timing, format, and confidentiality of such disclosures. This information is vital for the client to assess residual risk and take remedial actions.

Termination and “intellectual-property indemnification” – Many technology contracts include an indemnity clause whereby the provider indemnifies the client against third-party IP infringement claims. Upon termination, the indemnity may survive, ensuring that the client remains protected if a claim arises after the contract ends. The indemnity clause should specify the scope, limits, and procedures for invoking the indemnity.

Termination and “audit of compliance with open-source licences” – Open-source compliance is increasingly

important. A termination clause may require the provider to certify that all open-source components used in the delivered software comply with their licences. The client may retain the right to audit this compliance even after termination, to avoid liability for inadvertent licence violations.

Termination and “force-majeure” clause drafting – practical tip – Include a “materiality threshold” that defines the minimum impact required for force-majeure to apply (e.G., A disruption of at least 30 % of the service). This prevents parties from invoking force-majeure for minor performance hiccups and provides a clear benchmark for assessing whether termination is justified.

Termination and “recovery of confidential information” – Upon termination, the injured party should request the return or destruction of all confidential material. A written confirmation of destruction, possibly witnessed by a third party, can serve as evidence that the obligation was fulfilled, reducing the risk of subsequent infringement claims.

Termination and “post-termination audit rights for software licences” – If the client terminates a licence, the provider may be entitled to audit the client’s use of the software to ensure compliance with the licence terms up to the termination date. The audit clause should define the audit scope, timing, and cost allocation, and it should survive termination for a reasonable period.

Termination and “risk-allocation” in cloud-service agreements – Cloud contracts often allocate risk through limitation of liability clauses, capping damages at the total fees paid. However, such caps may be unenforceable for breaches involving data loss or statutory obligations. The contract should balance risk allocation by combining caps with specific exclusions for gross negligence, fraud, and data-protection violations.

Termination and “service transition plan” – A detailed transition plan, negotiated at the outset, outlines the steps each party will take if termination occurs. The plan typically includes data extraction schedules, knowledge-transfer workshops, and the handover of administrative access. Having a pre-agreed plan reduces uncertainty and facilitates a smoother exit.

Termination and “reliance on third-party software” – Many technology solutions embed third-party components. The contract should address the effect of termination on those components, including the need to obtain separate licences or to replace the components. Failure to consider third-party dependencies can result in the client inadvertently infringing licences after termination.

Termination and “contractual audit of security controls” – Security audits may be required periodically. The contract may stipulate that the provider must allow security audits throughout the term and for a limited period after termination. The audit clause should define the audit methodology, confidentiality obligations, and the handling of any findings.

Termination and “regulatory reporting obligations” – Certain technology services, such as financial-technology platforms, are subject to regulatory reporting. The contract must allocate responsibility for filing reports after termination, ensuring that the regulator receives accurate information and that the parties avoid penalties.

Termination and “non-competition” clauses – Some contracts contain non-competition provisions that survive termination, preventing the client from engaging a competitor for a defined period. In the technology sector, these clauses must be narrowly tailored to be enforceable, focusing on specific services or markets and limiting the duration to a reasonable time frame.

Termination and “liquidated damages” versus “actual damages” – When a breach is foreseeable, parties may prefer liquidated damages for predictability. However, if the breach is unexpected, actual damages may be more appropriate. The contract may include a hybrid approach: Liquidated damages for delays, and actual damages for quality failures. This hybrid model provides flexibility while preserving certainty.

Termination and “contractual amendment procedures” – The contract should specify how amendments, including termination clauses, can be modified. Typically, amendments require written agreement signed by both parties. Verbal agreements or email confirmations may not satisfy the “written form” requirement under § 126 BGB, potentially rendering the amendment ineffective.

Termination and “dispute-resolution mechanisms” – The contract must state how termination-related disputes will be resolved. Options include negotiation, mediation, arbitration, or litigation. Including a step-down approach (e.G., Negotiation → mediation → arbitration) can help preserve business relationships while providing a clear pathway to resolution.

Termination and “post-termination confidentiality” – Confidentiality obligations often survive termination indefinitely. The contract should clarify the duration and scope of post-termination confidentiality, particularly concerning proprietary algorithms, source code, and business processes. Breach of post-termination confidentiality can lead to injunctive relief and damages.

Termination and “data-retention policies” – The contract should align with the client’s data-retention policy, specifying how long the provider must retain data after termination before deletion.