Professional Certificate in Contract Law in Technology (Germany)

Contract Drafting and Review

Offer – The initial proposal made by one party that sets out the intention to conclude a contract on specific terms. In a technology context an offer may be presented as a software licensing proposal, a cloud-service quotation, or a development contract draft. The offer must be sufficiently certain, containing essential elements such as the subject matter, price, and duration, so that the offeree can accept it without further negotiation. Example: A software vendor sends an email stating, “We propose to grant you a non-exclusive license to use our analytics platform for three years at an annual fee of €50,000.” The moment this email reaches the potential client it becomes an offer, provided it is not labelled as “subject to further discussion.”

Acceptance – The unequivocal assent to the terms of the offer, communicated by the offeree. Acceptance must mirror the offer; any deviation creates a counter-offer rather than a binding agreement. In technology contracts acceptance is often conveyed via a signed purchase order, an electronic click-through on a SaaS sign-up page, or a written email confirming the terms. Practical tip: Always include a clause stating that acceptance is effective only upon receipt of a signed document or a specific electronic confirmation to avoid disputes over timing.

Consideration – The value exchanged between the parties, which can be monetary, a promise to perform, or a forbearance. German contract law (BGB) does not require consideration in the same way as common-law systems, but the principle of reciprocal obligations remains essential. In a cloud-service agreement the consideration is usually the subscription fee paid by the customer in exchange for access to the service.

Capacity – Legal ability of a party to enter into a contract. In Germany, individuals must be at least 18 years old and not under legal guardianship. Corporate entities must have the appropriate statutory authority, such as a board resolution authorising the signing of a software development agreement. Drafting practice: Include a representation clause where each party confirms it has the capacity to bind itself.

Legality – The contract’s subject matter must be lawful. Contracts that involve illegal activities, such as the distribution of pirated software, are void. In the technology sector, particular attention must be paid to data-protection regulations; a data-processing clause that contravenes the GDPR renders the agreement unenforceable.

Terms of Contract – The specific provisions that define the rights and duties of the parties. In technology contracts these typically include scope of work, licensing rights, service levels, payment schedule, confidentiality, and termination. Each term should be drafted with precision to avoid ambiguity. For instance, instead of stating “reasonable time,” specify “within five (5) business days after receipt of the invoice.”

Scope of Work (SoW) – A detailed description of the deliverables, milestones, and responsibilities. In a software development contract the SoW may enumerate functional specifications, programming languages, testing procedures, and documentation standards. A well-crafted SoW reduces the risk of scope creep and

provides a clear basis for measuring performance.

Milestones – Pre-defined points in the project timeline linked to deliverables and payment triggers. Example: “Milestone 1 – Completion of system architecture design, payable €20,000 within ten days of acceptance.” Milestones should be objectively verifiable, with clear acceptance criteria, to minimise disputes over whether a deliverable has been satisfied.

Service Level Agreement (SLA) – A contract-or-specific annex that sets quantitative performance standards such as uptime, response time, and resolution time. An SLA might state that “The service shall be available 99.9 % Of each calendar month, measured by the provider’s monitoring system.” Include remedies for breach, such as service credits or the right to terminate for repeated failures.

Uptime – The percentage of time a service is operational. In cloud contracts, uptime is often expressed as a monthly figure and is a key metric for customers. Drafting tip: Define how uptime is calculated, what exclusions (e.G., Scheduled maintenance) apply, and what penalties accrue if the target is not met.

Response Time – The maximum period within which the provider must acknowledge a support request. For critical incidents a response time of 30 minutes may be stipulated, whereas for non-critical queries a 24-hour window could be acceptable. Precise definitions prevent divergent interpretations.

Confidentiality – The obligation to protect non-public information exchanged during negotiations or performance. In technology contracts, confidential information often includes source code, algorithms, and business plans. A typical clause reads: “Each party shall keep the other party’s Confidential Information strictly confidential and shall not disclose it to any third party without prior written consent.”

Non-Disclosure Agreement (NDA) – A standalone contract or a clause within a larger agreement that governs the handling of confidential information. NDAs are frequently executed before any substantive negotiation, especially when discussing proprietary technology. Ensure the NDA defines the duration of confidentiality obligations, often “for a period of five (5) years after termination.”

Intellectual Property (IP) – The legal rights that protect creations of the mind, including patents, copyrights, trademarks, and trade secrets. In technology contracts the allocation of IP rights is a pivotal issue. Parties must decide whether the provider retains ownership of the software and grants a license, or whether ownership transfers to the customer upon payment.

Copyright – Protects original works of authorship, such as software code, documentation, and UI designs. Under German law (UrhG) copyright arises automatically upon creation, without registration. When drafting a software licence, specify whether the license is exclusive, non-exclusive, perpetual, or limited to a particular field of use.

Patent – Grants exclusive rights to an invention that is novel, inventive, and industrially applicable. In technology contracts, patent licences may be required for patented algorithms embedded in a product. A clause may read: “The Licensor grants the Licensee a worldwide, royalty-free, non-exclusive licence to use the patented technology solely for the purpose of operating the Software.”

Trademark – Protects signs that distinguish goods or services. In SaaS agreements, the provider may permit the customer to use its brand marks in marketing materials, subject to quality control. Include a clause that outlines the permitted use and any required approvals.

Trade Secret – Information that derives economic value from being secret and is subject to reasonable measures to keep it confidential. Trade-secret protection is especially relevant for proprietary algorithms. A confidentiality clause should expressly cover trade secrets and define the standard of care required.

License – The permission granted by the IP owner to another party to use, modify, or distribute the protected work under defined conditions. Licenses can be exclusive (sole right), non-exclusive (multiple licensees), or sole (only the licensor may grant additional licences). Clarify the scope: "The Licensee may use the Software in the Territory for the Business Purpose defined in Schedule A."

Territory – The geographic area where the license is valid. In cross-border software distribution, the territory may be limited to the European Economic Area (EEA) to simplify compliance with EU data-protection law. If worldwide use is intended, ensure that the licence does not conflict with export-control regulations.

Field of Use – The specific industry or purpose for which the licensed technology may be employed. Example: "The Licensee may use the Software solely for internal financial-risk analysis." Restricting the field of use can preserve the licensor's ability to license the same technology to competitors in other sectors.

Sublicensing – The right of the licensee to grant further licences to third parties. Sublicensing is common in platforms that enable developers to build on top of an API. If permitted, the contract should set conditions, such as requiring the sublicensee to adhere to the same confidentiality and IP obligations.

Open-Source – Software whose source code is made publicly available under a licence that permits use, modification, and redistribution. Open-source components may be incorporated into proprietary products, but the licences (e.G., GPL, MIT, Apache) impose obligations. Drafting tip: Include an "Open-Source Software" schedule that lists all open-source components and their licences, and specify whether the resulting work must be distributed under the same licence.

Indemnity – A promise to compensate the other party for losses arising from specified events, such as IP infringement claims. In technology contracts a typical indemnity clause reads: "The Provider shall indemnify the Customer against any third-party claim that the Software infringes a valid patent, provided the Customer promptly notifies the Provider and gives it control of the defence."

Limitation of Liability – A clause that caps the amount of damages a party can be required to pay. Common caps are based on the total fees paid under the contract, or a multiple thereof. Example: "Neither party shall be liable for indirect, consequential, or punitive damages, and each party's total aggregate liability shall not exceed three (3) times the fees paid in the twelve (12) months preceding the claim."

Force Majeure – Events beyond the parties' control that excuse performance, such as natural disasters, war, or pandemics. German law (§ 275 BGB) recognises impossibility of performance, but a force-majeure clause provides contractual certainty. Draft a list of qualifying events, notice requirements, and the right to suspend or terminate the agreement if the event persists beyond a defined period (e.G., 30 Days).

Governing Law – The legal system that will interpret the contract. For a German-centric technology programme, the governing law is often the German Civil Code (BGB). Including a clause such as “This Agreement shall be governed by and construed in accordance with the laws of the Federal Republic of Germany” provides predictability.

Jurisdiction – The court or tribunal that has authority to hear disputes. In cross-border contracts parties may select a specific German court (e.G., The Berlin Regional Court) or opt for arbitration. A jurisdiction clause might read: “All disputes arising out of or in connection with this Agreement shall be finally settled by the International Chamber of Arbitration (ICC) under its Rules.”

Arbitration – A private dispute-resolution mechanism where an arbitrator, rather than a court, decides the outcome. Arbitration can be faster and more confidential than litigation. Include details on the number of arbitrators, language of proceedings, seat of arbitration, and the applicable rules.

Assignment – The transfer of contractual rights to a third party. In technology contracts, a provider may wish to assign its rights to a parent company, while a customer may seek to assign the contract to a subsidiary. A typical clause restricts assignment without prior written consent, except for transfers in connection with a merger or acquisition.

Novation – The substitution of one party for another, with the consent of all original parties, resulting in a new contract that extinguishes the old one. Novation is useful when a service provider is sold and the new owner wishes to assume the existing contracts. Include a provision stating that any novation requires a written agreement signed by all parties.

Severability – The principle that if one provision is found to be invalid or unenforceable, the remainder of the contract remains in force. A severability clause typically reads: “If any provision of this Agreement is held to be invalid, illegal or unenforceable, the remaining provisions shall continue in full force and effect.”

Entire Agreement – Also known as the integration clause, it declares that the written contract represents the complete and exclusive understanding between the parties, superseding all prior negotiations, drafts, and oral statements. This prevents a party from relying on extrinsic evidence to reinterpret the terms.

Amendment – The process of modifying the contract after it has been executed. An amendment clause should require that any changes be made in writing and signed by authorised representatives of both parties. Verbal modifications are ineffective, which is particularly important in fast-moving technology projects where informal “quick fixes” may be proposed.

Schedule – An annex that contains detailed, often technical, information such as specifications, pricing tables, or service-level metrics. Schedules are incorporated by reference and form part of the contract. Ensure each schedule is clearly labelled (e.G., “Schedule 1 – Technical Specification”) and that any amendment to a schedule follows the amendment procedure.

Annexure – Similar to a schedule, an annexure may contain supplementary documents, such as data-processing agreements, privacy impact assessments, or third-party licences. When referencing annexures, use precise language: “Annexure A – Data Processing Agreement (DPA) attached hereto.”

Definitions – A section that provides precise meanings for key terms used throughout the contract. Defining terms such as “Software,” “Effective Date,” “Confidential Information,” and “Incident” eliminates ambiguity. Example: “‘Software’ means the computer program identified in Schedule 2, including all updates, patches, and related documentation.”

Interpretation – Rules that guide how the contract’s language is understood. In German law, the principle of “contra-proferentem” (interpretation against the drafter) may apply if a clause is ambiguous. Include an interpretation clause that states: “Words importing singular include the plural and vice versa; headings are for convenience only and shall not affect interpretation.”

Representations – Statements of fact made by a party that induce the other party to enter the contract. In technology agreements, representations may cover ownership of IP, compliance with data-protection law, and the absence of pending litigation. Breach of a representation can give rise to a claim for misrepresentation or rescission.

Warranties – Promises that certain facts are true or that certain conditions will be met. Distinguish warranties from representations: Warranties are contractual obligations that, if breached, give rise to a right to damages. Typical software warranties include: “The Software will perform in accordance with the specifications set out in Schedule 1 for a period of twelve (12) months from the Acceptance Date.”

Conditions Precedent – Events that must occur before a party’s performance becomes due. In a development contract, a condition precedent may be the customer’s delivery of source data. Draft the clause to specify the exact nature of the condition, the deadline, and the consequences of non-fulfilment (e.G., Right to terminate).

Performance Obligations – The duties each party must fulfil under the contract. For a technology provider, obligations may include delivering software, providing updates, and maintaining support. For the customer, obligations may include paying fees, providing access to systems, and cooperating with testing. Clearly allocate responsibilities to avoid gaps.

Acceptance – The formal confirmation that the deliverables meet the agreed specifications. Acceptance procedures often involve a written notice stating that the deliverable has been examined and is satisfactory. Include a cure period: “If the Customer objects to any deliverable, it shall notify the Provider within five (5) business days, specifying the deficiencies. The Provider shall have ten (10) business days to cure the deficiencies.”

Change Control – A mechanism for managing modifications to the scope, schedule, or cost of a project. A change-control clause should define how change requests are submitted, evaluated, approved, and documented, and how they affect the price and timeline. Example: “Any change request shall be recorded in a Change Order, signed by both parties, and shall become an amendment to this Agreement.”

Escrow – An arrangement where the source code or other critical assets are deposited with a neutral third party, to be released under specified conditions such as the provider’s bankruptcy. An escrow clause should specify the escrow agent, the trigger events, the verification process, and the rights of the beneficiary.

Data Protection Agreement (DPA) – A contract that governs the processing of personal data on behalf of a data controller, required under the GDPR. The DPA must set out the purpose of processing, the categories of data, security measures, sub-processor approvals, and breach notification obligations. In technology contracts, the DPA is often incorporated as an annex.

GDPR – The General Data Protection Regulation, EU legislation that imposes strict rules on the handling of personal data. Contracts involving EU residents must ensure compliance, including lawful basis for processing, data-subject rights, and cross-border transfer mechanisms. When drafting a SaaS agreement, reference the GDPR and embed the necessary data-protection clauses.

Cross-Border Data Transfer – The movement of personal data outside the European Economic Area. Under the GDPR, such transfers require a lawful mechanism, such as Standard Contractual Clauses (SCCs) or an adequacy decision. Include a clause that states: “Any transfer of Personal Data to a third country shall be subject to the Standard Contractual Clauses approved by the European Commission.”

Standard Contractual Clauses (SCCs) – Model clauses approved by the European Commission to facilitate lawful data transfers. When incorporating SCCs, ensure that the parties are identified correctly (data exporter and data importer) and that the contract reflects the required technical and organisational measures.

Technical and Organisational Measures (TOMs) – Security safeguards required by the GDPR to protect personal data. In a technology contract, specify the TOMs, such as encryption, access control, and incident-response procedures. Example: “The Provider shall implement encryption of data at rest using AES-256 and shall maintain an intrusion-detection system with real-time alerts.”

Breach Notification – The obligation to inform the other party and, where applicable, supervisory authorities of a data breach. Under the GDPR, the controller must notify the authority within 72 hours. A contract clause should set out the timeline, the content of the notice, and the cooperation required for remediation.

Termination – The right to end the contract before its natural expiry. Termination can be for cause (e.G., Material breach) or without cause (e.G., Convenience). A termination-for-cause clause typically requires a cure period: “If either party commits a material breach, the non-breaching party may terminate the Agreement after giving ten (10) days written notice, unless the breach is cured within that period.”

Convenience Termination – The ability of a party to terminate the contract without needing to prove breach. This is common in long-term service agreements where business needs may change. Include appropriate compensation provisions, such as payment for work performed up to the termination date and any pre-paid fees that may be refundable.

Notice – The method and address for delivering formal communications, including termination notices. Specify the acceptable forms (e.G., Registered mail, email with read receipt) and the timeframes for deemed receipt. Example: “All notices shall be deemed received on the third business day after dispatch if sent by registered post, or on the day of transmission if sent by email with confirmation of receipt.”

cure period – The time allowed for a breaching party to remedy a default before the other party can enforce

remedies such as termination. The length of the cure period should be reasonable given the nature of the breach; for a failure to deliver software, a 30-day cure period may be appropriate.

Force Majeure Notice – The requirement to promptly inform the other party of a force-majeure event. Typically, the notice must be given within a specified time (e.G., Five days) and must detail the expected impact and duration. Failure to provide timely notice may result in loss of the force-majeure defence.

Risk Allocation – The distribution of potential losses between the parties. In technology contracts, risk allocation is often achieved through indemnities, limitation of liability, and insurance requirements. Identify the principal risks (e.G., IP infringement, data breach, service outage) and allocate them to the party best able to manage them.

Insurance – The procurement of policies to cover certain liabilities. Common policies in technology contracts include professional indemnity, cyber-risk insurance, and product liability. An insurance clause may require the provider to maintain a minimum level of coverage (e.G., €1 Million per claim) and to furnish certificates of insurance upon request.

Third-Party Rights – The ability of persons who are not parties to the contract to enforce its terms. Under German law, a contract may expressly confer rights on a third party, but this is rare in technology agreements. More often, parties will include a clause stating that no third-party may rely on the contract, thereby limiting external claims.

Subcontractor – A party engaged by the primary contractor to perform part of the work. In software development, subcontractors may be used for specialised components. Include a clause that requires the primary contractor to obtain the customer's consent before engaging subcontractors, and that the subcontractor must comply with all obligations of the main contract.

Compliance – The requirement to adhere to applicable laws, regulations, and standards. In technology contracts, compliance may cover data-protection law, export controls, industry-specific regulations (e.G., Medical-device standards), and accessibility requirements. Draft a compliance clause that obliges each party to maintain all necessary licences and to conduct the work in accordance with relevant statutes.

Export Control – Legal restrictions on the transfer of technology, software, or technical data across national borders. German export-control law (AUSTRV) and EU regulations may prohibit the export of encryption software to certain destinations. Include a representation that the provider holds all required export licences and will not ship restricted technology to prohibited jurisdictions.

Audit Rights – The ability of one party to inspect the other's compliance with contractual obligations, especially regarding data protection and security. An audit clause may grant the customer the right to perform on-site or remote audits, subject to reasonable notice and confidentiality protections.

Business Continuity – Plans and measures to ensure the continuation of services in the event of disruption. Include a clause that requires the provider to maintain a business-continuity plan, to test it regularly, and to provide the customer with a summary of the plan upon request.

Backup and Recovery – The processes for copying data and restoring it after loss. In SaaS contracts, the provider typically bears responsibility for regular backups. Specify the frequency (e.G., Daily incremental, weekly full), the retention period, and the recovery time objective (RTO).

Performance Metrics – Quantitative indicators used to assess whether the provider meets its obligations. Common metrics include latency, transaction throughput, error rate, and system availability. Define each metric, the measurement method, and the penalties for non-compliance.

Penalty Clause – A provision that imposes a predetermined sum for failure to meet a performance metric. Penalties are often expressed as service credits (e.G., A credit of 5 % of the monthly fee for each hour of downtime beyond the SLA). Ensure that penalties are enforceable under German law, which may limit punitive damages.

Escalation Procedure – A step-by-step process for handling unresolved issues, typically moving from operational support to senior management. Include contact details for each escalation level and the timeframes for response at each stage.

Intellectual Property Assignment – The transfer of ownership of IP from one party to another. In custom software development, the client often expects an assignment of all copyrights in the deliverables. Draft a clear assignment clause: “Upon full payment, the Provider hereby assigns to the Customer all present and future rights, title, and interest in the Work Product, including all related copyrights and patents.”

Work Product – The output created under the contract, such as code, designs, documentation, and test results. Define whether the work product is a “work made for hire” (in jurisdictions that recognise the concept) or whether it is subject to an assignment. In Germany, the default rule is that the creator retains copyright unless an assignment is made.

Moral Rights – Rights of the author to be identified as the creator and to object to derogatory treatment of the work. German law provides strong moral rights that cannot be waived, only waived by agreement. Include a clause where the author waives the right to be identified if the client wishes anonymity, but recognise that moral rights may still survive.

Non-Compete – A restriction that prevents a party from engaging in competing activities for a defined period and geographic area. In technology agreements, a non-compete may be imposed on the contractor to protect the client’s proprietary processes. Ensure the restriction is reasonable in scope, duration, and geography to be enforceable under German competition law.

Non-Solicitation – A clause that forbids one party from poaching the other’s employees or contractors. Typical language: “During the term and for twelve (12) months thereafter, neither party shall directly or indirectly solicit any employee of the other party.”

Retention Bonus – A financial incentive to keep key personnel on a project. While not a contract term per se, the inclusion of a retention bonus in the remuneration schedule can be linked to milestone completion, reinforcing performance.

Intellectual Property Warranty – A promise that the software does not infringe third-party rights. The warranty may be limited to a specific period (e.G., Twelve months) and may be subject to the provider's obligation to indemnify and defend the customer against infringement claims.

Data Ownership – The designation of who owns the data uploaded or generated by the service. In a SaaS contract, the customer typically retains ownership of its data, while the provider may claim a limited licence to use the data for service provision, analytics, and improvement. Clarify the licence scope and any restrictions on data use.

Data Retention – The period for which the provider may store the customer's data after termination. Include a clause that specifies the provider will delete or return the data within a defined timeframe (e.G., Thirty days) and certify the destruction.

Data Portability – The right of the customer to obtain its data in a structured, commonly used format and to transfer it to another service. Under the GDPR, data portability is a statutory right, and contracts should reflect the provider's commitment to facilitate it.

Data Residency – The location where data is stored. Some customers require that data remain within the EU or within a specific country for compliance reasons. Include a clause specifying the data centre locations and any restrictions on moving data to other jurisdictions.

Security Incident – An event that compromises the confidentiality, integrity, or availability of data. The contract should define what constitutes an incident, the provider's duty to report, and the remedial actions required. Example: "A Security Incident shall be any actual or suspected breach of the Provider's security measures that results in unauthorized access to Personal Data."

Patch Management – The process of applying updates to software to fix vulnerabilities. In a maintenance agreement, specify the frequency of patches, the testing procedures, and the communication protocol to the customer.

Upgrade – The provision of newer versions of the software that may include additional features or improvements. Distinguish between "minor upgrades" (bug fixes) and "major upgrades" (new functionality) and state whether upgrades are included in the subscription fee or subject to additional charges.

Support Services – Assistance provided to the customer for troubleshooting, configuration, and usage questions. Define the support hours (e.G., 9 Am-5 pm CET, Monday-Friday), the channels (phone, email, ticketing system), and the response and resolution times.

Training – Instruction provided to the customer's staff on how to use the software. If training is part of the contract, outline the format (on-site, remote, self-paced), the number of participants, and any additional fees for extra sessions.

Change of Control – An event where a party undergoes a significant ownership shift, such as a merger or acquisition. Contracts often contain a clause that allows the other party to terminate or renegotiate upon a change of control, to protect against unknown risk.

Force Majeure Event – An example list includes natural disasters, terrorist acts, wars, strikes, epidemics, or governmental actions that prevent performance. Specify that the affected party must mitigate the impact where possible and provide evidence of the event's effect on performance.

Compliance Audit – A systematic examination to verify adherence to contractual obligations, especially those concerning data protection and security. The audit clause should state the audit's scope, the auditor's qualifications, and the confidentiality obligations of audit findings.

Data Processor – The party that processes personal data on behalf of the data controller. In a cloud-service arrangement, the provider is typically the processor, while the customer is the controller. The DPA must articulate the processor's duties, such as acting only on documented instructions and implementing appropriate security measures.

Data Controller – The entity that determines the purposes and means of processing personal data. The controller bears the ultimate responsibility for GDPR compliance. In a SaaS contract, the customer is usually the controller, and the clause should require the provider to act solely under the controller's instructions.

Sub-Processor – A third party engaged by the processor to carry out specific processing activities. The contract must require the processor to obtain the controller's prior written consent before engaging any sub-processor, and to flow down the same data-protection obligations.

Data Breach – A security incident that leads to the accidental or unlawful destruction, loss, alteration, or disclosure of personal data. The contract should obligate the processor to notify the controller without undue delay, provide a detailed report, and cooperate in remediation.

Incident Response Plan – A documented set of procedures for handling security incidents. The provider should maintain and periodically test an incident-response plan, and the contract may require the provider to share the plan with the customer upon request.

Business Impact Analysis (BIA) – An assessment that determines the effects of a disruption on business operations. While not always contractually mandated, a BIA can be a prerequisite for a robust business-continuity clause, especially for critical-infrastructure services.

Redundancy – The duplication of critical components or functions to increase reliability. In cloud contracts, redundancy may be achieved through multi-region deployment. Specify the level of redundancy (e.G., "N+1") and the impact on service availability.

Performance Bond – A guarantee, usually issued by a bank, that the contractor will fulfill its obligations. If the contractor fails, the bond can be drawn upon by the client. Performance bonds are less common in technology contracts but may be used for large-scale system-integration projects.

Retention of Records – The obligation to keep certain documentation for a prescribed period. In technology contracts, records of system logs, audit trails, and change logs may need to be retained for compliance purposes (e.G., Six years under German tax law).

Conflicts of Interest – Situations where a party's personal interests could interfere with its obligations. Include a representation that each party has disclosed any conflicts that could affect the performance of the contract.

Entire Agreement Clause – As noted earlier, this clause confirms that the written contract supersedes all prior discussions. It prevents parties from introducing extrinsic evidence to interpret ambiguous terms, reinforcing the importance of precise drafting.

Governing Law Clause – The selection of German law as the governing law provides predictability for parties operating in Germany. It also ensures that any disputes are resolved in accordance with the BGB, the German Commercial Code (HGB), and relevant statutes such as the GDPR and the UrhG.

Jurisdiction Clause – Choosing a specific court (e.G., The Frankfurt District Court) or an arbitration institution (e.G., The ICC) determines where disputes will be resolved. In cross-border technology contracts, many parties prefer arbitration to avoid national court bias.

Arbitration Rules – If arbitration is selected, reference the specific set of rules (e.G., ICC Rules 2021). State the number of arbitrators (usually one or three), the language of the proceedings (often English), and the seat of arbitration (e.G., Berlin).

Confidentiality Exceptions – While confidentiality is generally absolute, exceptions may be carved out for information that is already public, independently developed, or required by law. Define these exceptions narrowly to preserve the protective intent of the confidentiality clause.

Public Domain – Information that is generally available to the public without restriction. A confidentiality clause may state that the obligation does not apply to information that becomes part of the public domain through no fault of the receiving party.

Independent Development – Information that a party independently creates without reference to the other party's confidential material. Include a carve-out that protects the receiving party if it can demonstrate such independent development, typically by maintaining contemporaneous documentation.

Legal Compliance Clause – A broad clause obligating each party to comply with all applicable laws, regulations, and standards. This includes, but is not limited to, data-protection law, export controls, anti-corruption statutes, and industry-specific regulations.

Anti-Corruption – A representation that each party will not engage in bribery or other corrupt practices. Incorporate a reference to the German Criminal Code (StGB) and the UK Bribery Act if the contract involves multinational parties.

Export Control Clause – The obligation to obtain necessary licences before exporting controlled technology. Example wording: "The Provider shall not export, re-export, or otherwise transfer any software, technical data, or related services to any prohibited destination without first obtaining all required export licences."

Data Sovereignty – The concept that data is subject to the laws of the country in which it is stored. For

customers with strict regulatory requirements, a data-sovereignty clause may require that all data be stored within a specific jurisdiction, such as Germany.

Data Localization – A specific form of data sovereignty where data must remain on servers physically located within a particular country. Include a clause that obliges the provider to host the data exclusively in German data centres and to certify the location upon request.

Business Continuity Plan (BCP) – A documented strategy to maintain essential functions during a disruption. The contract may require the provider to maintain a BCP, to test it annually, and to provide the customer with a summary of the plan and test results.

Disaster Recovery (DR) – The set of procedures to restore systems after a catastrophic event. A DR clause should define recovery time objectives (RTO) and recovery point objectives (RPO), and specify the responsibilities of each party in the event of a disaster.

Escalation Matrix – A table that lists contact persons, their roles, and escalation levels. Include this matrix as an annex to ensure that both parties know who to contact for technical, contractual, or executive issues.

Service Credits – Monetary or non-monetary compensation provided when the provider fails to meet SLA metrics. Service credits are often calculated as a percentage of the monthly fee for each hour of downtime beyond the SLA threshold.

Penalty – A predetermined sum payable for non-performance, distinct from damages.