SAKIZLI FIVE-PHASE CONSULTING MODEL

Below, I present the "Sakizli Five-Phase Consulting Model", a five-phase consulting model that builds seamlessly on the existing "Sakizli Model", which addresses ethical questions and Governance principles in detail. The Five-Phase Consulting Model extends this foundation to contractual, legal, and regulatory questions arising from the use of AI. It gives AI consultants a practical framework for addressing these challenges systematically and through an interdisciplinary approach. By integrating with the Sakizli Model, it keeps ethics and Governance in view while placing a strong emphasis on the applicable legal framework. This integrated approach helps organizations reduce legal risk and make responsible use of the opportunities created by a rapidly evolving AI environment.

Phase 1: Preparation and Intake Assessment

Clarification of objectives:

- Define contractual and regulatory objectives: Clearly define the legal and contractual objectives, e.g. ensuring Compliance, liability protection or data protection optimisation.

Information collection:

- Technological context: Analysis of the AI technologies, infrastructure and interfaces used.
- Existing contracts: Review of current agreements, licensing agreements and cooperation agreements.
- Relevant laws and standards: Identification of national and international legislation, industry-specific standards and regulatory requirements (e.g. General Data Protection Regulation, product liability).

Define framework conditions:

- Project planning: Setting timelines, milestones, and resources.
- Stakeholder analysis: Identification of all internal and external actors (legal experts, technologists, Compliance officers, etc.).

Phase 2: Analysis and problem definition

Needs analysis:

- Identification of key challenges: Uncovering gaps in existing contractual regulations and legal uncertainties.
- Topics: data protection, liability issues, intellectual property and regulatory Compliance.

Risk and opportunity assessment:

- SWOT analysis:
  - Strengths: Existing Compliance mechanisms, proven internal processes.
  - Weaknesses: Lack of legal clarity in existing contracts, inadequate adaptation to new technological developments.
  - Opportunities: Optimization potential through new contractual regulations, proactive integration of current regulatory developments.
  - Risks: Data breaches, liability risks, or delays due to unclear responsibilities.

Prioritization:

- Urgency assessment: Ranking the identified issues according to their relevance and influence on overall success to ensure a focused consulting process.

Phase 3: Consulting and Solution Development

Development of concrete proposals for solutions:

- Tailor-made contract drafting: Development of specific regulations that address liability issues, data protection requirements and Compliance guidelines.
- Risk mitigation measures: Formulation of strategies to minimize identified legal and regulatory risks.

Integration of best practices:

- Best Practice methods: Adoption and adaptation of proven procedures from the existing Sakizli Model, supplemented by legal checklists and Compliance frameworks.
- Consultative approach: use of interactive workshops and case studies to develop practical and sustainable solutions.

Interdisciplinary cooperation:

- Expert network: Involvement of lawyers, technologists, data protection officers and other specialist areas in the advisory process to ensure a holistic view.

Phase 4: Implementation and documentation

Action plan:

- Step-by-step planning: Creation of a detailed implementation plan with clearly assigned responsibilities, deadlines and resource allocation.
- Implementation steps: Definition of concrete tasks, from contract revision to the introduction of new Compliance processes.

Documentation:

- Report preparation:

Summary of all developed contractual regulations, legal recommendations and measures in a comprehensive report or presentation.

- Evidence: Archiving relevant decisions, risk assessments and communication strategies as a reference for future Audits.

Communication strategy:

- Transparency: Determine how the results are communicated internally (e.g. in workshops, trainings) and externally (e.g. in partner meetings or public statements) in order to strengthen the trust of stakeholders.

Phase 5: Evaluation and follow-up

Feedback and Review:

- Evaluation cycles: Implementation of regular feedback loops and reviews to monitor the effectiveness of the measures and identify the need for adaptation at an early stage.

Customization:

- Dynamic updating: Ongoing adaptation of the model to changing technological, legal or regulatory frameworks.
- Lessons Learned: Documentation of experiences and success factors for continuous improvement.

Long-term support:

- Follow-up meetings: Planning regular monitoring and optimization meetings to ensure sustainable ongoing Compliance and proactively address new challenges.
- Monitoring: Establishment of KPIs and metrics to measure the success of the implemented measures.

The Sakizli Five-Phase Consulting Model in Detail

Phase 1: Preparation and Intake Assessment - Detailed Explanation

This first phase lays the foundation for the entire advisory model by systematically capturing all relevant legal perspectives and comprehensively analyzing the context in which the AI applications operate. In the following, the central elements of this phase are explained, with a special focus on legal issues and applicable directives and laws.

1. Clarification of objectives

Definition of contractual and regulatory objectives:

- Compliance and liability: Determining which Compliance goals (e.g. GDPR, EU AI Act) are to be achieved in order to minimize liability risks.
- Ensuring legal compliance: Identification of which laws and guidelines (e.g. eIDAS, DSA, DMA) are relevant for the planned use of AI and in which areas (media law, criminal law, commercial law, etc.) there are special requirements.
- Protection of sensitive information: Determination of objectives regarding the protection of trade secrets, copyrights and data protection.
- Human rights and ethical principles: Alignment of legal objectives with human rights standards and ethical guidelines, for example to avoid discrimination or invasions of privacy.

2. Information collection

A. Technological context and business environment

- Technology and systems analysis: Recording of the AI technologies, algorithms, data sources and interfaces used that are relevant to specific areas of law (e.g. algorithmic decisions and their transparency in the light of the EU AI Act).
- Company-specific circumstances: Consideration of internal regulations, previous contracts and internal data protection concepts, which serve as a starting point for further adjustments.

B. Relevant legal frameworks and standards

- European legislation:
  - EU AI Act: Analysis of the requirements for transparency, risk assessment and liability issues that apply to the use of AI.
  - GDPR (General Data Protection Regulation): Review of data protection principles, rights of data subjects and data processing processes.
  - DSA (Digital Services Act) and DMA (Digital Markets Act): Examination of obligations in dealing with online platforms, algorithmic decision-making and competitive aspects.
  - eIDAS (Electronic Identification, Authentication and Trust Services): Assessment of electronic trust services and their legal requirements.
- National legislation and specific areas of law:
  - Copyright and media law: Examination of how copyright protection regulations as well as media law provisions (e.g. press law) influence the use of AI.
  - Criminal law aspects: Analysis of potential criminal law risks (e.g. misuse of AI systems or undue invasion of privacy).
  - Commercial law and contract law: Examination of commercial law frameworks that must be defined in contracts with service providers or partners.
  - Liability issues: Determination of how liability regulations (e.g. product liability, tortious liability) must be designed with regard to AI applications.
- Industry-specific standards and certifications: Collection of relevant industry standards, such as ISO standards or specific industry certificates, which can be used in addition to legal requirements.

C. Collection of internal and external documents:

- Existing contracts and policies: Analysis of existing contracts, data protection policies, Compliance regulations and internal procedural documents.

- External opinions and guidelines: Inclusion of studies, regulatory guidelines (e.g. from data protection authorities or European institutions) and Best Practice examples that contribute to the assessment of the legal situation.

3. Define framework conditions

A. Project Organization and Stakeholder Identification:

- Internal actors: Definition of the roles of legal departments, Compliance officers, IT security experts and specialist departments.
- External experts: Involvement of specialized lawyers, data protection experts, industry consultants and, if necessary, government regulators.
- Collaboration and communication: Defining communication channels and regular coordination processes to ensure interdisciplinary collaboration.

B. Timelines, Resources and Budget:

- Project period: Detailed timeline for information collection, analysis and subsequent implementation of the measures, including milestones to verify compliance with legal requirements.
- Resource allocation: Allocation of human and financial resources to ensure extensive legal reviews (e.g. external opinions on GDPR compliance).

C. Risk management and legal protection:

- Early risk identification: Implementation of mechanisms to identify potential legal stumbling blocks, such as liability issues or data protection violations.
- Preparation of a catalogue of measures: Definition of immediate measures and emergency plans in the event that critical legal gaps are identified as part of the analysis.

D. Documentation and reporting:

- Transparent collection: Complete documentation of all collected information, analyses and identified legal issues, including cross-references to specific laws and directives (e.g. specific articles of the GDPR, sections of the EU AI Act etc.).
- Reporting structures: Development of a structured reporting system that makes it possible to present the legal status quo and all identified challenges in a comprehensible manner - both internally and vis-à-vis external audit bodies.

Summary Phase 1 of the "Sakizli Legal Model" will create a sound starting point that covers all relevant legal dimensions in the context of AI applications. From the clarification of objectives to the detailed collection and analysis of technical, contractual and legal framework conditions to the definition of clear project and communication structures, all aspects - from copyright and media law to EU directives to liability issues and data protection - are systematically taken into account. This comprehensive preparation forms the basis for successful interdisciplinary consulting and the development of tailor-made legal and contractual measures based on it.

Phase 2: Analysis and problem definition - Detailed Explanation

In this phase, the foundation is laid for the later development of the solution. It is important to systematically identify the current status quo, the existing challenges and risks, and the existing opportunities. In doing so, particular care is taken to comprehensively analyze all relevant legal perspectives - from data protection to liability issues to specific regulatory requirements.

1. Needs analysis

Targeted recording of the initial situation:

- Legal gaps and challenges:
  - Review of existing contracts and internal policies regarding data protection (GDPR, eIDAS) and Compliance with regulatory requirements such as the EU AI Act, DSA and DMA.
  - Analysis of the extent to which copyright and media law provisions (e.g. copyright, press law) are currently taken into account or require adjustments in the future.
  - Identification of criminal law risks that may arise, for example, from the misuse of AI systems.
  - Identification of uncertainties in liability regimes, especially in the context of product liability and tortious liability in AI-based decisions.

- Internal and external influencing factors:
  - Mapping the technological environment and the AI algorithms used that have an impact on the legal assessment (e.g. transparency requirements in the EU AI Act).
  - Collection of existing internal documents, such as Compliance policies, data protection concepts, trade secret protection and previous Audit results.
  - Consideration of external expert opinions, guidelines and industry-specific standards (e.g. ISO standards) that serve as a benchmark for legal requirements.
- Stakeholder perspectives:
  - Inclusion of feedback and experience from the legal, Compliance, IT security and other relevant departments.
  - Coordination with external experts such as specialized lawyers and data protection consultants to ensure an objective inventory.

2. Risk and opportunity assessment

Conducting a comprehensive SWOT analysis:

- Strengths:
  - Existing Compliance measures and established processes in the areas of data protection and contract management.
  - Already integrated Best Practice standards and documented success stories in interdisciplinary collaboration.
- Weaknesses:
  - Potential gaps in existing contracts, especially with regard to liability issues and unclear responsibilities in the event of data breaches.
  - Insufficient adaptation of internal processes to new regulatory requirements, e.g. due to the EU AI Act or the new provisions from DSA and DMA.
  - Lack of transparency and documentation regarding trade secrets and the protection of intellectual property (copyright).
- Opportunities:
  - Optimization potential through the introduction of innovative contract models that explicitly address liability issues and data protection risks.
  - Competitive advantage by proactively adapting to current and upcoming regulatory requirements, which strengthens the trust of partners and customers.
  - Opportunity to consolidate one's own position in the market through certifications and industry-specific standards (e.g. ISO certifications).
- Threats:
  - High financial and reputational risks in the event of non-compliance with data protection regulations (GDPR) or disregard of the EU AI Act, which can lead to significant fines.
  - Criminal consequences for inadequate protection against misuse of AI systems or violations of human rights.
  - Unforeseen liability risks resulting from unclear contractual regulations and lack of protection in the area of commercial and contract law.
  - Potential conflicts with external partners or regulators when trade secrets or intellectual property are not adequately protected.

Specific legal assessments:

- Data protection and eIDAS: Assessment of the risks of improper data processing, possible violations of data subject rights and the requirements for electronic trust services.
- EU AI Act: Analysis of transparency requirements, risk classifications and liability regimes developed specifically for AI applications.
- DSA, DMA and media law: Examination of the requirements for digital services, competition regulations and media law requirements in order to avoid inadmissible practices.
- Contract and commercial law: Review of existing contracts for gaps in liability regulations and how to deal with unexpected risks in the trading context.

3. Prioritization

Systematic assessment of the identified challenges:

- Urgency matrix:
  - Creation of a matrix in which risks and opportunities are assessed according to their impact (high, medium, low) and probability of occurrence.
  - Critical areas (e.g., data breaches, liability issues) are prioritized to initiate immediate action.
- Assessment Metrics:
  - Develop quantitative and qualitative criteria that take into account, for example, potential fines, reputational damage, and legal consequences.
  - Integration of Stakeholder priorities to ensure that the most pressing issues - such as insufficient Compliance in the area of GDPR or EU AI Act - are at the top of the list.
- Interdisciplinary validation:
  - Regular coordination meetings with internal and external experts to validate and adjust priorities together.
  - Document and communicate priorities in a clear report that serves as the basis for solution development in Phase 3.

4.

Summary and documentation of the analysis

Preparation of a detailed analysis report:

- Structured presentation:
  -

Summary of all identified challenges, gaps and opportunities, each with reference to the relevant areas of law (GDPR, EU AI Act, copyright, liability law, etc.).

  - Detailed presentation of the SWOT analysis including specific points identified for each area of law.
- Documentation of prioritization:
  - Clear list of prioritized risks and opportunities, which serves as a basis for further measures.
  - Integration of charts and tables to visualize the urgency and potential impact of individual risks.
- Establishment of a Monitoring mechanism:
  - Develop a continuous monitoring system that ensures that changes in the legal, technological or regulatory landscape can be detected early and incorporated into future analyses. Conclusion on phase 2 The detailed analysis and problem definition phase creates a sound basis on which the later solution approaches are based. The systematic needs analysis, the differentiated risk and opportunity assessment and the clear prioritization of all identified challenges - with a special focus on all legal aspects such as data protection, liability, EU directives and other specific areas of law - ensure that no relevant legal perspective is ignored. This enables a targeted and interdisciplinary approach in the further phases of the "Sakizli Legal Model".

Phase 3: Consulting and Solution Development - Detailed Elaboration

In this phase, the foundation is laid for concrete, practical measures. The aim is to develop tailor-made solutions that address all identified legal challenges and are embedded in the interdisciplinary advisory process. Both innovative contract models and proven Compliance methods are incorporated.

1. Development of concrete proposals for solutions

A. Tailor-made contract drafting and legal regulations:

- Contractual clauses:
  - Liability clauses: Development of precise liability regimes that cover both product liability and tortious liability aspects. These clauses are intended to define clear responsibilities and include mechanisms for risk mitigation.
  - Data protection and Compliance: Integration of specific clauses for compliance with the GDPR, eIDAS and EU AI Act, such as regulations on data processing, rights of data subjects and reporting obligations in the event of data breaches.

- Intellectual property and trade secrets: Development of regulations for the protection of copyrights, media rights and internal trade secrets in order to avoid unwanted disclosures and competitive disadvantages.

- Regulatory coordination:
  - Review and integration of the latest regulatory requirements (e.g. DSA, DMA) into the contractual agreements.
  - Alignment of internal regulations with external guidance and expert opinions to ensure that all regulatory changes and industry-specific standards are taken into account.

B. Development of risk mitigation measures:

- Risk management Framework:
  - Establishment of a detailed risk management process that systematically records and evaluates legal risks (e.g. data protection violations, liability uncertainties) in particular.
  - Develop contingency and escalation plans in the event of unexpected legal challenges or regulatory changes.
- Specific recommendations for action:
  - Preparation of recommendations for action on how to deal with identified vulnerabilities, for example through additional training, the introduction of new internal control mechanisms or the use of technical measures to increase data security.

2. Integration of best practices

A. Best Practice methods and Standards:

- Guidelines and checklists:
  - Use of standardized checklists that cover all relevant areas of law - from data protection (GDPR) and EU AI Act to copyright and media law.
  - Use Best Practice documentation to ensure that innovative contract models and Compliance mechanisms meet the latest standards.
- Certifications and standards:
  - Integration of internationally recognized certifications (e.g. ISO standards, IT security standards) to ensure technical and legal security.
  - Reference to industry-specific certifications, which can also be anchored in contracts and internal processes as proof of quality.

B. Methodological approach:

- Workshops and case studies:
  - Conducting interactive workshops in which case studies from practice are analysed and concrete solutions are developed.
  - Use scenario analysis to determine how specific legal challenges (e.g., liability cases or data breaches) may play out in different settings.
- Benchmarking:
  - Compare internal procedures with industry standards and competitive practices to identify and exploit areas for improvement.

3. Interdisciplinary cooperation

A. Involvement of different expert groups:

- Legal experts and data protection officers:
  - Continuous coordination with internal lawyers as well as external specialized lawyers in order to address all legal issues - from copyright to criminal law - in a well-founded manner.
  - Involvement of data protection officers to ensure that all regulations are GDPR-compliant and forward-looking.
- Technological and operational experts:
  - Collaborate with IT security experts and technologists to assess and optimize the technical implications of the legal measures (e.g., in data storage and processing).
  - Involvement of operational and management representatives to ensure that the solutions developed are also operationally feasible and economically viable.

B. Interdisciplinary communication and coordination processes:

- Regular coordination meetings:
  - Establish regular exchanges between the different disciplines to continuously update information and discuss adjustments in real time.
  - Use of modern collaboration tools to collect documents, analyses and feedback centrally and make them transparent.
- Common goal definition:
  - Formulation of an integrated target image that takes into account legal, technical and operational requirements in order to align the overall strategy of AI use.
  - Determination of KPIs (Key Performance Indicators) and success criteria that make the progress in the implementation of the developed solutions measurable. Conclusion on Phase 3 In the consulting and solution development phase, concrete, practical measures are developed that meet the legal, contractual and regulatory requirements for the use of AI. Through the targeted creation of tailor-made contractual clauses, the implementation of a robust risk management Framework as well as the integration of proven Best Practice methodologies and intensive interdisciplinary cooperation, it is ensured that all identified challenges - from data protection to liability issues to specific EU directives - are addressed comprehensively and sustainably. This procedure forms the basis for the successful implementation and subsequent evaluation of the implemented measures in the further phases of the "Sakizli Legal Model".

Phase 4: Implementation and documentation - Detailed Explanation

In this phase, the previously developed strategy is translated into concrete, implementable measures. In addition to the implementation of the legal and contractual regulations that have been developed, complete documentation and transparent communication are key. All steps are systematically planned, executed and recorded in a comprehensible manner.

1. Action plan

A. Step-by-step implementation:

- Detailed planning:
  - Create an action plan: Structure the individual measures (e.g. contract revision, introduction of new data protection processes, implementation of liability regulations) into clearly defined work packages.
  - Assign responsibilities: Determine which internal departments (e.g., legal, IT, Compliance) or external partners (e.g., specialized lawyers, privacy experts) are responsible for implementation.
  - Time milestones: Define concrete deadlines and intermediate goals in order to be able to continuously monitor progress.
- Risk management and escalation plans:
  - Risk identification: Detailed recording of potential implementation risks, for example with regard to technical integrations or legal uncertainties (e.g. due to changes in the EU AI Act or the GDPR).
  - Contingency strategies: Develop escalation and contingency plans that take effect in the event of Compliance violations or delays.
  - Continuous monitoring: Implementation of a Monitoring system that reacts early to deviations and allows for adjustments.

B. Resource and budget planning:

- Resource allocation:
  - Detailed list of the required human, financial and technical resources.
  - Coordination with the respective stakeholders to identify and eliminate bottlenecks at an early stage.
- Budgeting:
  - Establish a budget for implementation, including external consulting services, technical implementations, and training.

2. Documentation

A. Comprehensive coverage of all measures:

- Project documentation:
  - Creation of a central project Dashboard that documents all relevant data, progress and decisions.
  - Minutes of meetings, decisions and important coordination with internal and external partners.
- Legal traceability:
  - Detailed documentation of all adjustments in contracts and internal policies with reference to relevant laws and standards (e.g. articles of the GDPR, sections of the EU AI Act).
  - Archive risk analyses, Audit results, and evaluation reports for reference for future Compliance audits.

B. Reporting structures:

- Internal reports:
  - Regular status reports to management that provide information on progress, identified challenges and need for adjustment.
  - Establishment of a reporting system that ensures transparent follow-up of the implemented measures.
- External communication:
  - Documentation of the results in a final implementation report, which also serves as proof to regulators or partners.

3. Communication strategy

A. Internal communication:

- Ensuring the flow of information:
  - Setting up regular meetings and updates (e.g. in the form of workshops or digital platforms) to continuously inform all stakeholders involved.
  - Use of internal communication channels (intranet, newsletter, internal training) to disseminate information about changes and progress.
- Training and awareness-raising:
  - Conducting targeted training and workshops to educate employees about new legal regulations, data protection requirements and liability regulations.
  - Creation of guides and FAQ documents that make it easier to deal with the new processes.

B. External communication:

- Transparent display:
  - Publication of information on the measures taken, for example in the form of press releases, Whitepapers or public reports.
  - Coordination with external partners and regulators to increase confidence in the measures taken.
- Stakeholder dialogue:
  - Establishment of feedback mechanisms (e.g. stakeholder roundtables, surveys) to incorporate external feedback into the ongoing optimization of processes.

Conclusion

Phase 4 of the "Sakizli Legal Model" ensures that the developed legal, contractual

and regulatory measures. A detailed action plan, transparent and comprehensive documentation and a clear communication strategy not only control the implementation and make it comprehensible, but also strengthen the trust of internal and external Stakeholder. This approach forms the basis for a sustainable implementation and subsequent evaluation of the measures taken in order to always meet the requirements in a dynamic legal environment.

Phase 5: Evaluation and follow-up - Detailed Explanation

In this final phase, it is ensured that the implemented measures have a sustainable effect and are continuously adapted to changing legal, regulatory and technological frameworks. A systematic process for evaluation and continuous improvement will be established that takes into account all relevant legal perspectives (e.g. GDPR, EU AI Act, copyright, liability law, etc.).

1. Feedback and Review

A. Establishment of regular evaluation cycles:

- Fixed inspection intervals:
  - Implementation of quarterly or bi-annual reviews to monitor the effectiveness of the new contractual arrangements and Compliance measures.
  - Define specific KPIs (e.g., number of data protection incidents, contractual clause update rate, Audit results) to measure success.

B. Integration of internal and external Stakeholder:

- Internal Reviews:
  - Regular meetings with the legal department, Compliance managers, IT security and other relevant departments to discuss the current challenges and potential for improvement.
  - Conducting internal Audits to verify compliance with legal requirements (e.g., GDPR, EU AI Act).
- External expert opinions and Audits:
  - Cooperation with external experts (e.g. data protection officers, specialised lawyers) for the objective assessment of the measures taken.
  - Use of external Audits to validate internal evaluation and identify optimization opportunities.

C. Documentation and communication of the results:

- Preparation of detailed evaluation reports:
  - Complete documentation of all feedback, Audit results and identified areas for improvement.
  - Ensure that these reports are archived in an audit-proof manner and kept available for future Compliance audits.
- Transparent communication:
  - Regular internal reports to management as well as information exchange with relevant external stakeholders (e.g. regulatory authorities).

2. Customization and continuous optimization

A. Dynamic updating of the model:

- Responsiveness to legal changes:
  - Ongoing monitoring of the legal situation and regulatory developments (e.g. changes in the GDPR, updates to the EU AI Act or new requirements from

DSA/DMA).

- Immediately incorporate legislative changes into the model to stay up-to-date.

- Adaptation of internal processes:
  - Revision and optimization of contracts and internal policies based on the evaluation results.
  - Conduct workshops and training to inform all affected employees about new processes and legal requirements.

B. Implementation of Lessons Learned:

- Recording of empirical values:
  - Systematic analysis of the evaluation reports to identify recurring challenges and successful measures.
  - Integration of these findings into future adjustments to the model.
- Optimization of risk management strategies:
  - Adapt contingency plans and escalation strategies to respond more quickly and effectively to newly identified risks (e.g., liability or data protection incidents).

3. Long-term support and Monitoring

A. Establishment of a continuous Monitoring system:

- Real-time monitoring:
  - Development of a Dashboard for continuous monitoring of relevant KPIs and regulatory changes.
  - Use Monitoring tools to provide early warning of potential Compliance violations or regulatory adaptation needs.

B. Regular Follow-up appointments:

- Planning and conducting control meetings:
  - Regular meetings with interdisciplinary teams to check the long-term effectiveness of the implemented measures.
  - Establish responsibilities to ensure continuous compliance with legal requirements.

C. Sustainable integration into the company:

- Long-term support:
  - Establishment of a permanent Compliance management system that continuously adapts to new challenges and carries out regular updates.
  - Ensuring that the model is integrated into the corporate strategy and anchored in operations for the long term.

4. Documentation and reporting

A. Archiving and revision security:

- Comprehensive documentation:
  - All evaluation reports, adaptation measures and training documents are archived in an audit-proof manner and are available for internal and external audits.
- Preparation of a final report per cycle:
  -

Summary of all results and adjustments, which serves as a reference for future evaluation cycles.

B. Communication to Stakeholder:

- Internal reporting:
  - Regular internal updates and reports to management to ensure transparency on the progress and effectiveness of the measures.
- External reports:
  - Publish results and adjustments as needed to increase the trust of external partners and regulators.

Conclusion

Phase 5 of the "Sakizli Legal Model" ensures the sustainable effectiveness of the implemented

measures through a structured and continuous evaluation and adaptation process. Regular feedback, systematic reviews, dynamic adjustments and long-term support ensure that all legal, contractual and regulatory requirements are complied with, even in the changing environment. This enables the company to react proactively to changes, identify risks at an early stage and secure the trust of stakeholders in the long term.

Application example:

Scenario: Consultation for a RunwyML-based AI solution with Instagram integration

Initial situation:

Your client plans to use an AI solution to optimize their social media strategy for Instagram. The solution is intended to use RunwyML to perform data-based analyses - for example, for target group addressing, content optimization and trend forecasting. At the same time, there are high requirements in terms of data protection, liability, copyright and regulatory Compliance (e.g. GDPR, EU AI Act).

Phase 1: Preparation and Intake Assessment

1. Clarification of objectives:

- Define contractual and regulatory goals: Together with the customer, you clarify which legal framework conditions (e.g. data protection, liability issues, use of platform APIs) must be observed in the project.
- Specific objectives: The customer wants to ensure that the AI solution is not only technically efficient, but also complies with all regulatory requirements (GDPR, EU AI Act, eIDAS, etc.) - especially when processing Instagram data.

2.Information collection:

- Technological context: You will analyze how RunwyML works and clarify how this platform processes data from Instagram.
- Legal basis: Collection and review of all relevant laws and standards: data protection (GDPR, eIDAS), copyright (with regard to content on Instagram), media law, liability regulations and industry-specific requirements (EU AI Act, DSA, DMA).
- Stakeholders and resources: Assessment of internal competencies (e.g. Your legal department, IT security) and external experts (data protection consultants, specialized lawyers).

3. Define framework conditions:

- Project organization: Clear assignment of responsibilities (e.g. who supervises the technical integration, who supervises the legal Compliance).
- Time and budget planning: Setting realistic milestones and budgets to implement all necessary legal reviews and technical adjustments.

Phase 2: Analysis and problem definition

1.Needs analysis:

- Identification of legal gaps: Analysis of the extent to which existing contracts with Instagram and the use of RunwyML already cover all relevant legal requirements.
- Technical and legal challenges: Assessment of whether, for example, data processing processes are GDPR-compliant or whether liability issues could arise in the event of incorrect predictions from the AI solution.

2.Risk and opportunity assessment:

- SWOT analysis: You identify strengths (e.g. state-of-the-art AI technology), weaknesses (possible gaps in data security), opportunities (competitive advantages through early Compliance) and risks (high fines for data breaches).
- Legal focus areas: Special attention is paid to topics such as data protection, copyright, liability and the specific requirements of the EU AI Act.

3.Prioritization:

- Urgency matrix: The identified risks (e.g., unclear liability rules in the event of errors in AI evaluation) are prioritized according to their relevance and probability of occurrence, so that the most pressing issues (such as data protection) are addressed immediately.

Phase 3: Consulting and Solution Development

1. Development of concrete proposals for solutions:

- Contract drafting: Development of tailor-made contractual clauses that clearly regulate liability issues, data protection (GDPR-compliant data processing) and copyright issues (when using Instagram content).
- Risk mitigation measures: Define measures such as regular Audits, escalation plans, and technical checks to prevent potential Compliance breaches.

2.Integration of best practices:

- Best Practice methods: Use of standardized checklists that cover all relevant areas of law.
- Workshops and case studies: Implementation of interdisciplinary workshops in order to shed practical light on the solution and possible risks in concrete case studies (e.g. data export from Instagram).

3. Interdisciplinary cooperation:

- Expert panels: Involvement of lawyers, data protection officers and technical experts to ensure that both the legal and technical aspects are optimally considered.

Phase 4: Implementation and documentation

1.Ma action plan:

- Step-by-step implementation: Create a detailed plan that includes, for example, contracting with Instagram, integrating the RunwyML interface, and adapting internal data protection processes.
- Responsibilities: Clear assignment of tasks to internal teams and external partners (e.g., specialized privacy lawyers).

2.Documentation:

- Transparent tracking: All changes, meetings, and decisions are documented in detail - from contract adjustments to technical implementation details.
- Reporting: Regular reports to management and the Stakeholder involved, which make the progress of the implementation and any challenges transparent.

3.Communication strategy:

- Internal communication: Regular updates and training for all affected employees to communicate the new processes and legal requirements.
- External communication: informing partners and, where appropriate, the public about compliance with all relevant requirements in order to build trust.

Phase 5: Evaluation and follow-up

1.Feedback and Review:

- Regular evaluation cycles: After implementation, continuous monitoring is carried out, e.g. through quarterly Audits, to ensure that all measures (e.g. GDPR compliance, liability regimes) are working.
- Integration of stakeholders: Feedback from internal teams and external consultants is systematically collected and evaluated.

2.Customization:

- Dynamic updating: The model is continuously adapted to new regulatory requirements (e.g. adjustments in the EU AI Act or changes to the Instagram terms of use).
- Lessons Learned: Optimizations are derived from the evaluation cycles in order to improve the process in the long term.

3. Long-term support:

- Monitoring: A permanent Monitoring system continuously monitors compliance with all legal requirements and identifies the need for adaptation at an early stage.
- Follow-up appointments: Regular meetings ensure the long-term success and continuous development of the solution. Conclusion This scenario shows how the "Sakizli Five-Phase Model" is used as a structured guide in a consultation to provide legal, contractual and regulatory protection for a complex project - in this case an AI solution that integrates RunwyML and Instagram. By systematically applying all five phases, you ensure that the customer not only

receives a technically innovative solution, but that it also meets all relevant legal requirements and can therefore be operated successfully and compliantly in the long term.

ONLY APPLICABLE LEGAL QUESTIONS ARE REFERRED TO IN ORDER TO MODEL TO THE SCENARIO AND ELIMINATE UNNECESSARY ASPECTS (DEPENDING ON THE CLIENT'S PROJECT IDEA FOR CONSULTING) NOT CONSIDERED. THE REALISTIC IMPLEMENTATION IS DEFINITELY IN THE FOCUS AND DETERMINES THE DEPTH OF THE ELABORATION OF THE MODEL

Scenario: "Alex Meier - The Independent Influencer" Alex Meier is an up-and-coming influencer on Instagram who wants to increase his reach and the added value of his content through data-based insights. He plans to deploy an AI solution that runs on the RunwyML platform and interacts directly with his Instagram account. His goal is to optimize content strategies, identify trends early and thus improve his engagement rate. As Alex operates as a sole proprietor, he must also ensure that all legal and regulatory requirements - such as the GDPR, the EU AI Act and copyright and media law regulations - are complied with. His budget is €15,000 for the entire project.

Phase 1: Preparation and Intake Assessment

1. Clarification of objectives

- Contractual and regulatory objectives:
  - Alex wants to optimize his Instagram activities without violating Instagram Terms of Service.
  - The AI solution should process data in a GDPR-compliant manner so that he does not risk warnings or fines.
  - He wants to address liability issues - e.g. in the case of inaccurate trend forecasts - at an early stage in contracts and internal guidelines.
- Specific objectives:
  - Increase engagement rate by 15% within 6 months.
  - Automated trend analysis that identifies at least 3 relevant content topics per month.
  - Ensuring that all data processing (e.g. from Instagram) complies with the requirements of the EU AI Act and the GDPR.

2. Information collection

- Technological context:
  - Analysis of the RunwyML platform in terms of its interfaces to Instagram and the processing of social media data.
  - Checking the technical requirements: Alex uses a modern smartphone and a laptop, which can be used to implement the integration well.
- Legal framework:
  - GDPR & eIDAS: Examination of how personal data (e.g. comments, likes) can be processed in compliance with data protection regulations.
  - EU AI Act: Evaluation of the transparency requirements and risk classification of the AI solution.
  - Copyright and media law: Ensuring that images and videos analyzed via the platform may also be used in a legally sound manner.
  - Liability law: Development of regulations that protect Alex from possible liability risks (e.g. in the event of incorrect analyses).
- Stakeholders and resources:
  - Since Alex acts as a sole proprietor, he takes on the main responsibility.
  - He hires an external data protection consultant (approx. €2,000) and a freelancer for technical integration (approx. €4,000) - both within budget.

3. Define framework conditions

- Project organization:
  - Alex remains the primary point of contact. He regularly coordinates with the technical freelancer and the legal advisor.
- Time and budget planning:
  - Total project period: 3 months.
  - Budget allocation: approx. €6,000 for external consulting (data protection and legal review), €4,000 for technical implementation, €2,000 for workshops and internal training, €3,000 as a buffer for unexpected costs.
- Risk management:
  - Establishment of an escalation plan: In case of data protection concerns, the external consultant is contacted immediately.

- Establish a Monitoring system (e.g., regular internal reviews) to detect Compliance violations at an early stage.

Phase 2: Analysis and problem definition

1. Needs analysis

- Legal gaps and challenges:
  - Existing contracts: Alex has so far only had informal agreements with cooperation partners - there is a lot of catching up to do here, especially with regard to liability and data protection.
  - Technical aspects: RunwyML's use of the Instagram API must comply with the current Terms of Use to avoid suspensions or legal action.
- Technical and legal challenges:
  - Privacy: Ensuring that all personal data (follower interactions) is anonymized or processed in a sufficiently protected manner.
  - Liability issues: Clear regulation of who is liable in the event of an error - Alex as the end user or the service provider in case the AI makes incorrect recommendations.
- Stakeholder perspectives:
  - The external data protection consultant sees particular risk in data aggregation from social media channels.
  - The technical freelancer points out possible API limitations and their influence on data quality.

2. Risk and opportunity assessment

- SWOT analysis:
  - Strengths:
    - Innovative AI solution with modern technology (RunwyML).
    - Flexibility and fast decision-making processes for a sole proprietor.
  - Weaknesses:
    - Limited budget that only allows for targeted risk management.
    - Lack of in-house legal department, which makes external advice indispensable.
  - Opportunities:
    - Increase reach and engagement through data-driven insights.
    - Competitive advantages through early adaptation of regulatory requirements.
  - Risks:
    - Data protection violations could lead to fines.
    - Possible violations of Instagram Terms of Use due to improper use of API.
- Prioritization:
  - Top priority: data protection and GDPR compliance (critical for personal data).
  - Second priority: Clear liability regulations and technical compliance with Instagram's API specifications.
  - Lower priority: Extended copyright issues, as long as only publicly accessible content is used.

3. Prioritization of risks:

- Data protection Compliance (GDPR, EU AI Act) is considered paramount.
- Technical implementation issues (API compliance) are addressed in parallel, but with lower budget intensity.

Phase 3: Consulting and Solution Development

1. Development of concrete proposals for solutions

- Contract drafting and legal regulations:
  - Data protection clauses: Integration of specific wording that governs the handling of Instagram data and guarantees anonymization and secure storage.
  - Disclaimers: Formulation of clauses that stipulate that liability is excluded or limited in the event of incorrect analyses by the AI - despite regular updates.

    - API Terms of Use: Consultation with the technical freelancer to ensure that the use of the Instagram API is in accordance with the Platform Guidelines.
- Risk mitigation measures:
    - Technical measures: Implementation of an automated Monitoring tool that reports anomalies in data processing.
    - Training and awareness: conducting a small workshop (virtual, approx. €500) with the data protection consultant to sensitize Alex to all relevant GDPR requirements.

2. Integration of best practices:

- Checklists: Creation of a checklist that covers all critical points (GDPR, EU AI Act, Instagram API).
- Best Practice documents: Use templates and guides that have been successfully used by other influencers or small businesses.

3. Interdisciplinary cooperation:

- External experts:
    - A data protection consultant (budget approx. €2,000) reviews the final data protection clauses.
    - A technical freelancer (budget approx. €4,000) ensures rule-compliant API integration.
- Regular voting:
    - Weekly calls (via Zoom) between Alex, the technical freelancer and the data protection consultant to monitor progress and react to changes at short notice.

Phase 4: Implementation and documentation

1. Action plan and implementation:

- Step-by-step plan:
    - Weeks 1-2: Detailed planning, draft contracts and gathering all necessary information.
    - Week 3-6: Technical integration of the RunwyML interface and initial tests of data transmission with Instagram.
    - Week 7-10: Adjustment of contracts and internal processes based on the first test results.
    - Week 11-12: Final Go-live and handover to Alex.
- Responsibilities:
    - Alex coordinates the project and makes final decisions.
    - The technical freelancer implements the interfaces, while the data protection consultant checks the legal aspects.

2. Documentation:

- Project Dashboard:
    - All milestones, decisions and changes are recorded in a central Dashboard (e.g. Trello or Asana).
    - Minutes of weekly calls are archived.
- Legal documentation:
    - Contracts and data protection guidelines are stored in an audit-proof manner, including cross-references to relevant legal articles (e.g. GDPR Art. 5, EU AI Act requirements).

3. Communication strategy:

- Internal communication:
    - Alex receives weekly updates via email and in short video meetings to be informed of progress and any issues.
- External communication:
    - If there are public inquiries (e.g. from cooperation partners or followers), there are prepared statements confirming compliance with all legal requirements.

Phase 5: Evaluation and follow-up

1. Feedback and Review:

- Regular evaluation cycles:

- Monthly reviews (in the form of video calls) with all parties involved to check the functioning of the AI solution, compliance with the GDPR and the effectiveness of the contractual clauses.

- Measurable KPIs:
  - engagement rate: The goal is to increase by 15% within the first 6 months.
  - Number of data protection incidents: The goal is zero incidents.
  - Technical performance: 99% system availability and smooth API integration.

2. Adaptation and continuous optimization:

- Dynamic Update:
  - In the event of changes to the Instagram Terms of Use or new legal requirements (e.g. adjustments to the EU AI Act), the contracts and processes will be adjusted immediately.
  - Lessons Learned from the monthly reviews are included in an update document that makes all adjustments traceable.

3. Long-term support:

- Monitoring system:
  - A permanent Monitoring Dashboard is set up to monitor all relevant KPIs in real-time.
- Follow-up dates:
  - After project completion (after 3 months), quarterly Follow-up meetings are arranged to ensure long-term compliance with legal requirements and the further development of the solution. Scenario

Summary Alex Meier, a self-employed influencer, wants to optimize his social media strategy with an AI solution based on RunwyML and Instagram. With the help of the "Sakizli Five-Phase Model"

developed a project plan that includes the following fictitious answers and benchmarks:

1.Phase 1 - Preparation and Intake Assessment:

- Clear goal definition: Increase engagement by 15%, GDPR-compliant data processing and liability protection.
- Collection of all relevant technical and legal bases, taking into account Instagram, GDPR, EU AI Act, copyright and liability issues.
- Project organization with clear budget and time planning (3 months, €15,000).

2.Phase 2 - Analysis and problem definition:

- Identification of gaps in previous contracts and uncertainties in the use of API.
- Conducting a SWOT analysis that classifies data protection and liability as the highest risks.
- Prioritize risks so that data protection (GDPR, EU AI Act) is dealt with first.

3.Phase 3 - Consulting and Solution Development:

- Development of concrete contractual clauses and data protection guidelines to safeguard liability and data processing.
- Technical measures to comply with Instagram API guidelines and integrate RunwyML.
- Regular coordination between Alex, a technical freelancer and an external data protection consultant.

4.Phase 4 - Implementation and documentation:

- Implementation in a 12-week timeframe with clear milestones and responsibilities.
- Detailed documentation of all project steps and transparent communication via weekly updates.
- Establishment of a project dashboard and audit-proof archiving of all legal documents.

5. Phase 5 - Evaluation and follow-up:

- Monthly reviews with measurable KPIs (engagement, system availability, privacy incidents).
- Continuous adaptation to new legal requirements and Lessons Learned from the evaluation cycles.
- Established a long-term Monitoring and quarterly Follow-up meeting. This scenario shows how Alex Meier uses the "Sakizli Five-Phase Model" to successfully implement his AI solution in a legally compliant manner - despite a limited budget and as a sole proprietor. This ensures that

his technical innovation goes hand in hand with the necessary legal protection and that he benefits sustainably from the data insights gained.

QUESTIONNAIRE WITH SAMPLE ANSWERS FOR PRACTICAL USE OF MODEL:

Phase 1: Preparation and Intake Assessment

Questions

1. Project and goal clarification:

- Question: What are your primary goals with the planned AI solution? Example answer: "I want to increase my engagement rate on Instagram by 15% and get data-driven insights to optimize my content strategy."
- Question: What contractual and regulatory objectives are to be achieved? Example answer: "The solution must be GDPR-compliant, clearly regulate liability issues and enable the use of Instagram data in a legally secure manner."

2.Collection of information (technical and legal context):

- Question: Which technical systems and platforms are used (e.g. RunwyML, Instagram)? Example answer: "I plan to implement the AI solution via the RunwyML platform, which will be connected directly to my Instagram account."
- Question: Which legal requirements are relevant for your project? Example answer: "The GDPR, EU AI Act, eIDAS, copyright and media law as well as liability issues in connection with API uses are important."
- Question: What existing contracts, guidelines or internal regulations are already in place? Example answer: "As a sole proprietor, I have so far had informal agreements with cooperation partners, but no formally secured contracts."

3. Define framework conditions:

- Question: Who are the internal and external stakeholders (e.g. technical freelancer, data protection consultants)? Example answer: "I work as a sole proprietor and hire an external data protection consultant and a technical freelancer."
- Question: What is your budget and what is the timeframe? Example answer: "My total budget is about 15,000 €, and I plan to implement it for 3 months."
- Question: What resources are available internally? Example answer: "I have a modern smartphone and a laptop, but otherwise use external experts."

Phase 2: Analysis and problem definition

Questions

1. Needs analysis and identification of gaps:

- Question: What legal gaps or challenges do you currently see in your existing contracts and processes? Example answer: "There are gaps in the liability regime and there is a lack of clear privacy clauses regarding the use of Instagram data."
- Question: What technical challenges do you expect to face when integrating the RunwyML platform with Instagram? Example answer: "The use of the Instagram API must comply with current policies, and there is a risk of data inconsistencies."

2.Risk and opportunity assessment:

- Question: Which risks (e.g. data protection violations, liability risks) do you consider to be particularly high? Example answer: "The biggest risk is in the area of data protection, especially in the processing of personal data of followers."
- Question: What opportunities does the implementation of the AI solution offer for your business? Example answer: "Through data-driven insights, I expect a significant increase in reach and improved content strategies that give me a competitive advantage."
- Question: How do you prioritize these risks and opportunities? Example answer: "Privacy and liability issues are top priority, followed by technical API requirements."

3.Stakeholder perspectives:

- Question: What expectations do your external consultants (e.g. data protection experts, technical freelancer) have of the project? Example answer: "My data protection consultant emphasizes the need for strict GDPR-compliant measures, while the technical freelancer points to compliant API use."

Phase 3: Consulting and Solution Development

Questions

1. Development of concrete proposals for solutions:

- Question: What contractual adjustments do you expect to make to safeguard liability issues and data protection? Example answer: "I need tailored data protection clauses that govern the handling of Instagram data, as well as disclaimers that apply in the event of incorrect analyses."
- Question: What technical measures should be implemented to ensure compliance with platform policies? Example answer: "An automated Monitoring tool needs to be set up that monitors data transfers and takes into account API terms of use."

2.Integration of best practices:

- Question: What Best Practice methods or checklists do you want to integrate into the solution development process? Example answer: "I would like to use standardized checklists that cover all critical areas (GDPR, EU AI Act, Instagram API)."
- Question: How do you envisage the interdisciplinary exchange between technical and legal experts? Example answer: "Weekly coordination calls between me, my technical freelancer and my data protection consultant are intended to ensure that all aspects are optimally coordinated."

Phase 4: Implementation and documentation

Questions

1.Ma Action Plan and Implementation:

- Question: What should the implementation timeline look like (e.g., milestones, deadlines)? Example answer: "I'm planning a 12-week period: 2 weeks for planning, 4 weeks for technical integration and initial testing, 4 weeks for customization, and 2 weeks for the final Go-live."
- Question: Who takes on which responsibilities in the project? Example answer: "I remain the main point of contact, while the technical freelancer implements the API integration and the data protection consultant takes care of the legal review."

2.Documentation:

- Question: What tools do you want to use for project management and documentation? Example answer: "I use tools such as Trello or Asana for project management and store all legal documents in the cloud in an audit-proof manner."
- Question: How should progress and compliance be documented? Example answer: "Weekly reports, minutes of the coordination meetings and a central project dashboard make progress transparently traceable."

3.Communication strategy:

- Question: How should internal and external communication be organized during implementation? Example answer: "Internal updates are provided weekly via email and short video meetings, while prepared statements are used for external requests."

Phase 5: Evaluation and follow-up

Questions

1.Feedback and Review:

- Question: How often should evaluation and feedback meetings take place? Example answer: "I schedule monthly reviews via video call to check progress and identify optimization potential."
- Question: What KPIs do you consider to be crucial for measuring success (e.g. engagement rate, system availability, data protection incidents)? Example answer: "The key KPIs are a 15% increase in engagement rate, 99% system availability, and zero data breaches."

2.Customization and continuous optimization:

- Question: How do you plan to respond to new regulatory changes or technical challenges? Example answer: "Through regular reviews and the establishment of a Monitoring system, adjustments are implemented promptly."
- Question: How will Lessons Learned be incorporated into future project phases? Example answer: "Results of the reviews are summarized in an update document and used as a basis for the next project phases."

3. Long-term support:

- Question: What Follow-up measures do you plan to take after the project is completed? Example answer: "After the Go-live, quarterly Follow-up meetings will be arranged to ensure long-term compliance."
- Question: How is the Monitoring of the solution to be guaranteed in the long term? Example answer: "A permanent Monitoring Dashboard will be set up to monitor all relevant KPIs in real time."

Summary This questionnaire covers all relevant topics - from goal clarification to risk analysis and solution development to implementation and evaluation. It provides you with a structured template to receive comprehensive information from your customers (whether influencers, small businesses or larger organizations) that you can use optimally in the Sakizli Legal Model. The sample answers give a realistic indication of what typical customer requirements can look like and help to adapt the model individually.