Digitalization and Information Security in German Intellectual Property Firms

Implementing data protection, cyber security and compliance in a holistic and practical manner

Digitalization, cloud infrastructures, and generative artificial intelligence (AI) are fundamentally changing the way businesses and law firms operate. They also increase the regulatory requirements for handling data, information, and digital systems.

A purely data protection-based approach falls short in this context in Germany: in addition to the General Data Protection Regulation (GDPR), information security, cybersecurity requirements, the professional codes of conduct for lawyers and patent attorneys, the protection of trade secrets, and the EU Artificial Intelligence Act (AI Act) also merit particular attention.

This is especially relevant for patent and generalized law firms, as they regularly process personal data, client information, unpublished inventions, trade secrets, and valuable know-how. The use of digital systems and AI therefore simultaneously affects data protection, confidentiality, information security, and corporate governance.

These various regulatory areas pursue different protective objectives:

Area	Subject of protection & regulatory focus
Data protection	Personal data (protection of natural persons)
Information security	All information, IT infrastructures and systems
Professional secrecy	Confidential client information and descriptions of inventions
Protection of trade secrets	Commercially sensitive know-how and technical development data
AI Act	Trustworthy, transparent and competent use of AI

The legally compliant use of digital and AI-supported systems therefore requires not only isolated technical security measures but also a holistic understanding of the various regulatory requirements and their dynamic interactions.

Key regulatory requirements

1. Data protection law (GDPR and BDSG)

Data protection law, comprising the GDPR[1] and the German Federal Data Protection Act (»Bundesdatenschutzgesetz«, BDSG), forms the central framework for the lawful processing of personal data. Of particular importance are lawfulness, transparency, purpose limitation, data minimization, integrity, and confidentiality in accordance with Article 5 of the GDPR.

Of particular relevance to German intellectual property firms are the legal bases for processing, special categories of personal data, data processing on behalf of others, the record of processing activities, and appropriate technical and organizational measures. In the case of cloud and AI services, these are supplemented by data protection impact assessments, transfers to third countries, purpose limitation, data minimization, and »privacy by design« and »privacy by default«.

When using generative AI, it is imperative to check whether personal data, client information, or confidential content is being processed, stored, used for training purposes, or disclosed. Relying on Article 6(1)(f) of the GDPR requires a documented balancing of interests; furthermore, in accordance with the European Data Protection Board (EDPB) and the EDPB opinion on AI models of 18 December 2024,

Article 6(1)(f) of the GDPR:

Processing is lawful only if at least one of the following conditions is met:

[…]

f. the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

[1] REGULATION (EU) 2016/679 of 27 April 2016

an assessment as to whether an AI model can actually be considered anonymous must be made on a case-by-case basis. Client data should therefore only be processed in authorized systems with clear rules of use, safeguards, and contractual assurances.

Furthermore, in the event of a data protection incident – such as the unintentional disclosure of client data to an AI provider or a data breach – the reporting obligations under Article 33 of the GDPR (reporting to the supervisory authority within 72 hours) and, where applicable, Article 34 of the GDPR (notification of data subjects) must be observed. Appropriate processes for incident response and data breach notification must also be established.

Relevant regulations:

- *Regulation (EU) 2016/679 (GDPR), in particular Articles 5, 6, 9, 25, 28, 30, 32, 33, 34, 35 of the GDPR*
- *Federal Data Protection Act (»Bundesdatenschutz-gesetz, BDSG«)*
- *EDPB Opinion 28/2024*

2. Information security and regulatory cybersecurity requirements

Information security extends beyond data protection to encompass all information, IT systems, communication channels, and business processes within a law firm. The aim is to achieve an appropriate, risk-based level of protection for confidentiality, integrity, and availability. In intellectual property firms, this relates in particular to client confidentiality, unpublished inventions, deadline and file management, trade secrets, and operational capacity.

Cybersecurity requirements arise in particular from the European Network and Information Security Directive NIS 2 directive[2] and its transposition into German law[3]. Whether IP firms are directly covered by the directive depends on the individual case; however, the requirements often have an indirect impact via supply chain and client requirements. NIS 2-regulated clients, KRITIS[4]-related companies, banks, industrial enterprises, or public contracting authorities increasingly demand robust evidence of security, policies, and protection concepts.

Standards such as ISO/IEC 27001, sector-specific requirements and baseline IT protection in accordance with the German Federal Office for Information Security (»Bundesamt für Sicherheit in der Informationstechnik«, BSI) provide a structured basis for an Information Security Management System (ISMS[5]). This enables risks, responsibilities, protective measures, and effectiveness checks to be systematically documented – which is particularly important in the case of sensitive client information, patents, and trade secrets.

In practice, this requires secure cloud usage, secure interfaces and API[6] access, role-based access controls, strong authentication, encryption, robust backups, monitoring, and protection against data leakage. When using AI systems, additional requirements include monitoring approved tools, prohibiting the entry of confidential data into unauthorized systems, and assessing risks relating to providers, subcontractors, and data leakage.

Relevant regulations:

- *Act Implementing the NIS 2 Directive and Strengthening Cybersecurity (NIS2UmsG) / Directive (EU) 2022/2555 (NIS2)*
- *ISO/IEC 27001, ISO/IEC 27002 (Specification for an ISMS)*
- *BSI Basic Protection Compendium (Federal Office for Information Security), 2023, BSI Standards 200-1, 200-2 and 200-3*

[2] DIRECTIVE (EU) 2022/2555 of 14 December 2022, inter alia on measures for a high common level of cybersecurity across the Union
[3] In the *Act implementing the NIS 2 Directive and strengthening cybersecurity (NIS2UmsG)*
[4] KRITIS: Critical Infrastructure
[5] ISO/IEC 27001, ISO/IEC 27002
[6] API: Application Programming Interface
[7] Sections 43a(2) and 43e BRAO
[8] Section 2 BORA
[9] Section 39a(2), 39c PAO
[10] Section 4 BOPA
[11] Implementation of DIRECTIVE (EU) 2016/943 of 8 June 2016 on the protection of confidential know-how and confidential business information (trade secrets) against unlawful acquisition, use and disclosure

3. Professional regulations and (patent) attorneys' duty of confidentiality

(Patent) attorneys are also subject to strict confidentiality obligations under criminal and professional law. A breach of these obligations may, for example, in Germany be a criminal offence under Section 203(1)(3) of the German Criminal Code (StGB) (breach of private confidentiality); the confidentiality obligations in Germany are set out in particular by the Federal Lawyers' Act[7] (BRAO), the Professional Code of Conduct for Lawyers[8] (BORA), the Patent Attorneys' Act[9] (PAO) and the Professional Code of Conduct for Patent Attorneys[10] (BOPA), including the provisions governing the involvement of external service providers.

Protection is afforded not only to personal data, but to all information entrusted to, or disclosed in, the course of professional practice, in particular client information, descriptions of inventions, intellectual property strategies, unpublished application documents, and other sensitive business or technical data.

External IT service providers, as well as cloud and AI systems, may therefore only be used subject to a clear contractual confidentiality obligation, appropriate technical and organizational safeguards, and controlled storage, deletion, logging and subcontracting of processing (Section 39c PAO; Section 43e BRAO). Confidential client or invention data should, as a rule, not be stored in freely accessible or unauthorized AI systems, as uncontrolled disclosure – particularly in the case of patent-related information – may jeopardize patentability.

Even though there is no general duty of disclosure regarding the use of AI systems, it is advisable, in the interests of transparency, to include a corresponding provision in the client agreement. This does not affect (patent) attorneys' duties to provide advice and information.

Relevant regulations:

- *Section 203 of the German Criminal Code (StGB)*
- *Sections 43a(2) and 43e of the Federal Lawyers' Act (BRAO)*
- *Section 2 Code of Conduct for Lawyers (BORA)*
- *Section 4 Code of Conduct for Patent Attorneys (BOPA)*
- *Sections 39a(2), 39c Patent Attorneys' Regulations (PAO)*

4. Protection of trade secrets

In Germany, the protection of trade and business secrets is governed by the Trade Secrets Act (»Gesetz zum Schutz von Geschäftsgeheimnissen[11]«, GeschGehG) . Under section 2(1) GeschGehG, information is only protected if it is not generally known or readily accessible, is of economic value due to its confidential nature, and is subject to appropriate confidentiality measures. A mere intention to keep information confidential is therefore not sufficient; active and verifiable protective measures are required.

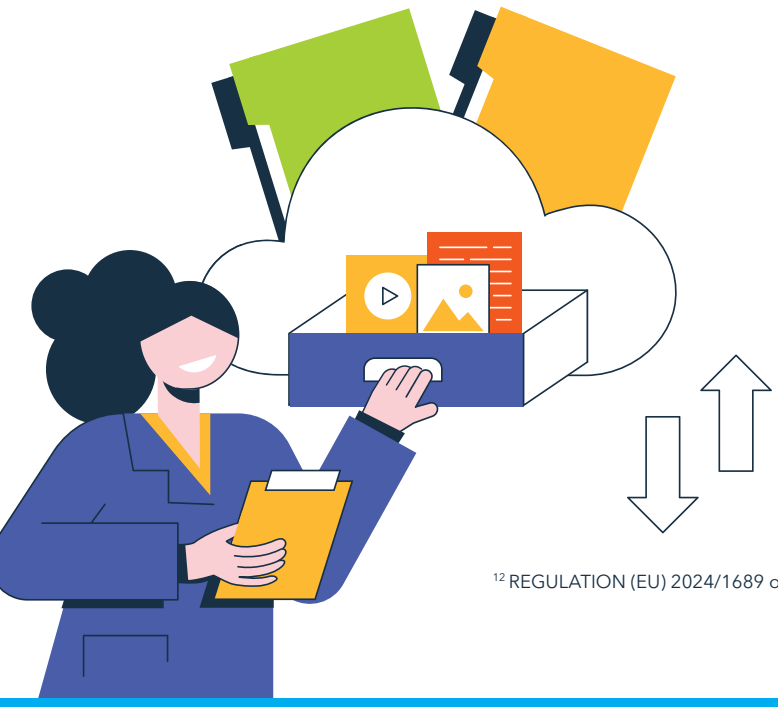
This is particularly relevant for patent and IP law firms in general, as unpublished inventions, technical specifications, R&D data, source codes, intellectual property strategies, and sensitive client information often form the core of a client's mandate. In the case of cloud services and generative AI, additional risks arise from storage, use for training purposes, or disclosure to subcontractors. Risk-appropriate measures are therefore required, such as information classification, role-based access controls, confidentiality agreements, approval processes for external tools, protection against data leakage, logging, and clear deletion and retention policies.

Relevant regulations:

- *Trade Secrets Act (GeschGehG), in particular Section 2(1) GeschGehG*
- *Directive (EU) 2016/943 on the protection of confidential know-how and confidential business information*

5. AI regulation and the EU AI Act

The AI Act[12], the EU Artificial Intelligence Act, establishes a risk-based legal framework for artificial intelligence, setting out requirements regarding prohibited AI practices, high-risk systems, transparency obligations, and AI literacy. As the obligations come into force in stages, it is necessary to assess in each case which requirements already apply to the specific use in question.



For IP firms, Article 4 of the AI Act (on AI competence) and Article 50 of the AI Act (on transparency obligations) are particularly relevant. Risk-aware training, internal usage guidelines, and clear responsibilities for the approval, monitoring and documentation of AI applications are required. A duty to disclose to clients does not arise in every instance of internal AI use but depends on the specific application, output, and professional review by qualified practitioners.

The AI Act does not replace the GDPR, professional regulations, or trade secret protection, but rather complements them. Legally compliant use of AI in IP firms therefore requires a coordinated approach encompassing data protection, confidentiality, information security, trade secret protection and AI governance.

Relevant regulation:

- *Regulation (EU) 2024/1689 on artificial intelligence (EU AI Act)*

in particular regarding AI competence, prohibited AI practices, high-risk AI systems, transparency obligations and tiered applicability (Articles 4, 5, 6 et seq., 50 and 113 of the AI Act)

Summary: Overarching compliance and governance requirements

The regulatory requirements outlined above can no longer be viewed in isolation within modern German law firm operations. Rather, they merge to form a comprehensive compliance and governance system.

For IP firms, this means there is an absolute necessity to establish integrated policies governing the use of digital systems and AI applications, to carry out structured risk and impact assessments, to define organizational responsibilities (e.g., to appoint AI officers), and to implement continuous technical security controls. The legally compliant use of digital tools is no longer purely an IT task, but a core component of strategic IP firm management.

[12] REGULATION (EU) 2024/1689 of 13 June 2024, inter alia, laying down harmonized rules on artificial intelligence

Technical and organisational measures as a common guiding principle

The implementation of the GDPR is based on technical and organizational measures (TOM) in accordance with Article 32 of the GDPR. Further regulatory requirements contain numerous provisions that can equally be classified as technical and organizational measures. Technical measures directly secure IT systems, for example through encryption, multi-factor authentication or DLP[13] systems. Organizational measures establish the necessary structures, in particular clear processes, authorization frameworks, documentation requirements, and training on AI literacy. Technology alone is not sufficient if responsibilities, authorizations, and procedures are lacking; conversely, guidelines remain ineffective if the systems are not effectively protected.

Systematization of IP firm TOMs

Technical measures (infrastructure protection)	Organisational measures (process & risk governance)
End-to-end encryption (in transit and at rest)	IP firm guidelines & AI policies
Role-based access controls	Granular authorization models
Automated backup and recovery systems	AI competence training (Art. 4 AI Act)
Network segmentation & firewalls	Clear governance responsibilities
Multi-factor authentication (MFA)	Binding approval and verification processes
Centralized logging & SIEM monitoring	Comprehensive procedural documentation
Securing API interfaces to AI models	AI compliance & incident management

Only the coordinated interplay of technical and organizational measures ensures that regulatory requirements are effectively met in the day-to-day running of a law firm.

[13] Data Loss Prevention

Key technical measures for IP firm practice

1. Multi-factor authentication: now a must, not an option

The most important immediate measure is the consistent implementation of **multi-factor authentication (MFA)**. A password alone no longer provides sufficient protection for email accounts, cloud services or law firm systems. Phishing attacks and stolen login credentials have long been part of everyday life.

MFA should be mandatory for at least the following accounts:

- email accounts
- Microsoft 365
- IP firm software and DMS
- remote access
- administrator accounts
- client and collaboration portals

Whenever possible, authenticator apps or hardware tokens should be used. SMS is better than nothing, but the technically weaker option.

In practice , MFA must not be undermined by exceptions. Partners, administrators, clients, and senior management alike must adhere to the same standard of protection as everyone else in the firm.

2. Microsoft Azure and Entra ID: centralized management instead of scattered individual accounts

Many IP firms already use Microsoft 365. This makes Microsoft Entra ID the central component for managing identities and access rights. Used correctly, it can significantly enhance security.

The following features are particularly useful:

- centralized user management
- Conditional Access, i.e., access rules based on device, location or risk
- single sign-on
- risk-based detection of suspicious logins
- temporary admin rights instead of permanent full access

This is particularly important for hybrid working models: access to sensitive files should ideally only be possible from **managed and secure endpoints**.

Anyone using Microsoft 365 should not just »let Entra ID run in the background«, but actively use it for security management. The following are particularly useful:

- MFA for all users
- Conditional Access for sensitive applications
- regular review of old user accounts
- separate accounts for normal use and administration.

3. Password security: simple, but clearly regulated

Even with MFA, passwords remain relevant. In many IP firms, the problem lies not in passwords being too short, but in password reuse, poorly documented emergency passwords, or shared accounts.

Reasonable minimum standards are:

- long, unique passphrases
- no reuse across different services
- use of a password manager
- no shared user accounts
- strict separation of user and administrator accounts

A good password manager should be rolled out across the whole firm and its use made mandatory. This reduces the use of insecure DIY solutions like Excel spreadsheets, browser notes, or shared password files.

4. Backups: not just backing up, but truly mastering recovery

Backups are often mentioned, but in practice are too rarely tested consistently. For law firms, it is not enough simply to have »a data backup somewhere«. What matters is whether it is possible to actually get back up and running quickly following an attack or operational error.

A robust backup strategy should include:

- automatic, regular data backups
- backups of emails, files, document management systems (DMS), databases and cloud data
- versioning of older data sets
- separate or immutable backups
- documented recovery procedures
- regular restore tests

The difference between theory and practice is particularly evident in the case of ransomware. If backups have been encrypted along with the data or have never been tested, they are of little use in an emergency.

IP firms should test whether critical systems can actually be restored at least quarterly. The following should be prioritized:

- email
- deadline and file management
- document management
- centralized file storage
- communication systems.

5. Next-generation firewalls and network segmentation

A modern **next-generation firewall** does not merely provide protection based on the old principle of »port open or closed«, but also recognizes applications, suspicious connections, and known attack patterns. This is particularly relevant in environments involving cloud usage, home working and mobile devices.

Network segmentation is also important. Not every system should be allowed to communicate directly with every other system. This prevents an attacker from spreading unhindered throughout the entire IP firm's network following a successful phishing incident.

At a minimum, the following should be separated:

- workstation systems
- servers
- back-up systems
- guest networks
- printer and telephony infrastructure
- remote access

Even simple, properly configured segmentation often results in a significant improvement in security.

6. Email security: securing the most important point of entry

Most attacks still begin via email. Typical methods include phishing, manipulated links, malware in attachments, and forged sender addresses. For IP firms, there is an additional risk: attackers often target communications that appear particularly credible, such as payment instructions, deadlines, or the sending of sensitive documents.

A modern level of protection includes:

- spam and malware filters
- scanning of suspicious attachments
- link scanning
- SPF, DKIM and DMARC to prevent domain abuse
- flag external emails
- protection against mailbox tampering and forwarding rules

Technology alone is not enough here. For sensitive instructions, such as changes to bank details or exceptional payment authorizations, there should always be a second verification step, for example a confirmatory phone call.

7. End-point protection: don't forget laptops and smartphones

In day-to-day working life, risks often arise at end-user devices. Laptops, smartphones, and home workstations are frequent targets of attack. Traditional antivirus software alone is usually no longer sufficient to deal with this.

The following are particularly advisable:

- professionally managed end-point security
- hard drive encryption
- centralized update management
- restricted local admin rights
- mobile device management for smartphones and tablets
- options to lock or remotely wipe lost devices

Access to firm data should only be possible from managed devices. Personal devices without security controls pose an unnecessary risk to sensitive client data.

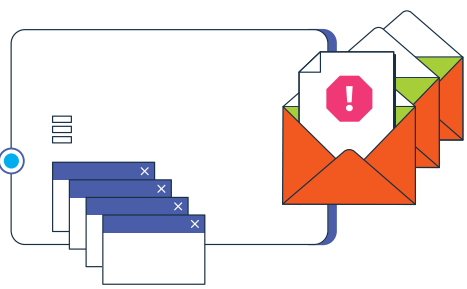
8. Patch management: quickly closing known vulnerabilities

Many successful attacks exploit vulnerabilities for which updates have long since been available. That is why **patch management** is one of the most effective – yet often underestimated – protective measures.

Particularly critical are:

- firewalls
- VPN systems
- email infrastructure
- browsers
- office programs
- PDF software
- IP firm and DMS systems

There should be clear lines of responsibility and fixed maintenance windows. Critical security updates must not be left unaddressed for months on end simply because they »might disrupt day-to-day operations«.



9. Encryption: Protection during transmission and storage

Encryption protects data both during transmission and while in storage. Both aspects are relevant for IP firms. A lost laptop without hard-drive encryption or the insecure transmission of files can immediately lead to a security incident.

Key measures include:

- encrypted connections to all central services
- hard drive encryption on mobile devices
- secure exchange platforms for particularly confidential documents
- clear rules for downloads and local caching

For highly sensitive documents, one should not rely solely on standard email. Protected data rooms or secure file-sharing solutions are preferable.

10. Logging, monitoring and incident response

No IP firm can prevent attacks with absolute certainty. It is therefore crucial to detect incidents at an early stage and respond to them in an organized manner. This requires **logging, monitoring**, and a workable **contingency plan**.

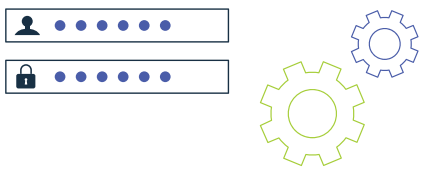
It is particularly important to analyze:

- unusual logins
- failed access attempts
- suspicious changes to user rights
- suspicious file activity
- mass deletions or mass encryption

Even smaller firms should at least define:

- who is responsible in the event of an incident,
- who informs the IT service provider and management,
- how systems are to be isolated,
- how communication with clients takes place,
- when data protection notifications need to be reviewed.

In an emergency, a previously prepared procedure saves valuable time.



Implementation in IP firm practice

Anyone wishing to take a structured approach to information security, data protection, and AI governance should not limit themselves to individual technical measures. A pragmatic starting point is to follow these priorities:

Implement in the short term:

- Introduce MFA for all accounts.
- Review email security and domain protection mechanisms.
- Make the use of password managers mandatory.
- Review the backup strategy and carry out a restore test.
- Ensure hard drive encryption on all mobile devices.
- Reduce local admin rights.

Expand in the medium term:

- Systematically utilise Entra ID and Conditional Access.
- Segment the network.
- Manage end devices centrally.
- Improve logging and alerting.
- Streamline authorization policies.
- Organize patch management in a mandatory manner.

Embed as part of the strategy:

- Establish an incident response process.
- Managing the use of AI from both a technical and organizational perspective.
- Carry out regular access rights reviews.
- Prioritize critical systems and document recovery plans.
- Jointly review and update technical and organizational measures.

In IP firms, technical and organizational measures are not an abstract compliance issue, but a practical safeguard for confidential client data and the day-to-day running of the firm. What matters is not the greatest possible complexity of the IT infrastructure, but the consistent implementation of a few key principles: strong authentication, properly managed access, reliable backups, effective email protection, hardened end devices, up-to-date systems, and clear response procedures in the event of an emergency.

Those who systematically implement these points not only improve their regulatory resilience but, above all, their day-to-day operational security.

In-house development, on-premises, or cloud: security assessment for IP firms

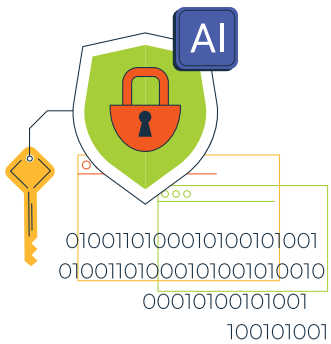
When introducing digital applications and AI-supported systems, IP firms face a fundamental decision: should a solution be developed in-house, operated locally, or procured as a cloud service? There is no one-size-fits-all answer to this. Each model has its own strengths and weaknesses – particularly with regard to security, control, effort, and accountability.

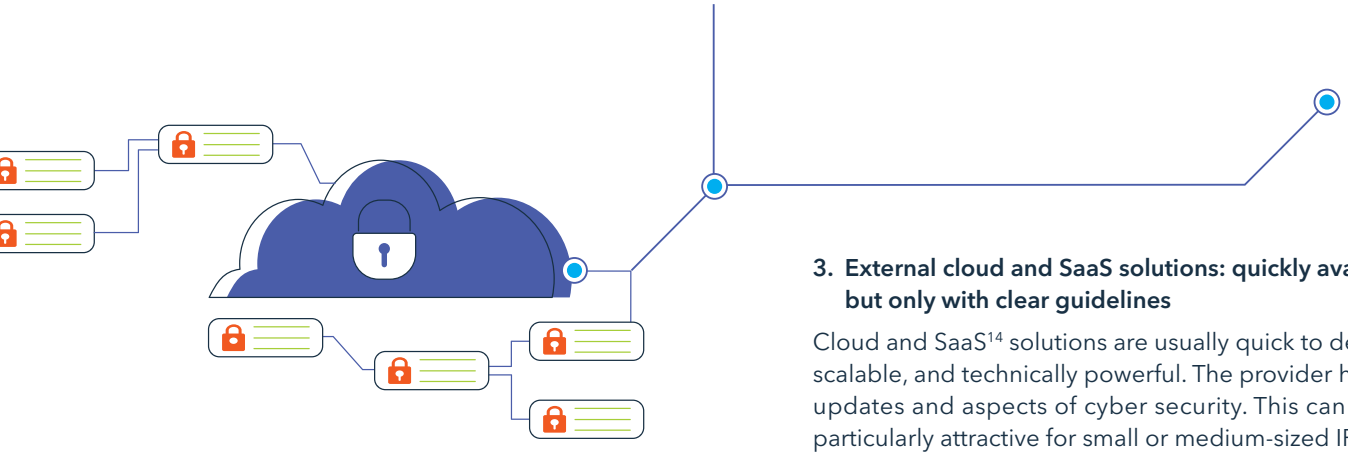
1. In-house development: a great deal of control, but also a great deal of responsibility

An in-house solution offers the greatest freedom of design. Functions, data flows and interfaces can be tailored precisely to the firm's processes. Control over source code and data processing is also greatest in this scenario.

The downside is that the IP firm bears virtually the entire responsibility for security itself. It must not only develop the system, but also ensure that it is developed securely, as well as test, document, update, and monitor it. Typical risks include incorrect access permissions, inadequately protected interfaces, missing updates, or excessive reliance on individual developers.

In-house development is therefore only advisable if there is a permanent supply of sufficient technical expertise and clear security processes in place.





2. On-premises or private cloud: high level of data control, but professional operation required

In the on-premises or private cloud model, the solution runs in a controlled environment within the IP firm or on a dedicated infrastructure. This is often attractive from a confidentiality perspective, as sensitive data does not leave the controlled environment.

However, a great deal of responsibility still rests with the IP firm or its IT service provider. Systems must be hardened, access secured, updates installed, logs analyzed and backups tested. Locally operated AI solutions, in particular, place additional demands on servers, interfaces and storage.

This model is often a good middle ground – but only if operation, maintenance, and security are professionally organized.

3. External cloud and SaaS solutions: quickly available, but only with clear guidelines

Cloud and SaaS[14] solutions are usually quick to deploy, scalable, and technically powerful. The provider handles updates and aspects of cyber security. This can be particularly attractive for small or medium-sized IP firms.

However, it is important to note that responsibility for security does not disappear. Even with SaaS, the IP firm must manage user accounts, permissions, and authorized data processing. The situation becomes critical when confidential client data is uploaded to services whose contractual and security arrangements have not been properly vetted.

From a technical perspective, the key is to integrate cloud and SaaS solutions seamlessly into the firm's existing security architecture. This includes, in particular, integration with SSO[15] and Microsoft Entra ID, mandatory multi-factor authentication, clear assignment of roles and permissions, and the logging of access events. Equally important are contractual provisions regarding data storage, deletion, and the involvement of sub-processors.

SaaS is not inherently insecure – but it is only viable if the solution is properly integrated as an enterprise service and not used like a freely available consumer tool.

Criterion	In-house development	On-premises / Private cloud	External cloud / SaaS
Control over data and data flows	Very high	Significant	Limited
Control over security responsibilities	To be managed entirely in-house	To be managed largely by the law firm or IT service provider	Shared responsibility with the provider
Implementation effort / time-to-value	Longer lead time required	Moderate implementation effort	Can be implemented in the short term
Ongoing operational and maintenance costs	Very high	Moderate to high	Low to moderate
Adaptability and scalability	Very high	Pronounced	Depends on the provider and contract
Suitability for confidential client and invention data	Very good with well-established security processes	Good with professional operation and clear access controls	Only where contractual, security and data processing arrangements have been verified

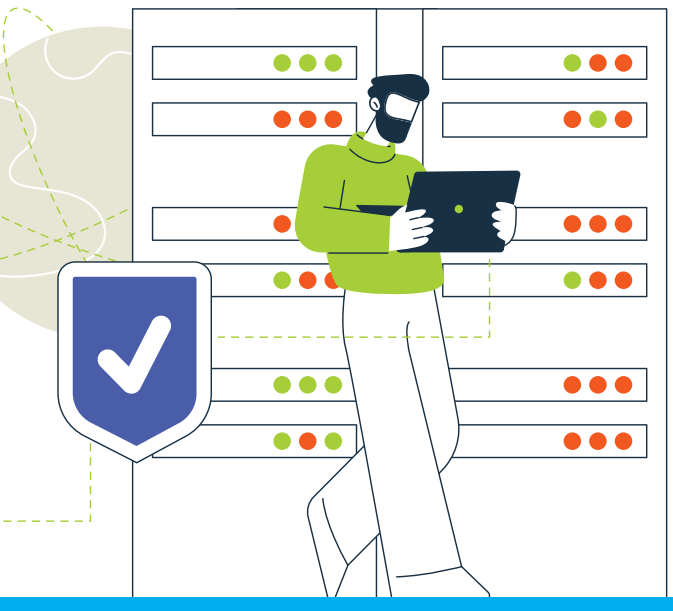
[14] Software as a Service
[15] Single Sign-on

Conclusion and assessment

For IP firms, the location where a solution is hosted is less important than the question of whether security can be reliably managed during day-to-day operations. The key factors are who manages user accounts and access rights, who is responsible for security updates and system hardening, who detects and handles incidents, who backs up data and tests recovery procedures, and who monitors interfaces, data flows, and potential data leaks.

None of the three options just discussed is superior in its own right. In-house developments offer the greatest control and may be particularly suitable for confidential client and invention data, but they require a consistently high level of security discipline. On-premises and private cloud solutions offer a viable middle ground where strict confidentiality requirements apply, but they do require professional management. SaaS solutions are readily available and high-performing, but are only suitable for sensitive content if the contractual, security, and data processing arrangements have been carefully reviewed and the solution is seamlessly integrated into the law firm's environment.

For IP firms, therefore, the key considerations are manageable security responsibilities and the specific suitability for confidential client and invention data. Effective access protection, reliable operation, comprehensive logging, robust backups, clear governance, and traceably controlled data flows are crucial.



Outlook

The digitalization of law firm work will continue to accelerate. Cloud services, automated workflows and generative AI will be integrated even more closely into client case management, research, document creation and IP firm organization in future. At the same time, the digital attack surface grows with every additional interface, every external service, and every instance of mobile access. IT security is thus becoming not merely a technical side issue, but a fundamental prerequisite for trustworthy and resilient law firm processes.

This results in a shift of focus: data protection, information security, cybersecurity, and AI governance will no longer be merely reactive compliance issues, but will become ongoing management tasks for IP firm leadership. Rising risks from phishing, compromised login credentials, ransomware, vulnerabilities in cloud and software solutions, and attacks on supply chains demonstrate that technical safeguards, clear lines of responsibility, and well-rehearsed response processes must be considered as an integrated whole.

For IP firms, it will be crucial not to select digital solutions based solely on efficiency, cost, or ease of use. Rather, the decisive factors will be whether confidential client and invention data can be protected, access effectively controlled, security responsibilities clearly assigned, and AI systems managed in a transparent manner. Those who combine technical and organizational measures at an early stage will not only ensure regulatory compliance but also build trust with clients and stability in the day-to-day running of the firm.

In the long term, those IP firms that view digitalization not as a one-off IT project, but as a strategic governance and security task will have the advantage: with clear guidelines, robust security processes, documented AI expertise, regular risk assessments, and a conscious selection of suitable operating models. In this way, digital innovation can be harnessed without jeopardizing confidentiality, professional secrecy, the protection of sensitive development data, or operational capability.

Rainer Braun
/ Head of IT Infrastructure, Operations and Support

Lars Weißbach, M.A.
/ Advisor to the Management Board
/ Business Support
/ M.A. Business Administration and Management