Implementation of LegalTech Solutions in a Law Firm – Methodology of Risk Assessment and Risk Management

Małgorzata Kurowska

1. Introduction

LegalTech solutions – due to the automated information processing operations, as well as the generally significant level of technical complexity – trigger potential risks from the perspective of the core values associated with the legal profession. The values at stake here are ensuring the confidentiality of information covered by professional secrecy, trust between client and lawyer, or ensuring the highest possible level of service. Violation of these values – as indicated in the chapter *Legal Tech vs Data in Organisation* – involves potential disciplinary liability, and in certain cases may also constitute a civil tort or, still worse, a criminal offence.

A lawyer should therefore take a systematic approach to the project of implementing LegalTech solutions in a law firm – including ensuring accountability of the process of selecting and deciding on implementation in the context of risks related to implementation process.

This section describes such proposals for approaching the above-mentioned project as are intended to mitigate the risk of an alleged failure to exercise due diligence in this context. It should be noted here that the proposals refer to LegalTech solutions that are defined in this paper on several occasions. The proposed model will also be successful in projects involving new information technologies, qualified as LegalTech 1.0. (e.g. implementation of a document repository in a public cloud in a Law Firm), but also more advanced tools of Legaltech 2.0. or 3.0.

It should also be noted that this chapter's perspective is focused only on information security and legal/organisational/technical risks management, resulting from specifics of Legaltech tools. Such issues as business analysis of implementation process, operational aspects or principles internal communication are outside the scope of below considerations.

The basic implementation principles are described at the outset. These principles will serve as a reference for interpreting further steps discussed in the following parts of the section, i.e. information classification and

preliminary assessment of the acceptability of solution implementation, through risk estimation to risk monitoring.

Naturally, the size of this paper does not allow for these issues to be broadly discussed and, as such, the following considerations should be considered as a starting point for developing an optimal approach – in the case of an individual lawyer and his or her practice – that ensures compliance with the ethical standards of the legal profession and mitigates the risk of disciplinary liability or liability for damages.

2. General Principles

2.1. Principle of Proportionality

When implementing a new LegalTech solution, one should take account of the principle of proportionality, both balancing the associated risk and defining the necessary conditions for its use. One should take into account both the type of information to be processed as part of the solution (information classification) as well as its scale and processing context. Measures for safeguarding information handled in the process should match the conditions so defined.

On the other hand, the real possibilities of action on the part of a lawyer (Law Firm) must also be taken into account. In the case of an individual law firm or a law firm employing several or more individuals, extensive paperwork and internal requirements might deter the team and impede the use of LegalTech solutions, thus undermining the efficiency and quality of work.

When balancing sometimes conflicting arguments and making an ultimate decision, a lawyer should bear in mind liability attached to a violation of professional rules, in particular with regard to the protection of information covered by professional secrecy. As such, the principle of proportionality should not be relied on to justify a decision not to conduct an analysis or to apply measures that provide merely an apparent safeguard against the risks identified.

2.2. Principle of Transparency

The implementation of modern LegalTech solutions should take into account the subsequent transparency of actions of a lawyer who will use the

solutions, in the context of his or her relationship with the client. Trust between client and lawyer is a core ethical value of a legal profession and a practical use of the solution should only be allowed where such trust is preserved.

In certain cases, the duty to inform the client will be an explicit legal requirement. This will be the case, for example, for the processing of personal data using profiling – cf. Article 5(1)(a) in conjunction with Article 21(4) of the General Data Protection Regulation (GDPR), or automated decision-making[1] – Article 22 GDPR. Principles of transparency may also be set out in a lawyer's code of ethics or derive from the case law of commercial courts.

However, even in cases where no personal data are processed via the solution used, a lawyer should assess to what extent it is reasonable to inform the client of the use of a particular technology, bearing in mind the crucial importance of trust for the lawyer-client relationship. In practice, a different assessment will apply to solutions that support legal research or the drafting of standard documents, that are subsequently reviewed by a lawyer, and a different assessment will apply to tools whose use may entail specific risks to the confidentiality of client-related information: be it personal data of an individual, data of corporate clients, or data constituting business secrets, etc.

Methods of ensuring transparency may also vary, ranging from individualised information provided at the contract stage to privacy policies posted on a Law Firm's website.

2.3. Principle of Accountability

When implementing LegalTech tools, a lawyer should be able to demonstrate that he or she has exercised due diligence when selecting and implementing the solution (accountability).

It is therefore important to ensure that:

- *all activities related to the selection and implementation of the solution are documented.*
- The activities should be documented in such a manner that makes it possible to establish what steps have been taken, when, by whom and in what order.

1 In the latter case, a lawyer must, in addition to informing the client of personal data processing, provide a specific legal basis set out in this provision.

- For this purpose, the analyses should be recorded in the form of a document – either a hard copy or an electronic version; depending on the specific needs and circumstances, such a document may additionally be protected against subsequent modifications (e.g. by means of an appropriate electronic signature).
- *roles have been clearly defined for the processes of implementation and use of the solution, i.e. specific responsibilities or authorisations have been clearly assigned to them.*
- This approach makes it possible to avoid both positive and negative conflicts of competence and to clearly allocate intra-corporate responsibility. On the other hand, it improves the comfort of work for the Law Firm's employees and associates whose tasks and responsibilities are clearly defined.
- In defining these competencies, a lawyer should take into account the different roles performed in a Law Firm, associated with different levels of disciplinary liability depending on the professional status, as well as the liability of the owner or manager(s) of the Law Firm for acts and omissions of its employees or associates. In this context, it is particularly important to consider:
- the specific role of managing partners or other persons performing managerial functions. Depending on the organisational model, these may not only be partners, but also team coordinators or other senior staff;
- the position of lawyers who are not yet fully licensed but who are required to comply with the relevant code of ethics (trainees);
- the situation of lawyers that are not subject to codes of ethics. In this case, the need to impose certain contractual obligations must in particular be assessed;
- the specific nature of work of those who support the provision of legal services – such as administrative staff, assistants or trainees.

In practice, it is a good solution, especially in the case of teams composed of several dozen or more individuals, to designate a person responsible for all activities related to the use of LegalTech solutions. Such a project manager manages the selection and operation of tools, and ensures that tasks assigned to various risk owners (cf. below) are properly carried out.

2.4. Due Dilligence

We have looked in detail at the principles of lawyer's liability in the chapter Legal Tech vs Data in Organisation. At this point, it is worth recalling that the central importance of protecting professional secrecy and promoting trust between lawyer and client is an essential element of the legal profession. Violation of these ethical principles may give rise to disciplinary liability, and civil liability may also be involved if the client additionally suffers damage. In view of the foregoing, a lawyer should exercise due professional care not only to protect himself or herself against such liability, but above all to avoid causing damage to the client (whether in the form of a tangible financial loss or a moral loss). In practice, this diligence will be reflected in conducting a detailed analysis of the solution to be implemented, learning how it works and identifying the risks associated with its use. In order to structure this process, it is possible – based on the standard information security management model set out in ISO 27 001 – to define the following scheme of action for a lawyer embarking on the implementation of a new LegalTech tool:

1. PRELIMINARY ASSESSMENT PURPOSE: Determining the features of the LegalTech tool, identifying the purpose of the process and the information resources processed by the LegalTech tool. a. Determining the process flow. b. Collecting information on the currently applied information classification and risk estimation principles. c. Collecting documents to be reviewed (provider agreements, policies, internal procedures).	2. INFORMATION CLASSIFICATION AND ASSESSMENT PURPOSE: Determining the features of the LegalTech tool, identifying the purpose of the process and the information resources processed by the LegalTech tool. a. Assigning information resources used in the process to classes. b. Assessment of whether there are any limiting or excluding grounds. c. Assessment of the relevance of the information and its nature.	3. PRELIMINARY DECISION TO USE THE LEGALTECH TOOL	4. RISK ESTIMATION PURPOSE: Risk identification and management. a. Identification of risks associated with the use of LegalTech tool. b. Determining the impact of the risk materialisation and the likelihood of its occurrence. c. Estimating initial risk and identifying countermeasures. d. Identifying residual risk and risk response strategy.

5. RISK RESPONSE DECISION	d. Estimating the scale of the process. 6. IMPLEMENTATION AND APPLICATION OF COUNTERMEASURES PURPOSE: Mitigation of identified risks, process accountability. a. Designating individuals responsible for risk management. b. Conducting ongoing risk monitoring. c. Evidencing actions taken.	7. LAUNCHING LEGALTECH TOOL	8. RISK MONITORING

Detailed comments on the individual elements of the above scheme are described below.

3. Information Classification and Process Evaluation

3.1. Preliminary Analysis and Classification of Information

In view of the liability implications, a lawyer, when opting for a specific solution, should select, in addition to the tool itself, the types of information to be processed as part of the contemplated operations and the manner of processing. This step helps to structure the project assumptions and is the starting point for the risk analysis that follows.

Information classification is nothing more than the assignment of individual pieces of information to categories, singled out as per criteria defined by the organisation. Information classification should be regarded as the first step in implementing information security risk management. Information classification handled on an ongoing basis provides the organisation with up-to-date knowledge of information resources and how they are used, and consequently allows the organisation to respond to changes in its environment.

How to classify information

On the practical side, classification should begin with an inventory of the Law Firm's information resources. A record of processing activities (so-called RPA), maintained pursuant to Article 30 of the GDPR, may be a helpful, albeit not an exclusive, source of information in this respect. However, the Law Firm's internal records (such as RPA, or other records) are sometimes obsolete or incomplete in practice. Therefore, the information inventory should be based on arrangements made directly with those involved in information processing. For small organisations, such as law firms employing a few individuals or so, it is most practical to collect information directly, at meetings; for larger entities, audit questionnaires can be a functional solution.

The inventory should result in a list of information resources, set in the specific context of the organisation.

Example:

Type of information	**Scope of information**	**Context (description)**
Client contact information (B2B)	Business name, email address, telephone number, mailing address	Contact details in the team's CRM, used to contact and send marketing information
Information – client matters	Assignment-related correspondence, content of legal opinions, pleadings, documentation provided by the client	Information covered by professional secrecy which constitutes the content of legal assistance
HR information	Full name, type of agreement, amount of remuneration,	Information on employees – team members

It is worth bearing in mind that at this stage the breakdown of data is based solely on a mainly intuitive functional separation. Only at the next stage – the classification – will the inventoried information be assigned to a specific category (class). However, this requires a **decision on the classification criteria**.

The selection of each classification criterion always remains at the discretion of the organisation (a lawyer). In the context of the objective of ensuring information security, it is reasonable to rely on the criterion of information confidentiality, i.e. the criterion relating to the consequences of disclosing information to an unauthorised individual or individuals).

Example:

Class designation	Description	Examples of information
Class A	*Public data – no confidentiality measures are required*	*Contact details of the Law Firm* *Full names of team members*
Class B	*Internal use information – information that may be disclosed to individuals within the organisation and, if necessary, to specific third parties*	*Contact details of the Law Firm's employees* *Procedure for reporting security incidents*
Class C	*Restricted information – information that may be disclosed to individuals other than its owner only subject to certain conditions, that do not fall under Class D*	*Information on the Law Firm's financial performance* *Information contained in personnel files*
Class D	*Information covered by professional secrecy – accessible only to a lawyer and persons assisted by him/her*	*Information on the subject matter of legal assistance, content of pleadings drafted*

One of the common mistakes made at this stage is to single out an excessive number of classes. This is due to the temptation to describe the information in the organisation as precisely as possible, but this results in losing sight of the fundamental objective of simplifying information management. Singling out a number of classes has no practical consequences as it would not be possible to implement different security rules for so many categories of information.

Another solution is the use of hybrid criteria, i.e. criteria that are attributes of information security (e.g. confidentiality) coupled with normative criteria (e.g. personal data). This type of classification, although encouraging at first sight, turns out to be of little practical use.

Example:

In X Law Firm, "Personal Data" has been singled out as a separate class and a principle has been put in place that no information constituting personal data may be processed with the use of cloud computing.

No one has noticed that the Law Firm uses Jira – in this particular case in a SaaS model – for project management; therefore, full names of team members and project names are recorded in the cloud. The Law Firm also uses Gmail to handle emails.

Context of Solution Implementation

Once the information has been classified by reference to technically neutral criteria (standards) adopted by the organisation, we move on to the selection of LegalTech tools. This is always done in a specific context, which should be properly described before making a decision to implement the solution.

The basic elements to be considered by a lawyer include:

a) **Nature of Information**
   This is the element most closely related to the classification of information and involves establishing whether the information processed with the use of the selected tool, or as part of the assumed operation, constitutes professional secrecy. In certain jurisdictions, professional secrecy related to the provision of legal services in a criminal case (secrecy of defence) may also require additional distinction.
b) **Scale of Information Processing** (**planned scale of use of the tool**)
   The scale should be established taking into account both an objective factor (the actual volume of data processed by the tool or the processes it implements) and a subjective factor (the scale of the process in relation to the scale of the Law Firm's operations).
c) **Legal Constraints**
   A lawyer should make a search for legal constraints that may affect the acceptability of implementing a specific solution. These constraints can:

- **take the form of a specific provision of law**

Example:

no legal basis (Article 22 of the GDPR) for the automated processing of contractual or organisational data for the purpose of making relevant decisions concerning an individual.

- **have a contractual nature**

Example:

Law Firm's client – a financial sector entity – has expressly stipulated in a legal services agreement that it is not possible to process the information concerning it in a public computing cloud.

- **have an intra-organisational nature**

Example:

The Law Firm's corporate requirements, which apply globally, mandate prior notification to head office of any intended implementation of AI-based tools.

d) **Relevance of information**
In order to assess whether it is acceptable to use the selected Legal Tech tool, it is reasonable to take into account, in addition, an attribute which, for the purposes of this paper, will be referred to as relevance of information.
Relevance should be understood as the adequacy of information, taking into account primarily the impact of potential security breaches related to the use of the LegalTech tool on the elements that are most important from the point of view of the legal profession – both from an ethical and a purely practical (organisational) perspective. It is therefore advisable, when determining the relevance of information, for a lawyer to take into account aspects such as security threats related to information constituting professional secrecy and continuity of provision of legal assistance (ethical aspects), as well as to a lawyer's financial situation and reputation – as aspects affecting the practical possibility of practising law.

Assessing the Acceptability of Implementing the LegalTech Solution

The final step of this stage should be a preliminary assessment of the acceptability of implementing the selected LegalTech solution. This assess-

ment should be based on confirmed information – both concerning the tool itself and the context of its use across the organisation. It is worth bearing in mind that in this model the initial assessment precedes the risk analysis, which may result in the identification of additional conditions or qualifications related to implementation.

Depending on the model adopted, the assessment may also indicate the extent to which a risk analysis will be carried out – in particular whether the Law Firm allows for a simplified risk analysis in a given case, in accordance with the standards it has defined.

4. Risk Assessment

4.1. Risk-based Approach

The risk-based approach is one of the concepts that have in recent years been used by legislators and regulators in the area of information protection (including personal data or other sensitive information). This is justified by rapid technological change, requiring a complete change of an approach to the obligation to protect information. Instead of defining, as previously, only "hard" technical and organisational requirements, the legislator now expects an entity responsible for protecting information to analyse the risks to information security itself and to select adequate security measures. At the same time, while regulations such as e.g. the GDPR expressly encourage a "pure" risk-based approach, for specific sectors or areas of law – both the EU legislator and the legislator in the Member States – supplements the risk-based approach by defining a certain standard as a minimum set of functionalities or features that need to be implemented.

ISO 31000 Risk management – Principles and guidelines is a global standard on risk management. The approach set out below takes into account the above standard while respecting the principle of proportionality.

Risk-based Approach in Implementing LegalTech

When implementing LegalTech solutions in a Law Firm, while a key element, risk assessment requires a well-thought, case-by-case approach. The principle of proportionality requires that both the scope of analytical activities and the safeguards to be implemented be adequate – both in

the context of the Law Firm's day-to-day operations and the planned implementation process.

For this reason, it is worth taking into account the possibility of grading the complexity of the analytical process and defining principles for **simplified risk analysis** in the solutions adopted. Such a simplified risk analysis may in particular consist in verifying the fulfilment of the conditions considered to be the minimum acceptable standard for the Law Firm (cf. comments below).

In any event, when deciding to implement a structured approach to risk management, a lawyer should consider elements such as:

a) precise definition of the process and a good understanding of the LegalTech tool under analysis;
b) definition of the context of the process (what information will be processed, whether the information is sensitive, the scale of the processing, its purpose, etc.).

As can easily be seen, clauses a) and b) are comprised in the step above referred to as classification of information and assessment of the acceptability of implementation.

In addition to these elements, as part of risk management, and regardless of the methodology chosen for its assessment, it is necessary:

c) to decide **which areas will be relevant in the context of risk**
For example, such areas may include the security of professional secrecy, continuity of provision of legal assistance, the financial situation or reputation of the Law Firm.
d) to identify, according to the method selected, **the risks associated with the selected solution**;
Risks can be identified, for example, on the basis of a standard risk "checklist", based on brainstorming, the expertise of those involved in the process, or by analysing the so-called "worst case scenario"[2].
e) To carry out a risk assessment in the context of the above areas – in line with the method selected.

A proposal on how to carry out steps from c) to e) is described below under "Risk analysis". It should be stipulated here that there are numerous risk assessment methods – the ISO 31000 standard is adopted below. At the outset of the risk assessment method decision stage, it is important to look at the standards indicated, including **31010:2019 Risk Management –**

2 31010:2019 Risk Management – Risk Assessment Techniques.

Risk Assessment Techniques, which contains a comprehensive discussion of the assessment methods. An ultimate decision should take into account the circumstances of the Law Firm, including its organisational capacity and ease of implementation.

f) Defining the risk response strategy and the risk monitoring rules

However, the risk assessment alone should not put an end to the process. The next step in the risk management process is to define a risk response strategy, the rules for risk monitoring and reporting the results of such monitoring (see below).

4.2. Risk Analysis

Identification of Risk Areas

The first assumption under this approach is based on the identification of areas for which risk will be assessed. It should be noted that a single event can generate different types of risks. From the perspective of implementing the LegalTech solution, we consider at least the following risk areas to be reasonable:

- Risk to the security of information covered by professional secrecy,
- Risk of compromising the continuity of provision of legal services,
- Risk to the financial situation of the organisation (Law Firm),
- Reputational risk.

While the first two areas of risk are closely related to the ethical principles of the legal profession and as such are of paramount importance, especially from the perspective of disciplinary or civil liability, financial or reputational risks are essential from the perspective of the overall situation of the Law Firm as a business entity and workplace.

It should be noted that the above list is by no means exhaustive. Indeed, the obligation to carry out a risk analysis may arise directly from the law – the most typical example in this respect being the obligation to assess the risk to the rights and freedoms of natural persons, as set out in the provisions of the GDPR.

Risk Identification

For a standard risk analysis (leaving aside a simplified analysis here, as discussed below), each of the above areas should be reviewed for the risks they carry.

A **risk** is to be construed as *an event which may result in negative **consequences**, connected with a potential **event** (circumstances), concerning a given area* (e.g. security of professional secrecy, continuity of provision of legal services, financial situation or reputation of the Law Firm).

Example: geographical dispersion of data processing using BigData analytics based on cloud computing.

It is natural for a lawyer to identify **legal risks** – such as, for example, the "take-it-or-leave-it" nature of a contract based on a contractual template and subject to changes that are virtually beyond the user's control, absence of guarantees relating to professional secrecy as required by law to which the lawyer is subject – particularly when the provider is located in another jurisdiction and the contract is governed by the law of the provider's country.

However, it is important to remember that when identifying the risks associated with the selected LegalTech solution, one should not limit their analysis to legal risks alone. Factors of a non-legal nature may also be a source of risk – most notably these include:

- **Organisational factors**: e.g. no effective security incident response procedures; no training for tool users;
- **Technical factors**: e.g. no encryption of data subject to professional secrecy, no adequate authentication mechanisms.

For each defined risk, it is then possible to define basic parameters for risk estimation:

- Relevance of the impact (**consequences**) of the risk on the area(s) identified, and
- **Likelihood** of its occurrence.

Risk Impact Assessment

In a lawyer's practice, the impact of a particular risk will be assessed at an expert level – with an "expert level" to be construed not only as a lawyer's professional judgement, but also as the need, in certain cases, to use the assistance and judgement of a technical expert. When designing a risk

assessment tool, in order to increase the transparency of the assessment, one may consider breaking down the impact assessment into an analysis of the consequences of a given risk for each risk area separately. With this approach, it is only in the next step that an aggregate risk impact assessment is made.

Example:

A	B	C	D	E
Risk	Impact on the security of professional secrecy (1–4)	Impact on the continuity of provision of legal services (1–4)	Impact on the financial situation (1–4)	**Impact assessment** – the highest of the values specified in headings B to D
geographical dispersion of data processing using BigData analytics based on cloud computing	2	1	3	3

Whichever approach is selected, the widest possible range of information sources – such as industry portals, results of security tests carried out, independent calculations, etc. – should be taken into account to estimate the size of the risk.

Determination of the Likelihood of a Risk Occurring

The likelihood of a particular risk occurring may be assessed by taking into account, in particular, factors such as:

a) The attractiveness of the "resource" – primarily the information processed by the tool, or all the information processed in the Law Firm that is accessible by exploiting the vulnerabilities of the tool under analysis;
b) Known vulnerabilities of the tool or vulnerabilities identifiable based on technical expertise;

c) Historical data on similar past events, such as incident data relating to a given LegalTech solution or service provider;
d) Environmental and social factors that determine the possibility of a risk occurring, such as weather conditions or the political situation in the country where the information is processed.

Similarly to the assessment of impact of risk, likelihood can be assessed at an expert level.

Estimation of Overall Risk Value

The overall risk value is an ordered set of risk measures (numbers) for individual risk factors. A lawyer, managing risk at the Law Firm, will set priorities of preventive actions in a descending order of the individual measures once the overall risk value is obtained. This will ensure that the organisation does not waste resources on irrelevant issues and instead focuses on those relevant for its particular situation.

The simplest way to obtain the risk value is to use the following formula:

$$E_1 = I_1 \text{ x } L_1$$

$$\sum$$

where:

E_i – means the risk value for the risk factor

I_1 - means the impact of the consequences of the risk factor

L_1 – means the likelihood of the occurence of the risk factor

Once the risk value have been determined for all identified factors, i.e. E_1, E_2, E_3 , etc. we rank them – as described above – in a descending order, indicating the significance of the factor.

Assigning values (for example – from 1 to 4) to the impact and likelihood parameters, we obtain the following standard risk matrix:

Likelihood Impact	**Likelihood of risk occurrence**			
	low (1)	medium (2)	high (3)	very high (4)
low (1)	1	2	3	4
medium (2)	2	4	6	8
high (3)	3	6	9	12
very high (4)	4	8	12	16
Risk value	**1–3 (low)**	**4–8 (medium)**	**9–16 (high)**	

The above approach – necessarily presented above in a simplified and abbreviated manner – is subject to certain limitations; such as the sometimes strongly subjective evaluation of individual factors (impact and likelihood). However, it also has very important advantages; first of all, it allows risks to be presented in a numerical way, and consequently the results of the estimation are easily **comparable** – both among themselves and also over time. It is also relatively simple to implement in practice.

Issues to be Analysed

As mentioned above, risk assessment methods can vary and the complexity of the assessment method can vary as well. However, a lawyer should in any event consider and analyse the following aspects related to the implemented tool:

- **Legal requirements** related to the implemented tool in the area of:
  - Principles governing the protection of information constituting professional secrecy and personal data;
  - Intellectual property rights to the deliverables of the implemented LegalTech solution;
  - Access rights to the databases used in the solution and acceptability of their use for the intended purpose;
- **Professional conduct requirements**, including:

  - Assessment of the compliance of the solution with the ethical requirements applicable to a lawyer, in particular with regard to the protection of professional secrecy;
  - In the case of cross-border provision of services, the principles expected to be followed by the client;
- **Technical competence** in:
  - Verifying to what extent the organisation (the Law Firm, the users of the tool) has the resources to ensure the correct configuration of the solution and the monitoring of any irregularities;
  - Verifying the resources of potential business partners (solution implementer, maintenance provider, etc.);
- **Law Firm's organisational skills**, including:
  - Verifying that the necessary roles and responsibilities are defined so as to minimise the risk of conflicts of competence when using the solution;
  - Evaluating procedures to ensure the correct application of internal rules for the use of LegalTech solutions (compliance enforcement mechanism);
  - Maturity of the organisation understood as its readiness for a new solution with the possibility of effective implementation (level of awareness of employees and associates);
- **Technical and organisational security offered by solution provider:**
  - Assessment of declared technical and organisational safeguards;
  - Compliance with international norms or standards; or possession of cybersecurity certification from any EU Member State;
  - Use of data encryption, which is the source of information covered by professional secrecy, in any situation where the information would be stored or transmitted to a third party (provider). In the event that a provider were to have access to unencrypted information (e.g. for analytical purposes), the legal permissibility should be verified and the extent of such disclosure documented;
- **Location of data processing resources**
  - Irrespective of the legal requirements related to data localisation (primarily GDPR and client-specific requirements, e.g. cybersecurity requirements or requirements specific to the financial sector), a lawyer should also consider other risks relating to the location of processing centres and its consequences, e.g. the possibility of an actual on-site audit, the possibility of enforcing surveillance by public authorities, etc.;
- **Terms of a solution provider agreement:**

- In a prevailing number of cases, the terms of use of the LegalTech solution purchased are "take-it-or-leave-it" terms. This does not relieve a lawyer of his or her liability for assessing these conditions and balancing the risks;
- A lawyer should focus in particular on issues relating to:
  a) Rules for changing the terms of service and technical aspects of the solution offered;
  b) Commitments (guarantees) to comply with the standards described above (e.g. a contractual guarantee not to use the data for own purposes);
  c) offered SLA (service availability, incident recovery);
  d) Rules for communication (including notification of potential security incidents);
  e) Jurisdiction and applicable law.

4.3. Simplified Risk Analysis

A simplified risk analysis may be considered in certain situations. The criteria allowing for such an assumption should be established and justified by the Law Firm. However, a simplified risk analysis can, as a rule, be carried out especially when:

- The scale of information processing or intended use of the LegalTech solution is insignificant;
- The relevance of information (as defined above) is low;
- LegalTech solution has been granted a cybersecurity certificate based on the national law of the Member State, within the framework set out in the Cybersecurity Act[3];
- There are other specific documented circumstances that justify a simplified risk analysis.

Naturally, the mere possibility of applying the simplified approach in accordance with internal procedures **does not oblige** a lawyer to do so. Conversely, a lawyer **is obliged** to carry out a full-scale risk analysis in a situation where, despite the formal fulfilment of the prerequisites set out

3 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/20133 [2019] OJ L151.

by the Law Firm for relying on a simplified approach, there are specific circumstances that indicate the grounds for such an in-depth analysis.

The scope of the simplified risk analysis should be defined by the Law Firm, but should always refer to the risk areas indicated above. A simplified risk analysis may – for instance – take the form of a checklist in which the actual situation is compared with the minimum acceptable standard applicable in the Law Firm.

Example:

Issue	*Minimum acceptable standard*	*How the standard is complied with*	*Comment; information source*
Legal requirements related to data processing	*Compliance with GDPR (including as regards a personal data processing agreement, if applicable)*	*The processing agreement fulfils the conditions of Article 28 of the GDPR*	*Draft provider agreement dated XXXX - Clause 3, Clause 5*
		An impact assessment of the information provision has been carried out	*Processing impact assessment document – available on the web drive [link].*
		It has been ensured that data subjects are properly informed in accordance with the GDPR	*Draft email to clients containing an information notice [link].*
	An undertaking by the provider that the information processed will be kept confidential by the provider and by those it engages in performing the agreement (if applicable)	*In the agreement the provider undertakes to keep confidential any information processed and not to use the same for other purposes*	*Draft provider agreement dated XXX, Clause 8.3*
	Contractual prohibition from using information covered by professional secrecy for the provider's own purposes (if applicable)		

Issue	*Minimum acceptable standard*	*How the standard is complied with*	*Comment; information source*
Processing territory	*No transfer of information covered by professional secrecy outside the European Economic Area* *In other cases, ensuring GDPR-compliant mechanisms for transferring personal data outside the EEA*	*Data will be processed in a data centre in the EEA (Frankfurt am Main)*	*Order No. XXXXX*
Technical security	*Encryption of information covered by professional secrecy in transit and at rest* *The provider has an ISO 27001 certificate of conformity or a declaration of conformity with the standard*	***No information provided:*** *The provider has informed the law firm that it has an up-to-date ISO 27001 certificate of compliance, but fails to provide the same at the time of the assessment*	*The missing document must be received before the agreement is entered into*
Competences	*Guarantee of adequate technical competence on the part of the provider (if applicable)*	*Guarantees provided in the provider agreement*	*Provider agreement dated XXX, Clause 9*
	Providing necessary training or manuals to the Law Firm's team	*Training on the tool is planned in the Law Firm within 2 weeks after the tool has been launched*	*Information received from XYZ;* *Necessary monitoring of whether training has been provided*

4.4. Risk Response Strategy

For each risk identified, it is necessary for a lawyer to define *a risk response strategy*. Typically, four such strategies are distinguished:

- Risk Acceptance

There are situations where a lawyer can accept the risk. However, such a decision should be informed and justified. For example, as a rule the Law Firm may consider *Acceptance* for all circumstances for which the designated risk measure indicates a low level. A higher-level risk may be accepted in particularly justified cases where the benefits of the implemented solution outweigh the identified risk. It is also recommended to adopt the principle of non-acceptability of risk at a specific highest level, or in relation to a specific area.

Whenever the risk is accepted, it should be ensured that it is monitored to identify any new circumstances affecting its level.

- **Risk Mitigation**

Risk mitigation is the implementation of solutions that ultimately reduce the defined level of risk. This effect can be achieved by:

- **Modifications to the safeguards applied** (technical, organisational, contractual countermeasures) to reduce the likelihood of a particular risk occurring

Example:

The provider agreement stipulates that incident alerts will be directed to the client administration panel. In order to minimise the probability of an alert being omitted, the Law Firm designates a specific person required to log into the user panel on a daily basis to verify the status of alerts.

- **Modifications to the processes in which LegalTech is used**

Example:

The selected solution reviews court judgements in a specific region of the country to identify case law and generates a simplified description of the recommended litigation strategy. In order to minimise the risk of errors, all lawyers using the tool are required to independently review at least 20 % of randomly selected judgements indicated by the solution in order to analyse the usefulness of the tool in achieving its objective on an ongoing basis.

- **Risk Transfer**

Risk transfer is the transfer of the burden associated with a risk occurring to another entity.

Example:

– *Recourse clauses in a solution provider agreement*
– *Insurance policy for third party liability in connection with the use of the solution*

- **Risk Avoidance**

Risk avoidance is the abandonment of an intended action (in whole or in part). The strategy to be applied when identified risks go beyond the acceptable levels.

Example:

The ambiguous wording of a model provider agreement suggests that the provider may use the information covered by professional secrecy for its own purposes in order to improve the solution offered. Provision of data for these purposes is in direct violation of the Law Firm's ethical principles.

Designation of Responsible Persons

Defining a risk response strategy – that is not all. Risk management also requires that specific operations be defined.

Examples of countermeasures in the risk management process may include:

- putting in place internal procedures – in particular as regards communication and analysis of potential incidents;
- training of team members using the implemented tools;
- setting out necessary guarantees in a provider agreement;
- defining internal mechanisms for periodic verification of the effects of the implemented tools.

It is also recommended to document properly appointment of a specific person (or persons, which, however, undermines the effectiveness of the approach) responsible for carrying out specific activities. Apparently, this does not mean that the designated employees will in each and every case personally carry out the tasks assigned to them – rather, it is a question of clearly indicating the ownership of the individual risks. As such, the Law

Firm is able to efficiently verify and periodically account for risk owners, keeping the status of the risk management process under review.

4.5. Identification of Countermeasures

Unless an identified risk is accepted, a lawyer – intending to pursue the process – should identify countermeasures to minimise the level of identified risk.

As is the case with risks, countermeasures can be not only of legal, but also organisational nature.

Example:

Where a risk has been identified relating to a lack of adequate communication regarding security incidents, the following may be identified as countermeasures:

- *Monitoring mailbox designed to receive notifications;*
- *Monitoring publicly available information on security incidents related to a specific solution or provider;*
- *Defining an internal incident response procedure;*
- *Designing persons responsible for carrying out specific tasks related to security incident management.*

The identification of countermeasures then makes it possible to assess how the level of risk changes as a result of the application of countermeasures, and thus to determine whether the proposed countermeasures have been selected correctly, i.e. whether they lead to a reduction in the level of risk originally identified. It should be stressed here that the mere existence of a residual risk (which persists after countermeasures have been applied) is a principle and cannot by itself constitute an obstacle to the implementation of a solution. It is a lawyer (Law Firm) that assesses, based on the analysis carried out, whether such residual risk is acceptable to him or her.

4.6. Risk Monitoring

Regardless of the adopted strategy, risk monitoring is an extremely important element of risk management, including therisks identified as negligible. This ensures that if there is any change in circumstances likely to affect the level of risk, we can respond appropriately and put in place additional countermeasures, if necessary.

In order to monitor risk effectively, it is necessary to designate a specific person in the organisation to whom employees responsible for applying the countermeasures or monitoring process parameters report the results of their activities in this respect on an ongoing basis.

Risk monitoring can be done on an ongoing (regular reporting on individual risks, based on a uniform reporting scheme to ensure comparability over time) or ad hoc basis (ad hoc monitoring, e.g. by internal control in a selected area). Like the other steps in the process, the activities undertaken in relation to risk monitoring should be documented to ensure accountability.

5. Conclusion

This section discusses the basic principles that should apply to a LegalTech implementation project, as well as a proposed approach to estimating the associated risks. The aim of the presented actions is to minimise the risk of disciplinary, civil and, in the most extreme cases, even criminal liability that may attach to a lawyer if he or she violates professional rules. Above all, however, the proposed approach sets out a framework of conduct that allows for compliance with the ethics of the profession, which should underpin every decision taken by a lawyer.