

D1 – Methodology for Contractual Relationships in the Provision of Digital Forensic Analysis and Cybersecurity Incident Response Services



The Automation of Digital Forensic and Incident Response (ADFIR) project is funded by the European Union – NextGenerationEU through the Recovery and Resilience Plan of the Slovak Republic under project No. 09I05-03-V02-00079.

Contents

1 Project Description	3
2 Introduction	3
2.1 Purpose of the Methodology	3
2.2 Theoretical Background to Digital Forensic and Incident Response	6
2.3 KPB1.1 Task	7
3 Contractual Relationships in the Provision of Digital Forensic and Cybersecurity Incident Response Services	7
3.1 Stages of the Contractual Relationship	8
3.1.1. Pre-contractual Stage	8
3.1.2. Contract Conclusion	14
4 Overview	44
5 References	47

1 Project Description

The **Automation of Digital Forensic and Incident Response** project (hereinafter referred to as "ADFIR") is funded by the **European Union – NextGenerationEU through the Recovery and Resilience Plan of the Slovak Republic** under project No. 09I05-03-V02-00079. The project addresses one of the key challenges in cybersecurity and information security: how to process the enormous volume of digital evidence generated during cybersecurity incidents or forensic investigations. At present, this process is highly demanding in terms of human resources and time. Automation using machine-learning methods can therefore significantly **improve the quality of digital forensic analysis** and reduce the time required to carry it out. Overall, this enables security teams to respond to cyber threats more effectively. The main benefits of the project are:

- **Faster resolution of cybersecurity incidents.** The ADFIR project introduces automated approaches to the collection, processing and analysis of digital traces. This enables security teams to identify the causes of incidents more quickly and take effective measures to address them.
- **Reduced workload for forensic analysts.** Routine and time-consuming tasks associated with processing digital traces will be replaced by automated methods. This will allow analysts to focus on more complex cases and strategic decision-making.
- **Higher quality and consistency of outputs.** The use of uniform methodologies and tools ensures that processed digital traces are more accurate, consistent and easier to verify. This significantly reduces the risk of errors caused by human factors.
- **Potential use in criminal proceedings.** The project outputs will be developed in accordance with legal requirements and standards, enabling digital traces to be accepted as relevant evidence for investigations and court proceedings.

2 Introduction

2.1 Purpose of the Methodology

The development of information technologies and the growing dependence of organisations on information systems are leading to an increase in cyber threats, such as ransomware attacks, data breaches and unauthorised access to systems. Addressing these incidents often requires the involvement of specialised providers of digital forensic analysis and incident response services.

The purpose of this methodology is to establish a uniform framework of recommendations and procedures for entering into contractual relationships for the provision of such services. **The objective is** to ensure legal certainty, data protection, preservation of the evidentiary value of digital evidence and effective handling of security incidents.

Legal Purpose of the Methodology

One of the fundamental objectives of the methodology is to ensure that the services provided comply with applicable law. In the course of their activities, digital forensic service providers process data and information protected under a number of legal regulations. These include, in particular, personal data protection, cybersecurity, trade secret protection, copyright, civil and commercial law and, where applicable, criminal law. The most relevant legal regulations in the area of digital forensic analysis and cybersecurity incident response include:

- **Act No. 513/1991 Coll., Commercial Code** (which regulates, for example, the formation of contractual relationships as well as other matters);
- **Regulation (EU) 2016/679 of the European Parliament and of the Council** of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR), supplemented at national level by **Act No. 18/2018 Coll. on Personal Data Protection** (the GDPR affects, for example, contractual provisions concerning the legal basis for processing, security measures, confidentiality, the use of subprocessors and the allocation of roles between the controller and the processor);
- **Act No. 69/2018 Coll. on Cybersecurity**, as amended (which regulates, for example, the obligations of operators of essential services, the handling of cybersecurity incidents and the status of CSIRT units; its requirements may also be relevant to the contractual arrangements for DFIR services);
- **Directive (EU) 2022/2555 of the European Parliament and of the Council** of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (which lays down, for example, requirements for cybersecurity risk management, incident reporting and the use of security services);
- **Act No. 301/2005 Coll., Code of Criminal Procedure** (where digital evidence is intended for use in criminal proceedings);
- **Regulation (EU) 2022/2554 of the European Parliament and of the Council** of 14 December 2022 on digital operational resilience for the financial sector (DORA Regulation).

In addition to legal regulations, international standards also play an important role. Although they are not legally binding, they may serve as a benchmark for professional due care. These include, for example:

- **ISO/IEC 27037** – identification, collection, acquisition and preservation of digital evidence;
- **ISO/IEC 27041** – validation and suitability of forensic methods;
- **ISO/IEC 27042** – analysis and interpretation of digital evidence; ISO/IEC 27043 – incident investigation processes.

The methodology is intended to serve as a tool for identifying legal requirements that must already be taken into account when preparing and entering into the contractual relationship (with reference also to the relevant legal regulations and, where appropriate, the standards set out above). Its objective is to help the contracting parties correctly determine the scope of the service provider's authorisations, the conditions for data processing, confidentiality rules, the extent of liability for damage, dispute-resolution arrangements and other legal aspects of the cooperation.

Purpose of the Methodology from the Perspective of Digital Evidence Protection

A significant characteristic of digital forensic analysis is the handling of digital evidence. Unlike traditional means of evidence, digital evidence has specific characteristics that require a particular approach. It can be modified, copied or destroyed very easily, and even a minimal change may affect its evidentiary value.

The purpose of the methodology is to create conditions (in particular during the pre-contractual stage and the contract-conclusion stage) for preserving the authenticity, integrity and reliability of digital evidence throughout the process of its acquisition, processing, storage and, where applicable, transfer to competent authorities. The methodology is intended to define basic rules for handling digital evidence and recommended contractual provisions governing ownership of the evidence, rights to use it, conditions for its retention and rules for documenting individual actions performed during an incident investigation. Another important objective is to ensure that the results of forensic analysis can, where necessary, be used as relevant evidence in legal proceedings.

Security Purpose of the Methodology

The methodology is also intended to support effective management of cybersecurity incidents through pre-defined rules of cooperation between the client and the service provider. Its purpose is therefore also to provide recommendations for the contractual setting of incident-response processes, including the definition of response times, communication channels, responsibilities of the individual parties and incident-escalation procedures. This increases the organisation's preparedness to deal with security events and reduces potential damage caused by cyberattacks.

Purpose of the Methodology from the Perspective of Personal Data Protection

The investigation of security incidents very often involves the processing of personal data relating to an organisation's employees, customers or business partners. The service provider may have access to email communications, information-system logs, user accounts or databases containing personal data.

The purpose of the methodology is to provide recommendations that ensure lawful processing of personal data during digital forensic analysis and incident response.

Contractual and Organisational Purpose of the Methodology

Another objective of the methodology is to standardise contractual relationships in the field of digital forensics and incident response. At present, there is no single contract model that is generally used by all providers of these services. This may lead to varying quality of contractual documentation and uncertainty in the exercise of the rights and obligations of the contracting parties.

The methodology is therefore intended to provide recommendations for preparing contractual and related documentation associated with the provision of digital forensic analysis and cybersecurity incident response services, taking into account the matters referred to above (for example, compliance with applicable law).

2.2 Theoretical Background to Digital Forensic Analysis and Incident Response

Digital Forensics and Incident Response (DFIR) comprises professional activities focused on the identification, analysis and handling of security incidents, as well as the acquisition and processing of digital evidence. Their performance often requires access to an organisation's information systems, personal data, confidential information and other protected data.

For the purposes of this methodology, the significance of DFIR lies primarily in the fact that these services are generally provided on the basis of a contractual relationship between the client and a professional service provider. Given the sensitivity of the information processed and the potential legal consequences of incident investigations, it is essential to clearly regulate the scope of the provider's authorisations, conditions of access to data, confidentiality rules, protection of digital evidence, liability of the contracting parties and other related matters.

Digital forensic analysis includes activities aimed at acquiring, preserving and evaluating digital evidence, whereas incident response focuses on managing a security event, limiting its consequences and restoring the secure operation of information systems. The two areas are closely interconnected and require clear organisational and contractual rules.

For the purposes of this methodology, the objective is not to discuss the technical aspects of DFIR in detail, but rather to highlight their relevance to the proper structuring of legal and contractual relationships between the client and the service provider.

Properly performed forensic-analysis activities consequently help not only to preserve the integrity of potential evidence, but also to support its admissibility in legal, disciplinary or other proceedings.¹

2.3 KPB1.1 Task

This methodology is an output of task KPB1.1 of work package KPB1, "Legal Issues, Management and CDE", of the ADFIR project.

Task KPB1.1 – Analysis and determination of legal requirements for processing digital traces originating from identified security incidents, required for creating a dataset and improving analytical tools. Consideration of the legal specificities of digital traces and comparison with traditional means of evidence. Analysis of the possibility of entering into legal contractual relationships for the provision of digital forensic analysis and security incident response services (EISI).

This methodology follows on from the third part of the above task and provides a uniform framework of recommendations for entering into contractual relationships for the provision of digital forensic analysis and cybersecurity incident response services. The legal specificities of digital traces and the requirements for their processing are addressed in greater detail, in connection with tasks KPB1.2 and KPB1.3, in separate project outputs (Method for Anonymisation of Digital Traces; Methodology for Processing Digital Traces).

3 Contractual Relationships in the Provision of Digital Forensic Analysis and Cybersecurity Incident Response Services

Unlike ordinary contracts for the provision of IT services, DFIR requires increased attention to the contractual regulation of the mutual rights and obligations of the contracting parties. This is due in particular to the need to ensure lawful data processing, protection of confidential information, preservation of the integrity of digital evidence and a clear definition of liability for damage arising in connection with the handling of a security incident. Ambiguously drafted contractual provisions may lead not only to disputes between the client and the service provider, but also to challenges to the evidentiary value of the data obtained or to breaches of statutory obligations.

¹ MAKATURA, Ivan. Ciele dokazovania v kybernetickej bezpečnosti [Objectives of Proving in Cyber Security]. In: Acta Facultatis Iuridicae Universitatis Comenianae, 2023, Vol. 42, No. 1, pp. 116–146

The importance of contractual regulation is also increasing in connection with the growing use of external specialised DFIR teams, cloud services and cross-border data processing. The contract must therefore regulate not only the scope and manner of service provision, but also rules for handling digital evidence, personal data protection, the use of subcontractors, security measures, incident-handling procedures and the allocation of responsibility among the entities involved.

3.1 Stages of the Contractual Relationship

3.1.1. Pre-contractual Stage

The purpose of the pre-contractual stage is primarily the exchange of information between the prospective contracting parties, together with an analysis of their needs and requirements in relation to the future cooperation. In the DFIR field, this stage is particularly important because the service provider often gains access to sensitive information even before the contract is concluded, and the client must assess whether the provider is capable of ensuring the required level of expertise, confidentiality and security.

The objective of the pre-contractual stage is also to create a sufficient basis for entering into the contractual relationship, identify legal, technical and organisational risks and set the basic parameters of the future cooperation. Properly conducted pre-contractual preparation can significantly reduce the risk of disputes, uncertainties or security incidents during service provision.

Identification of the Client's Needs and Objectives

As part of identifying the client's needs and objectives, it is essential, before contractual negotiations begin, to determine **the nature of the required cooperation and the activities to be performed by the provider.** Proper definition of the subject matter of the future contractual relationship is fundamental to the contract-conclusion process itself.

At the pre-contractual stage, it is therefore necessary to analyse **whether the client requires a one-off service or long-term cooperation.** This question significantly affects not only the economic terms of the contract, but also the scope of the rights and obligations of the individual parties. If the client requires a one-off digital forensic analysis or investigation of a specific security incident, attention should focus primarily on defining the specific systems, devices or data to be analysed. In such a case, before entering into the contract it is necessary to identify what evidence is to be secured, the purpose of the investigation and whether its use is anticipated in an internal investigation, employment dispute, administrative proceedings or criminal proceedings. The answers to these questions then affect the requirements for documenting procedures, preserving evidence integrity and maintaining the chain of custody.

If the client requires an investigation of a specific security incident, basic information about the incident, its scope and possible consequences should already be obtained at the pre-contractual stage. The provider must be able to assess whether the incident involves unauthorised access to a system, a data breach, a ransomware attack, compromised accounts or another form of security incident. It is also necessary to determine whether the incident may trigger reporting obligations under the GDPR, cybersecurity legislation or sector-specific regulation. Without this information, the scope of services and the responsibilities of the individual parties cannot be set correctly.

Where the client is interested in long-term incident-response support or an Incident Response Retainer service, the organisation's level of preparedness for handling security incidents should be analysed before the contract is concluded. The provider should be familiar with the client's organisational structure, the availability of internal IT teams, existing security processes and the organisation's technical environment. Pre-contractual discussions should also determine expected response times, the method for activating the services and the scope of support expected by the client during the term of the contractual relationship.

Particular attention is required where **the client requests the introduction or development of forensic readiness**. In such a case, before the contract is concluded it is necessary to assess the current state of log-recording and retention processes, security-monitoring settings, the possibilities for acquiring digital evidence and the existence of internal policies governing incident response. This analysis usually identifies deficiencies that subsequently become part of the contractual performance.

Before concluding the contract, it is also necessary **to determine whether the client expects support in communications with public authorities or regulatory bodies**. If communication with law-enforcement authorities, the Office for Personal Data Protection, the National Security Authority or other regulatory bodies is anticipated, the scope of the provider's authorisations and the form of its involvement in these processes should be determined in advance. Any statutory obligations of the client that the provider will support through its services should likewise be identified.

An important part of identifying the client's needs is **determining whether the results of the provider's activities are intended to serve as evidence in future court, administrative or employment-related proceedings**. If such use is anticipated, the need to preserve the forensic soundness of procedures, document all actions and ensure the reliability of digital evidence must already be taken into account at the pre-contractual stage. These requirements will then significantly affect the content of the future contract, in particular the provisions on handling digital evidence, confidentiality, data protection and liability for damage.

In this context, it should also be noted that clients increasingly have cyber insurance in place. **Cyber insurance** is a specialised type of insurance intended to cover the financial consequences of cyber incidents and security events affecting an organisation's information systems, networks, electronic services or processed data. Coverage may include, in particular,

costs associated with incident response, digital forensic analysis, restoration of systems and data, legal advice, compliance with reporting obligations, crisis communications, business interruption or compensation for damage caused by a cyber incident.

As part of pre-contractual preparation, it is therefore advisable to determine whether the client has cyber insurance and whether the insurance terms contain requirements that may affect the manner in which digital forensic analysis and incident response (DFIR) services are provided. Although the insurance relationship is between the client and the insurer, its terms may significantly affect the scope of services provided during a security incident, the requirements for documenting actions taken, the manner in which digital evidence is handled or communications with other entities involved in the incident response.

Preliminary Analysis of the Client's Environment

Once the client's needs and objectives have been identified, the pre-contractual stage should include a preliminary analysis of the client's technical, organisational and legal environment. Its objective is to obtain sufficient information to structure the contractual relationship correctly, determine the scope of services, estimate the time and technical complexity of performance, and identify legal and security risks that may affect the future provision of DFIR services. **This is not the digital forensic analysis or security-incident investigation itself, but rather the collection of information required to prepare an appropriate contractual and procedural framework for cooperation.**

One of the first areas to be assessed is **the nature and overall complexity of the client's information systems**. The provider should obtain a basic overview of the number and types of systems used, the network architecture, the number of users, operating systems, platforms and other technological components. Different requirements will apply to an organisation using several local servers and a few dozen workstations than to an organisation operating extensive distributed infrastructure consisting of several data centres, cloud services and thousands of endpoint devices. The complexity of the environment directly affects the scope of future services, the professional resources required, time demands and the resulting price of the services.

Another important area of assessment is **the scope and nature of the data processed**. The provider should determine whether the client's information systems contain personal data, trade secrets, financial data, health records, data subject to banking secrecy or other categories of sensitive information. This information is necessary to identify legal obligations that must subsequently be reflected in the contract, particularly in relation to personal data protection, confidentiality, security measures and the possible use of subcontractors. At the same time, it helps identify risks associated with possible data leakage or unauthorised access during the provision of services.

The analysis should also cover **the technologies and cloud services used**. Today, many organisations use hybrid or cloud environments, while relevant data may be stored with several service providers. A DFIR provider should therefore determine whether the client uses

a public, private or hybrid cloud, what services are operated through external providers and the conditions governing access to those systems. This is particularly important from the perspective of acquiring digital evidence, because the client may not always have full control over the infrastructure in which the relevant data is located.

Particular attention should be paid to **the geographical location of data repositories and the places where data is processed**. If data is located outside the territory of the Slovak Republic or the European Union, additional legal requirements concerning cross-border data transfers, jurisdiction or cooperation with foreign service providers may arise. This may significantly affect the manner in which digital evidence is acquired and retained and its possible use in court or administrative proceedings.

The preliminary analysis should also focus on **the client's existing security measures**. The provider should obtain a basic overview of whether the organisation has security-monitoring tools, centralised logging systems, detection and response solutions, EDR or SIEM tools, and internal security-incident handling processes. The organisation's level of security maturity may significantly affect the scope of future services and indicate the extent to which the client will be able to cooperate in responding to incidents or securing digital evidence.

The analysis should also **assess the client's internal information-security and cybersecurity capabilities**. It is necessary to determine whether the organisation has its own security team, administrators capable of providing technical assistance, or persons responsible for personal data protection and security management. This information is important for determining the scope of services that will need to be provided externally and for setting communication and escalation mechanisms during service provision.

Identifying the regulatory requirements applicable to the client is also important. The provider should determine whether the client is subject to specific sectoral regulation, GDPR requirements, cybersecurity legislation, the NIS 2 Directive or other specific rules. These requirements may have a fundamental impact on the content of the future contract, particularly as regards data retention, reporting obligations, security measures or the manner in which digital evidence is handled.

It is also advisable to determine **whether the organisation has faced security incidents in the past and how they were handled**. Previous experience may reveal existing weaknesses, organisational shortcomings or recurring security problems that should be taken into account when designing the scope of future cooperation. It may also indicate the organisation's level of preparedness to cooperate with an external DFIR team.

When obtaining information at the pre-contractual stage, however, the principle of data minimisation under Article 5(1)(c) GDPR must be respected. The provider should obtain only information necessary to assess the scope of the future cooperation and prepare the contract. At this stage, there is generally no reason to disclose the digital evidence itself, the content of communications, employees' personal data or other detailed information

unrelated to the preparation of the contractual relationship. Compliance with the data-minimisation principle not only reduces legal and security risks, but also contributes to building trust between the prospective contracting parties.

Verification of the Provider's Professional Competence

Before entering into the contract, the client should carry out an appropriate assessment of the provider's professional and technical competence. In the case of DFIR services, selection of the provider should be based primarily on trustworthiness, experience and the ability to respond effectively to security incidents, while price should not be the sole decision-making criterion.

The assessment of the provider should include verification of professional certifications and staff qualifications, personnel and organisational capacity, references from comparable projects, experience in handling comparable incidents, technical equipment, internal security measures, quality-management processes, liability insurance and the ability to provide services in the required scope and availability regime.

Protection of Confidential Information During Negotiations

Because the pre-contractual stage of DFIR services **is characterised by an intensive exchange of information between the prospective client and provider, it is advisable to ensure the protection of such information before it is disclosed**. In practice, the most appropriate instrument is generally a **Non-Disclosure Agreement (NDA)**. Although certain information may also be protected under general legislation, in particular the provisions on the protection of trade secrets under Sections 17 to 20 of the Commercial Code, a separate NDA provides the contracting parties with a higher degree of legal certainty and enables them to define precisely the scope of protected information and the rules governing its use. The NDA should therefore specify which information is to be regarded as confidential. In the DFIR environment, confidential information may include not only the client's commercial and economic data, but also technical information about information systems, network infrastructure, security measures or security incidents. Information concerning information-system architecture, configuration of security solutions, technologies used, system vulnerabilities and the results of penetration tests, security audits or internal investigations is particularly sensitive. Such information can be a valuable source for potential attackers and therefore requires enhanced protection already at the negotiation stage.

The NDA should also clearly define the purpose for which confidential information may be used. The provider should be authorised to use the information obtained solely for assessing the possibility of future cooperation, preparing a draft contract or designing a technical solution.

Another important issue is **determining the group of persons who will have access to confidential information**. Given the specialised nature of DFIR services, it is often necessary to involve external entities in pre-contractual negotiations. The client should nevertheless be assured that access to confidential information is granted only to persons who strictly need it to fulfil the pre-contractual arrangements and, where applicable, subsequently to fulfil the

purpose of the contract. The NDA should include **requirements for appropriate technical and organisational measures to prevent unauthorised access to information, its loss or misuse** (for example, the use of encrypted communication channels, secure repositories or controlled access mechanisms).

An important part of the NDA should also be **the rules for handling information after negotiations have ended**. Pre-contractual negotiations do not always result in a contract, but even in such a case the protection of information already disclosed remains necessary. The NDA should therefore regulate the obligation to return, delete or otherwise securely dispose of all information provided and copies thereof, unless continued retention is required by law or justified by a legitimate interest of one of the parties. At the same time, an appropriate duration of the confidentiality obligation after the end of pre-contractual negotiations should be established, reflecting the sensitivity of the information disclosed.

In most cases, given the confidential nature of the information, the NDA also **regulates liability for breach of confidentiality obligations**. This most commonly takes the form of an agreed contractual penalty, the amount of which is left to the agreement of the contracting parties. A breach may also give rise to a claim for compensation for damage caused by the breach of the relevant obligation.

Where contractual penalties are linked to a breach of confidentiality obligations or rules for handling data, the secured obligation and the circumstances giving rise to the penalty should be defined as precisely as possible. The contracting parties should also maintain appropriate documentation enabling any breach to be demonstrated, such as records of access to data, data exports, transfers or further disclosures (cf. judgment of the Regional Court in Košice, case No. 4Cob/46/2024 of 23 April 2025).

Assessment of Personal Data Processing

As part of the pre-contractual preparation, it is necessary to determine whether the provider will access or process personal data during the provision of services. This issue is particularly important in forensic analyses, incident investigations and analysis of system logs, where personal data is frequently present.

If personal data processing is anticipated, the contracting parties must determine their roles under data-protection legislation in advance, identify the legal basis for processing, assess the need to enter into a data-processing agreement and verify the adequacy of technical and organisational security measures. Issues of cross-border data transfers, data retention and procedures in the event of a personal data breach must also be addressed.

Outputs of the Pre-contractual Stage

The outcome of the pre-contractual stage should be a comprehensive basis for entering into the contractual relationship and subsequently providing DFIR services. The principal outputs include in particular:

- a clear definition of the subject matter and objectives of the cooperation,

- identification of technical, security, legal and organisational risks,
- determination of the scope of services to be provided,
- execution of a non-disclosure agreement,
- identification of personal data protection requirements and preparation of related documentation,
- preparation of a draft contract and its annexes.

A properly conducted pre-contractual stage creates the conditions for transparent, secure and effective provision of digital forensic analysis and cybersecurity incident response services throughout the contractual relationship.

3.1.2. Contract Conclusion

Following completion of the pre-contractual stage and achievement of basic agreement between the prospective contracting parties, the contract-conclusion stage follows. This is a key stage of the contractual relationship, during which the identified needs of the client, technical requirements, security expectations and legal obligations are transformed into binding contractual provisions. The quality of the contractual arrangements at this stage significantly affects not only the course of digital forensic analysis and cybersecurity incident response services, but also the parties' ability to prevent future disputes and effectively address situations that may arise during service provision.

Selection of an Appropriate Contractual Model and Contract Documentation

The first step in concluding the contract is to determine the appropriate legal and commercial model of cooperation. In practice, DFIR services may be governed by different types of contractual arrangements depending on the scope and nature of the services provided.

The most commonly used arrangements are:

- one-off contract
- framework cooperation agreement,
- retainer agreement
- Service Level Agreement (SLA)
- and other arrangements

Criterion	One-off contract	Framework agreement	Retainer agreement	SLA
Handles a specific incident	Yes	No	No	No
Long-term cooperation	No	Yes	Yes	Supplementary

Guaranteed availability	No	No	Yes	Only if part of the retainer
Priority response	No	No	Yes	May be specified
Capacity reservation	No	No	Yes	No
Recurring fees	No	Generally no	Yes	No
Suitable for crisis situations	Limited	Partly	Yes	Supporting
Administrative burden during an incident	High	Medium	Low	Low

Table 1 – Comparison of Contractual Models for the Provision of DFIR Services

For long-term preparedness to address cybersecurity incidents, an appropriate model may be a combination of a framework agreement and a retainer agreement supplemented by an SLA. Such an arrangement provides a stable legal basis for cooperation, ensures the provider's preparedness for incidents and at the same time precisely defines required response times and qualitative service parameters.

A one-off contract is particularly suitable for organisations that use DFIR services only occasionally or are dealing with an isolated incident without a need for long-term cooperation.

Hybrid Contractual Models in Practice

At present, one of the most widely used models for providing digital forensic analysis and cybersecurity incident response services is **the hybrid contractual model**, consisting of several interconnected contractual documents. The basis of the cooperation is generally **a framework agreement governing** the general conditions for service provision, the rights and obligations of the parties, rules on liability for damage, protection of confidential information, dispute resolution and other fundamental aspects of cooperation. The framework agreement is usually supplemented by a **Non-Disclosure Agreement (NDA)**, intended to protect trade secrets, technical documentation, information on vulnerabilities of information systems and other confidential data to which the provider may gain access in the course of its activities.

If the services involve the processing of personal data, the contractual documentation will also usually include a **Data Processing Agreement (DPA)**, governing the conditions for processing personal data in accordance with the GDPR, including security measures, the scope of processing, the use of subprocessors and the rights and obligations of the controller and processor. Another important component of the hybrid model is the **Service Level Agreement (SLA)**, which specifies the required availability of services, response times, incident classification, escalation procedures and other measurable parameters of service quality.

For organisations requiring a high level of preparedness for security incidents, the cooperation is often supplemented by a **retainer agreement**. Its purpose is to reserve the provider's professional capacity in exchange for a recurring fee, while the client receives guaranteed service availability and priority response in the event of an incident. Individual investigations, incidents or projects are then carried out under separate work orders or Statements of Work

(SOWs), specifying the scope of services, timetable, required outputs and pricing terms for the particular assignment.

The advantage of the hybrid contractual model is that it separates the general conditions of cooperation from the specific requirements of individual incidents or projects. This approach creates a stable legal framework for cooperation, ensures the provider's preparedness to respond to security incidents and at the same time preserves sufficient flexibility for ordering specific services according to the client's current needs.

Identification of the Contracting Parties

Correct identification of the contracting parties is a fundamental prerequisite for a valid and effective contractual relationship. Although it may appear to be merely a formal element of the contract, proper identification has particular importance in the provision of digital forensic analysis and cybersecurity incident response (DFIR) services. Unambiguous identification of the parties is necessary to determine their rights and obligations, responsibility for contractual performance, protection of confidential information, personal data processing and the enforcement of contractual claims.

During the contract-conclusion process, the identity of the contracting parties, their legal capacity and the authority of the persons acting and signing on their behalf should be verified before signature. Insufficient verification may lead to legal uncertainty, disputes concerning the validity of the contract or difficulties in enforcing contractual rights.

In addition to identifying the contracting parties themselves, it is advisable to identify, at the contract-conclusion stage, **the persons responsible for communication and coordination of contractual performance**. In the field of DFIR services, immediate communication is often required during the handling of security incidents, so contact persons should be clearly designated, including substitute contacts.

In particular, it is recommended to identify:

- persons authorised to report security incidents;
- persons authorised to approve interventions in information systems;
- contact persons for technical communication;
- contact persons for legal and contractual matters;
- persons authorised to accept the outputs of the services provided.

Where services are provided on a 24/7 basis, the availability of these persons outside normal working hours should also be addressed.

If the provider anticipates **involving subcontractors or other external entities**, their status and the scope of their involvement should already be transparently defined when the contract is concluded. The client should be able to know which entities will participate in the provision of services and the extent of access they will have to the client's systems or data.

Definition of the Subject Matter of the Contract

The subject matter of the contract is one of its most important provisions. It should be formulated with sufficient precision to avoid uncertainty regarding the scope of services. **The basic recommendation is that the subject matter should be defined specifically rather than generally.** In practice, it is not sufficient to use formulations such as "provision of IT security services"; **the contract should specify whether the service concerns digital forensic analysis, response to a cyber incident or a combined DFIR engagement.** In practice, combining unrelated activities, such as DFIR services with IT infrastructure management or software development, is often problematic because it creates ambiguity in the legal framework. A properly defined subject matter should also specify the technical activities to be carried out by the provider (for example, collection and analysis of digital evidence, malware analysis, network forensics or work in cloud environments).

Another important element of the subject matter is a **clear definition of the objectives of the services.** These may include identifying the cause of an incident, determining its scope, securing and analysing digital evidence, restoring system security or supporting legal and insurance proceedings. **The subject matter should also be linked to the temporal and organisational framework for service provision, in particular response times, service availability and incident-escalation mechanisms.**

Particular attention should be paid to distinguishing reactive DFIR services from preventive activities such as monitoring, auditing or penetration testing. These areas have different purposes and legal regimes, and combining them within a single broadly defined subject matter may therefore lead to uncertainty and reduce the effectiveness of the response.

Specific Aspects of Public Procurement

If the client is a contracting authority or contracting entity, the rules of public procurement must also be taken into account when defining the scope of DFIR services. Particular attention should be paid to subsequent extensions of the scope of services through amendments, work orders or partial orders. If such an extension constitutes a substantial modification of the originally procured subject matter, it may not be possible to implement it solely by amending the existing contract, and a new public procurement procedure may be required. For this reason, the original procurement documentation should define the anticipated scope of DFIR services, mechanisms for their activation and permissible options or changes with sufficient precision (cf. judgment of the Administrative Court in Bratislava, case No. BA-1S/83/2020 of 29 October 2025).

Scope of the Provider's Authorisations

The provision of DFIR services often requires extensive access to the client's information systems. The contract should therefore precisely regulate the scope of the provider's authorisations. Ambiguously defined authorisations may lead not only to disputes between the parties, but also to security, operational or legal risks. **The scope of authorisations should always be proportionate to the purpose of the services and based on the Principle of Least**

Privilege, under which the provider is granted only such access rights and powers as are necessary to achieve the agreed purpose.

What should the contract contain in relation to the scope of the provider's authorisations?

- **Scope of access rights** – The contract should precisely specify the systems, applications, databases, cloud environments or repositories to which the provider is authorised to gain access. It should also define the level of access, for example whether access is read-only, includes administrator privileges or permits changes to systems.
- **Authorisation to access network devices** – The contract should specify whether the provider is authorised only to obtain information and logs from devices or also to make configuration changes. If interventions are permitted, the conditions for approving such actions and the persons authorised to give consent should be clearly defined.
- **Authorisation to analyse user accounts** – Given the potential interference with employees' privacy and the processing of personal data, the contract should clearly define the scope of such authorisation, the purpose of processing the data obtained and the rules for its protection. Compliance with personal data protection and employment legislation must also be ensured.
- **Authorisation to obtain logs and records** – The contract should define the types of logs that the provider may obtain and process, for example system logs, application logs, network records, authentication records, records from security solutions or cloud services.
- **Authorisation to create forensic copies of data** – Because the creation of forensic copies constitutes an intervention in the client's information environment and may involve processing large volumes of data, including personal data or trade secrets, the contract should precisely define the scope of this authorisation. It is recommended to regulate the manner in which forensic images are created, requirements for preserving data integrity, documentation of the Chain of Custody, retention periods for copies obtained and the conditions for their secure destruction or return to the client after the investigation is completed.
- **Authorisation to perform active interventions in systems** – Given that these activities may significantly affect system availability and the client's operations, it is recommended to define precisely which actions the provider may carry out independently, which require the client's prior approval, and which are permissible only in the event of a critical or imminent incident.
- **Authorisation to use automated tools** – The contract should regulate the scope of use of automated tools, responsibility for their configuration, the conditions for their deployment in a production environment and any restrictions on automated interventions performed without direct human involvement.
- **Conditions for involving subcontractors or other external entities** – The contract should regulate any requirement for the client's prior consent, the professional competence required of subcontractors and other external entities, the scope of information to which they may gain access and the obligation to ensure the same level of information protection as is required from the main provider. Responsibility for the

activities of subcontractors and other external entities should remain with the provider unless the contract expressly provides otherwise.

Client Obligations

Unlike many other services, the provider is generally unable to perform its activities independently without active cooperation from the client, its employees or responsible persons. The success of a security-incident investigation, the quality of forensic analysis and the ability to respond effectively to security threats therefore depend to a significant extent on the scope and quality of the cooperation provided.

The contract should clearly regulate the client's obligations and define the consequences of failing to comply with them. Insufficient or delayed cooperation may lead to longer response times, loss of evidence, limitations on the investigation or inability to achieve the required results.

The basic client obligations to be addressed by the contract should include, in particular:

- ensuring access to systems;
- providing the necessary documentation;
- designating contact persons;
- providing accurate and complete information;
- ensuring cooperation by employees;
- creating the conditions necessary for service performance.

To ensure a clear allocation of powers and responsibilities during incident handling, it is recommended to prepare a responsibility matrix (RACI matrix). This is one of the most effective tools for reducing the confusion that can arise during a critical cyber incident. In contracts for the provision of DFIR services, particularly Incident Response Retainer arrangements, the RACI matrix should be attached directly to the contract, thereby becoming **a legally binding document**. The standard RACI division of roles is used for DFIR contracts. The following RACI matrix is an illustrative example that should be adapted in each specific case to the client's organisational structure, its legal and regulatory obligations and the agreed scope of the provider's services.

- **R – Responsible:** The person who actually performs the technical or organisational work.
- **A – Accountable (Final decision-maker / Approver):** The person with decision-making authority. This person has the authority to veto or approve the relevant step (for each task in a RACI matrix there should be only one A, generally on the client's side).
- **C – Consulted:** An expert whose opinion or analysis is required before the relevant step is taken (for example, the legal department or an external forensic team).
- **I – Informed:** A person who is merely informed of the outcome or status after the step has been taken (for example, management or the PR department).

Incident specific task	phase	/	Client	Provider	DPO	Management
1. Detection, triage and activation						
Identification of suspicious activity and initial log collection			R	C	I	I
Activation of the DFIR contract (declaration of incident) and commencement of the SLA			C	R	I	A
2. Isolation and Mitigation (Containment)						
Decision to take production offline (shutdown of infrastructure/Internet)			C	C	I	A
Technical isolation of compromised systems and networks			R	R/C		I
Change of compromised credentials and administrator accounts			R	C		I
3. Forensic acquisition and analysis						
Securing forensic evidence (RAM, HDD) in accordance with standards			C	R	I	I
In-depth analysis of malware and logs and determination of the attack vector (Root Cause)			C	R		I
Identification of the scope of compromised data (whether data leakage/exfiltration occurred)			C	R	C	I
4. Remediation and Recovery						
Approval of the recovery strategy (e.g. restore from backups vs. negotiation)			C	C	C	A

Removal of attacker persistence (backdoors) from the infrastructure	R	R/C		I
Final security audit (hardening) before production restart	R	R		I
5. Legal obligations and closure				
Reporting the incident to the National Security Authority (NBÚ) / CSIRT (within the deadlines under applicable law)	I	R	C	A
Risk assessment and reporting to the Office for Personal Data Protection under the GDPR (72-hour deadline)	I	R	C	I
Preparation of the final forensic expert report	I	R	C	I

Table 2 – Sample RACI Matrix

Specific Aspects of the Use of Artificial Intelligence and Automation Tools

The contractual documentation must reflect the specific legal and technological risks associated with their use. When drafting the contract, the following safeguards should be implemented:

- Algorithmic transparency and verifiability (Explainable AI) and forensic integrity:** The contract should regulate the provider's procedures so that conclusions, detections, data selections or identifications of digital traces obtained through automated tools are, to an appropriate extent, retrospectively verifiable, documented and reviewable by a qualified professional. Depending on the nature of the tool used, the contractual documentation should regulate the retention of information necessary for subsequent verification of the result, in particular information on the tool and its version, relevant inputs, analysis parameters, time data and available logs of the analytical process. It is also advisable to require the provider, upon request, to provide, to an appropriate extent and subject to the protection of intellectual property rights and confidential information, information on the methodology used, the principles governing the operation of the tool and known limitations of automated analysis where necessary to verify or assess the result. If the result of automated analysis is to be used as a basis in court, administrative or other legal proceedings, adequate documentation and the possibility of professional review may be important when assessing its reliability and evidentiary value.

- **Data ownership, intellectual property protection and model-training clauses:** The contract should regulate whether, and under what conditions, the provider is authorised to use the client's data in artificial-intelligence systems. Without an express contractual and legal basis, neither the provider nor its subcontractors should use the client's data for further training, fine-tuning or validation of models beyond the purpose for which the data was made available. If the contract expressly permits such further use, it should precisely determine its purpose and scope, the categories of data concerned, the conditions for anonymisation or other appropriate modification of the data, protection of personal data, confidential information and trade secrets, as well as rules for handling the data after the contractual relationship ends. The parties should also clearly determine the rights to final analytical outputs, scripts and other results created during the incident.
- **Allocation of liability for automation errors, detection asymmetry and operational damage:** The contract should appropriately allocate risks and liability arising from automation errors, including false detection, failure to detect a threat and operational damage caused by an automated intervention. It is advisable to define contractual levels of autonomy and identify categories of incidents, conditions or thresholds under which a specific automated intervention may be performed without prior human approval; in other cases, the result or proposed intervention should be subject to appropriate human verification. The provider's liability should be assessed by reference to its specific contractual obligations and the circumstances of the case, taking particular account of the required standard of professional care, the agreed degree of tool autonomy, appropriate updating and maintenance of the tool, the extent of human verification and mandatory limits under applicable law. The contract should therefore not automatically exclude liability for a missed threat or create the impression that an automated tool guarantees an error-free result.

SLA and Response-Time Arrangements

In the provision of digital forensic analysis and cybersecurity incident response services, the Service Level Agreement (SLA) is one of the most important parts of the contractual documentation. SLA provisions determine the expected level of service availability, provider response times, communication rules and incident-handling procedures. Properly structuring these provisions is fundamental to effective management of security incidents, management of client expectations and prevention of disputes during contractual performance.

Unlike ordinary IT services, even a short delay in responding to a DFIR incident may significantly affect the extent of damage, availability of information systems, preservation of digital evidence or compliance with statutory reporting obligations. SLA parameters should therefore be formulated clearly, measurably and in a manner that permits objective assessment of compliance.

In practice, SLAs most commonly regulate the following areas:

- **Service availability** – A precise definition of the time periods during which the provider is required to make its services available. The extent of availability depends on the nature of the client, the level of risk and the importance of the services. In practice, services may be provided, for example, during specified working hours on business days or on a continuous 24/7 basis. Critical infrastructure, major operators or organisations with high business-continuity requirements generally require continuous availability of an incident-response team. The contract should also regulate how availability will be ensured, minimum staffing capacity and conditions for service provision on non-working days, public holidays or in exceptional circumstances.
- **Incident-reporting method** – The contract should regulate the communication channels through which the client may report an incident and the minimum information that the report must contain. Depending on the nature of the services, incidents may be reported via a telephone line, email, customer portal, ticketing system or another communication tool. It is also advisable to specify which methods of notification constitute an official incident report from which the SLA time limits begin to run.
- **Response times** – This is the period between the reporting of an incident and the provider's first response. A response does not necessarily mean resolution of the incident itself; it may consist, for example, of acknowledging receipt of the report, commencing communication with the client or carrying out an initial assessment of the situation. When setting response times, it is advisable to take account of the severity of the incident and its potential impact on the client's operations. Critical incidents generally require a response within minutes or hours, while less serious events may be subject to longer response periods.
- **Time limits for commencing intervention** – It is also recommended to define the maximum period within which the provider must begin carrying out specific activities aimed at addressing the incident.
- **Incident categorisation** – Because not all security incidents are equally severe, the SLA should contain rules for their classification. Categorisation makes it possible to adapt response times and the scope of measures to the actual significance of an incident. Classification criteria may include, in particular, the extent of the threat to information assets, the impact on the organisation's operations, the number of affected systems, the risk of a data breach, financial impacts or potential regulatory consequences. Several severity levels should be defined, with specific response times, escalation rules and required measures assigned to each level.
- **Escalation procedures** – Handling a security incident may require the involvement of additional experts or higher levels of management on the client or provider side. The contract should therefore include clearly defined escalation mechanisms. Escalation procedures should regulate the conditions for escalation, the persons authorised to make decisions, the method of communication and time limits for resolving escalated situations. Particular attention should be paid to incidents that may affect the organisation's critical processes, personal data protection or compliance with statutory obligations.

- **Availability of contact persons** – The contract must identify the persons authorised to communicate during the handling of a security incident, approve individual actions and take decisions necessary to secure or restore the operation of information systems.
- **Consequences of SLA non-compliance** – Their primary purpose should not be to punish the other party, but rather to create an incentive to comply with contractual obligations and ensure predictability of the services. In DFIR services, consequences are most commonly linked to failure to meet response times, unavailability of agreed professional capacity, failure to deliver outputs on time or breach of communication obligations during an incident. Contractual penalties, fee reductions, provision of additional services free of charge or other compensation mechanisms are commonly used in practice. The contract should also define circumstances in which such consequences do not apply, for example force majeure, insufficient cooperation by the client or technical obstacles caused by third parties.

Incident Severity Matrices are also an integral part of response-time arrangements. They define how quickly the provider must respond under the SLA and what resources both parties must activate in response to the incident. Without such a matrix, the client may demand an immediate response to a virus-infected employee laptop while, conversely, underestimating a stealth intrusion. A severity matrix has no contractual value unless it is linked to the **Service Level Agreement (SLA)**.

It is advisable for the contract to define an incident classification that takes particular account of:

- Business impact and continuity of operations (Business Impact)
- Scope and speed of incident propagation (Scope & Velocity)
- Legal impact, regulation and nature of the data (Compliance & Data Sensitivity)
- Threat actor context and motivation (Threat Actor Context)

When implementing the matrix in the contract, it is recommended to adopt a rule under which **the final incident severity is determined by the most severe indicator reached in any category**.

Contracts for DFIR services, or the associated SLAs, most commonly classify incident severity by level (for example critical, medium, high or low), linked to a description or characteristics of the incident (for example, an incident with an immediate impact on the organisation's operations or a high risk of serious damage). Once an incident severity level has been defined on the basis of those characteristics, it is essential to link the relevant factors to a recommended response time, i.e. **the maximum contractually guaranteed period within which the DFIR provider must begin taking active measures** from the moment the client officially reports the cyber incident. The contract may specify a simple response period (for example, within two hours) or provide a more detailed breakdown referring, for example, to availability, initial response and subsequently the commencement of analysis.

Defining response times in precise stages is more appropriate for the success of the forensic investigation and for legal certainty under the contract. A cyber incident within an organisation is a dynamic crisis in which seconds can determine the extent of damage and whether the evidentiary situation is preserved. If the response time were defined only as a single overall period, the provider could technically remain contractually compliant even if its internal teams spent the entire two hours merely coordinating logistics. A phased approach ensures that, while any physical transfer of experts to the incident site is being organised (**on-site response**), the remote team is already taking active measures in the first phase (**remote response**), such as isolating the network, blocking the attacker's command-and-control servers and stopping the spread of damage.

Protection of Confidential Information

As already stated in relation to the pre-contractual stage, disclosure of confidential information is an inherent part of DFIR services. The nature of such information means that unauthorised disclosure may cause not only financial loss, but also new security incidents, reputational damage or breaches of statutory obligations. **The contract should first contain a sufficiently precise definition of confidential information. A definition that is too narrow may leave certain categories of sensitive data without contractual protection, whereas an overly broad definition may create interpretative difficulties and uncertainty in contractual performance.** In a DFIR environment, it is recommended that the definition cover not only information expressly designated as confidential, but also all technical, organisational, operational, security, economic and legal information obtained during the provision of services, regardless of the form in which it is disclosed.

Personal Data Protection

Given the nature of DFIR services, the provider is often expected to have access to the client's information systems, electronic communications, security logs, backups, data repositories or digital evidence that may contain personal data relating to employees, customers, business partners or other natural persons.

The first step in preparing the contractual documentation should be to assess whether, and to what extent, personal data will be processed during the provision of the services. This is closely linked to determining the legal status of each contracting party. In most cases, the client will act as controller under Article 4(7) GDPR because it determines the purposes and grounds of the processing. The DFIR provider will generally act as processor under Article 4(8) GDPR and perform processing operations on the client's instructions. In certain cases, however, the legal status may differ, for example where the provider prepares an expert opinion or expert report or processes data on the basis of its own statutory obligation. If the provider acts as a processor, **a data processing agreement must be concluded** in accordance with the GDPR. The agreement must contain the elements required by Article 28 GDPR and should therefore clearly define the purpose of processing, the scope of processing operations, categories of personal data, categories of data subjects, duration of processing and the rights and obligations of both parties. Technical and organisational measures under Article 32 GDPR are also an important part of the contractual arrangements. The provider should maintain

security measures appropriate to the risks associated with the processing. Given the specialised nature of DFIR services, the use of subcontractors must also be addressed. In performing its obligations, the provider may use external experts, cloud services or specialised laboratories. The contract should therefore regulate the conditions of their involvement, the scope of data to which they may have access and the provider's responsibility for their activities. Personal data protection also includes provisions on cross-border transfers. Many forensic tools, cloud services or analytical platforms use infrastructure located outside the Slovak Republic or outside the European Economic Area. The contract should therefore clearly regulate whether transfers to third countries may occur, the legal basis for such transfers and the safeguards to be used to ensure compliance with Chapter V GDPR. The data processing agreement should also address retention and deletion of personal data after the end of the services and the handling of personal data security incidents.²

Handling of Digital Evidence

One of the key provisions in contracts for DFIR services concerns the handling of digital evidence. A contract governing DFIR services should therefore contain a separate section dedicated to digital evidence, as such material may subsequently be used in criminal, civil or administrative proceedings and often also contains personal data. General IT-service provisions are therefore insufficient; the contract must precisely define both the relevant terminology and the processes intended to preserve the legal usability and technical integrity of the evidence.

First, the contract **must clearly define what is considered digital evidence**. Without such a definition, uncertainty arises as to which data are subject to the DFIR provider's obligations and which outputs constitute evidentiary material. This category generally includes system and application logs, network records, disk and memory images, electronic communications and audit records from cloud environments. A precise definition is particularly important because it prevents disputes concerning the scope of responsibility and determines which data must be processed using forensic methods. The principal differences from traces in the physical world include:

- Intangibility;
- Latency;
- Temporal traceability;
- High information density;
- Recoverability;
- Originality;

² HUDECOVÁ, Irena – CYPRICHOVÁ, Anna – MAKATURA, Ivan et al. Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov/GDPR. Veľký komentár [Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data/GDPR. Major Commentary]. Volume 2. 2nd updated edition. Žilina: EUROKÓDEX, 2020

- Spatial characteristics;
- Encryption.

Another essential area is the manner in which digital evidence is acquired. The contract should provide that acquisition is performed in a forensically sound manner, for example, depending on the circumstances, by creating a bit-for-bit copy of the original data, while interventions in original systems and data are limited to what is necessary. Such an approach supports preservation of integrity and subsequent verifiability of the evidence. If the contractual documentation does not adequately regulate the acquisition and documentation of digital evidence, there is an increased risk that the method of acquisition, authenticity, integrity or evidentiary value will be challenged, potentially affecting its usability in the relevant proceedings.

Slovak law does not explicitly define uniform requirements for handling digital traces or impose a single set of specific requirements for all procedures or for the content of digital forensic analysis. From a legal perspective, the key requirement is that evidence be obtained and used in accordance with the rules applicable to the relevant proceedings. Breaches of the rules governing acquisition, securing or processing may lead to challenges to the lawfulness, authenticity, integrity or evidentiary value of the evidence and, depending on the applicable procedural regime, may also result in restrictions on or exclusion of its use.

In relation to the acquisition of digital evidence, as well as its subsequent securing and storage, **the Chain of Custody** is particularly important because it ensures traceability of every movement of and intervention in the evidence. The contract should require each item of evidence to be recorded from the moment it is acquired until it is archived or destroyed, including records of who handled the evidence, when and in what manner. This is decisive in practice because, where continuity of the chain of custody is missing, the evidence may readily be challenged as inauthentic or unverifiable.

In addition to preserving integrity and the chain of custody, it is necessary to ensure that the origin and lawful acquisition of digital evidence can be demonstrated. Depending on the nature of the service, the contractual documentation should therefore make it possible to retrospectively identify the data source, the manner and circumstances in which the data was obtained, the person or entity that provided it, and the legal or contractual basis authorising its acquisition and processing. This requirement is particularly important where outputs of the DFIR analysis are expected to be used subsequently in court or administrative proceedings (cf. judgment of the Supreme Administrative Court of the Slovak Republic, case No. 4Sfk/110/2022 of 24 April 2024).

Following from the above, the contract must also regulate **how evidence is stored and secured**. Evidence must be stored in an environment that protects it against unauthorised access, modification or deletion. This includes encryption, access-right management, separation of forensic storage from production systems and mandatory logging of all operations.

The analytical stage should also be regulated by the contract. Depending on the nature of the incident, the contract should require the analysis to be performed in a manner that minimises interference with the original data and, where possible and appropriate, on forensic copies. Significant procedures and interventions should be documented so that they can be reviewed and, to an appropriate extent, reproduced. This is fundamental for quality control because, in the event of a dispute, it must be possible to verify that the conclusions of the DFIR analysis are technically substantiated and independently verifiable. If these requirements are not adequately regulated and documented, the subsequent legal utility of the analysis results may be weakened.

Although personal data protection in DFIR contracts has already been addressed above, personal data contained in acquired and stored digital evidence must also be taken into account. The legal basis for processing must be identified, data minimisation ensured and the purpose of processing limited to handling the incident. Otherwise, there is a risk of GDPR infringement, which may lead to sanctions and liability for both contracting parties.

Understanding the principles governing the processing of digital evidence enables the contracting parties to structure the contractual terms more effectively, in particular the provisions concerning the handling of digital evidence. The basic principles include:

- **Evidence integrity** – interventions in original data should be limited to what is necessary and properly documented; where the nature of the incident permits, analytical operations should be performed on forensic copies.
- **Authenticity** – it must be demonstrable that the evidence originates from the declared source.
- **Auditability** – every action involving the evidence must be documented and retrospectively reconstructable.
- **Immutability** – original data should, to the greatest extent possible, be retained in a secure state protected against unauthorised modification; any necessary interventions must be documented.

When concluding a DFIR contract and drafting provisions concerning the handling of digital evidence, **the parties should also take into account applicable legislation and, where appropriate, relevant guidance or standards**. Guidance for specific activities involving digital traces is provided, for example, by the international technical standard **ISO/IEC 27037:2012**, Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence, issued by the International Organization for Standardization. The guidance in **ISO/IEC 27037** should be followed in investigations aimed at preserving the integrity, provenance and non-repudiation of digital traces and at applying methods for acquiring potential digital evidence that support its admissibility in criminal, civil, administrative or disciplinary proceedings, as well as in other relevant contexts. ISO/IEC 27037 does not, however, address the manner in which digital traces are analysed. Analysis and other processes associated with forensic science and the management of digital traces are partly

addressed in several technical standards, including **ISO 21043-2:2018** Forensic sciences – Part 2: Recognition, recording, collecting, transport and storage of items, which specifies requirements for the forensic process, particularly recognition, recording, collection, transport and storage of items of potential forensic value. It includes requirements for assessing and examining scenes and also applies to activities carried out within a facility. It also contains quality requirements.³

Liability for Damage

Liability is one of the most important parts of a contract for digital forensic analysis and cybersecurity incident response services. Given the nature of these services, which involve access to information systems, processing of sensitive data, handling of digital evidence and interventions in the client's production environments, failures by either party may have significant legal, financial, operational and reputational consequences.

The purpose of contractual liability provisions is **to establish a clear framework for determining the parties' rights and obligations in the event of damage, a security incident, breach of contractual obligations or other adverse events**. They also enable an appropriate allocation of risks between the client and the provider and help prevent disputes concerning the extent of liability for the resulting consequences.

When preparing a DFIR contract, it should be recognised that the provider often operates in an environment that has already been compromised or affected by a security incident. The mere existence of an incident therefore does not automatically make the provider liable for the resulting damage. The extent of its liability must be assessed by reference to its specific contractual obligations and the activities actually performed.

General Liability for Contractual Performance

Each contracting party is responsible for proper performance of its obligations under the contract. The provider is required to perform the services with professional due care and in accordance with current knowledge in digital forensics, cybersecurity and incident response. The client, in turn, is required to provide the necessary cooperation, ensure access to relevant systems and provide accurate and complete information necessary for the services.

The contract should clearly state that **the provider is responsible for the professional performance of the agreed activities, but not for circumstances outside its control**, such as incomplete data supplied by the client, hidden technical deficiencies in the client's environment or consequences of incidents that arose before the services commenced.

In the DFIR environment, it is particularly important **to distinguish liability for the performance of the services from responsibility for the outcome of the investigation**. The

³ Cf. MAKATURA, Ivan. Ciele dokazovania v kybernetickej bezpečnosti [Objectives of Proving in Cyber Security]. In: Acta Facultatis Iuridicae Universitatis Comenianae, 2023, Vol. 42, No. 1, pp. 116–146.

provider may perform all necessary steps with professional due care, but because of the nature of digital evidence it may not always be possible to identify the perpetrator of an incident conclusively or recover all lost data.

The provider should therefore bear liability for damage caused by breach of its contractual or statutory obligations. This may include, in particular, situations where it:

- intervenes in systems without the necessary authorisation,
- breaches agreed security procedures,
- discloses confidential information without authorisation,
- fails to protect data obtained,
- breaches obligations relating to personal data processing,
- fails to preserve the integrity of digital evidence,
- uses inappropriate or disproportionate forensic procedures,
- fails to comply with agreed SLA parameters.

The provider's liability should nevertheless be assessed in light of the nature of the services. DFIR services often involve activities performed under time pressure, with incomplete information and in an environment affected by a security incident. Liability should therefore be assessed in the context of the circumstances of the particular case and the professional standards applicable at the time of the intervention.

Client Liability

The contractual arrangements should address not only the provider's liability but also the client's responsibility for performing its obligations. In practice, the success of an investigation or incident response is often significantly affected by the quality of the client's cooperation.

The client may be responsible in particular for:

- providing incomplete or inaccurate information,
- failure to provide the necessary cooperation,
- late reporting of an incident,
- failure to provide access to systems or data,
- failure to follow recommended security measures,
- failure to perform obligations arising from the contract,
- unauthorised interference with the environment under investigation during the analysis.

If an act or omission by the client makes the provision of services impossible or substantially more difficult, the contract should provide for the possibility of limiting or excluding the provider's liability for consequences arising as a result.

Liability for the Protection of Confidential Information

The provision of DFIR services involves the processing of large volumes of sensitive information, including trade secrets, internal documents, security measures, vulnerability information and the results of incident investigations.

The contract should regulate liability for breach of confidentiality obligations and unauthorised disclosure of confidential information. The arrangements may include an obligation to compensate for damage, notify a security incident or take remedial measures to minimise its consequences. In practice, however, liability for breaches relating to confidential information is often regulated separately in the Non-Disclosure Agreement referred to above.

Liability for Personal Data Protection

If the provision of services involves the processing of personal data, the contract should regulate the allocation of responsibility between the controller and the processor in accordance with the applicable legislation.

The provider may be liable for breaches of obligations relating to personal data processing, in particular where it:

- processes data beyond the client's instructions,
- fails to ensure adequate protection of the data,
- discloses data to third parties without authorisation,
- fails to protect data against loss or misuse,
- breaches obligations arising from personal data protection legislation.

At the same time, the client remains responsible for the lawfulness of the processing itself and for correctly identifying the legal bases for processing personal data. Liability for personal data protection breaches is, however, often regulated, as in the case of confidentiality breaches, in a separate data processing agreement.

Limitation of Liability

In commercial practice, contracts commonly contain provisions limiting the extent of the parties' liability for breach of their obligations. In the case of DFIR services, however, any such limitation must be proportionate and must not conflict with mandatory provisions of applicable law.

The contract may regulate, for example:

- a maximum amount of compensation for damage,
- exclusion of liability for indirect damage,
- exclusion of liability for loss of profit,
- limitation of liability for damage caused by third parties,
- limitation of liability for force majeure events.

When setting such provisions, the value of the services, the degree of risk and the scope of the provider's access to the client's systems should be taken into account.

Liability Insurance

Given the potential consequences of security incidents and the high value of the information processed, it is recommended that the provider maintain adequate liability insurance.

The contract may regulate:

- the minimum amount of insurance coverage,
- the obligation to demonstrate that insurance is in place,
- the obligation to maintain insurance throughout the term of the contract,
- notification of changes to or termination of insurance coverage.

Although insurance does not replace the provider's liability, it is an important risk-management instrument for both contracting parties.

In practice, situations also arise in which the client itself already has cyber insurance. If the client has cyber insurance in place, it is therefore advisable to take this into account when preparing the contractual documentation. Many insurance policies contain specific requirements concerning the handling of cyber incidents, failure to comply with which may lead to a reduction or refusal of insurance coverage. The contractual documentation should therefore contain provisions enabling the insurer's requirements to be met. The client should be required to inform the provider of the existence of cyber insurance and of any relevant policy terms that may affect the provision of services. This is important because the provider may not be aware that the insurer requires a specific investigation procedure, the use of an approved vendor or compliance with particular deadlines. If the provider is unaware of those requirements, it may inadvertently cause a breach of the insurance terms. The contract should regulate the extent of the provider's cooperation in communications with the insurer and in preparing the materials required for settlement of the insured event, because insurers generally require expert documentation demonstrating the occurrence and extent of the insured loss.

Contractual Penalties and Sanctions

To secure performance of contractual obligations, the contract may also provide for contractual penalties or other sanction mechanisms.

These may be linked in particular to:

- breach of confidentiality obligations,
- unauthorised handling of data,
- breach of SLA parameters,
- failure to comply with security requirements,
- unauthorised use of subcontractors,
- delay in performing contractual obligations.

When setting contractual penalties, the principle of proportionality should be observed. The amount of the penalty should correspond to the significance of the breached obligation and the potential consequences of the breach. Disproportionately high penalties may be problematic in practice and may lead to disputes between the parties.

In addition to contractual penalties, it is advisable to regulate the relationship between the contractual penalty and compensation for damage. The parties should clearly determine whether payment of a contractual penalty extinguishes the claim for damages or whether damages may also be claimed beyond the amount of the penalty paid. In DFIR services, it is generally advisable to preserve the possibility of claiming damages in addition to the contractual penalty, particularly where the breach causes damage exceeding the agreed penalty.

A balanced approach is recommended when setting sanction mechanisms. Sanctions should not be directed unilaterally only against the service provider. The client's conduct may also significantly affect the provider's ability to perform its contractual obligations, for example by failing to provide necessary cooperation, withholding relevant information or interfering without authorisation with the environment under investigation. In justified cases, sanction mechanisms linked to breaches of the client's obligations may therefore also be considered.

For SLA parameters, **service credits** or contractual penalties for failure to meet guaranteed response times are often used in practice. Their purpose is not to penalise the provider for every minor delay, but to create a compensation mechanism where non-compliance with agreed parameters may negatively affect the client's ability to respond effectively to an incident.

Importance of Liability Provisions in DFIR Contracts

Precise liability provisions are one of the fundamental tools for managing legal and operational risks in the provision of DFIR services. They make it possible to allocate responsibility transparently between the client and the provider, create a predictable framework for dealing with loss events and increase legal certainty for both parties.

Given the sensitivity of the information processed, the importance of digital evidence and the potentially serious consequences of security incidents, liability should be regulated in detail, clearly and with due regard to the specific features of digital forensic analysis and cybersecurity incident response.

Liability for Digital Evidence

Particular attention should be paid to liability for digital evidence, which is one of the most specific aspects of DFIR services. Digital evidence may be decisive in internal investigations, disciplinary proceedings, civil disputes, administrative proceedings or criminal proceedings.

The provider should be responsible for preserving:

- the authenticity of the evidence,
- the integrity of the evidence,
- the demonstrability of the evidence's origin,
- a continuous Chain of Custody,
- secure storage of evidentiary material.

If any of these principles is compromised, the evidence may be challenged or completely excluded from the evidentiary process. The consequences of such a failure may have a significant impact on the client's legal position.

Price and Payment Terms

The price for DFIR services is one of the basic elements of the contract. Given the specific nature of these services, however, the remuneration structure is often more complex than for ordinary IT services. The complexity of individual incidents, their scope, urgency and the need to deploy specialised experts may significantly affect the total cost of the services provided.

The contract should therefore clearly regulate how the price is determined and all circumstances that may affect its adjustment. The price may be set as:

- a one-off fee for a specific service or project,
- an hourly rate for work performed,
- a fixed monthly fee,
- a combination of a fixed fee and hourly billing,
- a retainer model ensuring the preparedness of the incident-response team,
- remuneration linked to the scope or severity of the incident.

Particular attention should be paid to situations in which the scope of an incident cannot be predicted in advance. In such cases, it is advisable to regulate mechanisms for approving work beyond the originally agreed scope and the manner in which the client is informed of the expected increase in costs.

Payment terms should regulate, in particular, invoice maturity, invoicing procedures, conditions for advance payments, reimbursement of travel and other incidental expenses, billing conditions for on-call services and the billing regime for work performed outside standard working hours.

For long-term contracts, it is also advisable to regulate price-indexation mechanisms or conditions for changing remuneration in the event of a significant change in the scope of services.

Duration and Termination of the Contract

Provisions governing the duration and termination of a contract are fundamental elements of any contractual relationship. In contracts for digital forensic analysis and cybersecurity

incident response services (DFIR), however, they are particularly important because the services often involve sensitive information, security incidents, digital evidence and access to the client's information systems.

Properly structured duration and termination provisions ensure legal certainty for the contracting parties, continuity of services and prevention of situations that could jeopardise information-system security or the integrity of an ongoing investigation. The contract should therefore clearly regulate the commencement of the contractual relationship, its duration, the options for termination and the rights and obligations of the parties after cooperation ends.

The contract should precisely determine **when the contractual relationship begins and when the contract becomes effective**. In practice, the date of signature does not necessarily coincide with the date on which services commence.

Particularly in the case of DFIR services, the effectiveness of the contract may be conditional upon fulfilment of additional conditions, such as:

- signing a non-disclosure agreement,
- entering into a data processing agreement,
- performing an initial security audit,
- granting access rights,
- designating contact persons,
- completing the onboarding process.

A clear determination of the start of the contractual relationship is important in particular for assessing the parties' liability, the commencement of SLA time limits and the provider's entitlement to remuneration.

Both basic models of contract duration are used for DFIR services. **Fixed-term contracts** are used primarily for one-off projects such as forensic investigations of a specific incident, analysis of system compromise, expert opinions or specialist services. The duration of the contract is usually linked to achievement of a specific objective or delivery of defined outputs.

If the contract is concluded for a fixed term, it is recommended to regulate the conditions for any extension. In practice, automatic renewal is often used unless one of the parties gives notice within a specified period that it wishes to terminate the contract.

For DFIR services, it is advisable for any contract extension to be linked to a review of the current technical and security requirements, contact details, SLA parameters and scope of services. This ensures that the contract reflects the current state of the client's information environment.

By contrast, **contracts for an indefinite term** are generally used for long-term cooperation, particularly for incident-response retainer services, forensic-readiness services, ongoing monitoring of security events or specialised security support.

As regards **termination of the contractual relationship**, one standard method is termination **by notice**. The contract should clearly regulate the parties' right to give notice, the grounds for notice and the length of the notice period. For long-term DFIR services, the notice period should be set so as to allow safe termination of the cooperation, handover of documentation and implementation of necessary security measures. An excessively short notice period may jeopardise continuity of security services and increase the risk of incidents. Particular attention is required where a security incident is being handled at the time notice is given. In such cases, it is recommended to regulate the provider's obligation to complete activities already commenced or ensure an appropriate handover of the case to another entity.

Another method of ending the contractual relationship is withdrawal from the contract. **Withdrawal** is an extraordinary method of termination and is generally used in the event of a serious breach of contractual obligations.

The contract should list the circumstances giving rise to a right of withdrawal. These may include, in particular:

- a serious breach of confidentiality obligations,
- unauthorised disclosure of information to third parties,
- repeated breaches of SLA parameters,
- a serious breach of security obligations,
- a breach of personal data protection obligations,
- failure by the client to provide necessary cooperation,
- delay in payment for the services,
- loss of professional authorisations or certifications necessary for the provision of the services.

It is also recommended to regulate the obligation to provide the other party with an appropriate period to remedy an identified breach where the nature of the breach permits this.

One of the specific features of DFIR contracts **is the possibility that the contractual relationship may end while a security incident is still being handled**. Such a situation may represent a significant security risk and may adversely affect the investigation or implementation of remedial measures.

For this reason, the contract should regulate a special termination regime applicable during an incident. It is advisable to provide that the provider will complete at least the minimum necessary actions aimed at stabilising the situation or ensure proper handover of all relevant

information to the client or a new service provider. Such arrangements help preserve continuity of the investigation and minimise security risks.

Termination of the contractual relationship does not generally extinguish all rights and obligations of the parties. **In the case of DFIR services, many obligations remain relevant after the services have ended.**

The contract should regulate in particular:

- revocation of the provider's access rights,
- termination of remote connections and technical access,
- return or handover of documentation,
- handover of analysis results and final reports,
- handover of digital evidence and forensic copies,
- deletion or anonymisation of data,
- the method for disposal of backups and working copies,
- continuation of confidentiality obligations after the contract ends.

Particular attention should be paid to digital evidence that may be required for future court, administrative or criminal proceedings. After the services end, the provider should hand over to the client all outputs created in performing the contract. These may include in particular:

- forensic reports,
- technical analyses,
- records of actions performed,
- logs and evidence obtained,
- recommendations for remedying identified deficiencies,
- Chain of Custody documentation,
- outputs from the tools used.

The contract should regulate the form of handover, the manner in which data integrity is ensured and any conditions for the provider's continued retention of copies.

The contract should also distinguish the obligation to preserve potentially relevant digital evidence from the general retention of all acquired data. Retention and disposal rules should specify which data are retained, for how long, under what conditions deletion may be temporarily suspended because of pending or anticipated proceedings, and how deletion or destruction is documented. In subsequent proceedings, it may also be relevant which original records were preserved or destroyed and for what reason (cf. judgment of the Regional Court in Bratislava, case No. 3To/55/2019 of 17 September 2019).

In addition, **certain contractual provisions should survive termination of the contract.** These include, in particular, provisions concerning:

- protection of confidential information,
- personal data protection,
- handling of digital evidence,
- liability for damage,
- dispute resolution,
- protection of intellectual property rights.

The duration of these obligations should be clearly specified in the contract; in the case of confidentiality obligations, it is often advisable for them to remain effective for several years after the contractual relationship ends.

Careful regulation of contract duration and termination is an important tool for managing legal and security risks. It helps ensure continuity of services, protection of sensitive information, proper revocation of access to information systems and preservation of the integrity of digital evidence.

In digital forensic analysis and cybersecurity incident response, this part of the contract is particularly important because improperly or incompletely regulated termination may lead to loss of evidence, disruption of an investigation or the occurrence of additional security incidents. For this reason, duration and termination provisions should be regarded as a key component of every DFIR contract.

Dispute Resolution

Even with a carefully prepared contract, disputes between the client and the service provider cannot be completely excluded. In DFIR services, disputes may arise in particular in relation to the scope of services performed, evaluation of security incidents, compliance with SLA parameters, liability for damage or the amount of remuneration.

The contract should therefore **contain dispute-resolution mechanisms and define the procedure** to be followed by the parties before formal court proceedings are commenced. It is recommended to regulate in particular:

- the parties' obligation to attempt an amicable resolution of the dispute,
- internal escalation mechanisms,
- time limits for discussing disputed matters,
- the possibility of mediation,
- the possibility of obtaining an independent expert assessment,
- the governing law,
- jurisdiction of courts or arbitral tribunals.

In international contracts, the governing law and jurisdiction must be determined unambiguously because differences between legal systems can significantly affect the parties' rights and obligations. In disputes involving technical issues, it may be appropriate to provide for an independent expert report or expert opinion before court proceedings are commenced.

Contractual Regulation of DFIR Service Outputs

Outputs are one of the most important elements of the contractual relationship in the provision of DFIR services. They are the means through which the purpose of the contract is fulfilled, because they provide the client with information about the security incident, its causes, course, consequences and recommendations for remedial measures. Unlike many other information-technology services, however, **DFIR outputs are not merely technical in nature**. They often have significant legal, organisational, security and economic consequences. They may be used in internal investigations, in asserting claims against employees or suppliers, in communications with regulatory authorities or insurers, or as evidence in court and administrative proceedings. Their contractual regulation therefore requires particular attention.

A fundamental prerequisite for effective contractual regulation is **a precise definition of the outputs that the provider is to deliver to the client**. In practice, the subject matter of the contract is often defined relatively generally, for example as "provision of digital forensic analysis services" or "*handling of security incidents*", without a specific description of the results the client is to receive at the end of the process. This may lead to disputes over the scope of performance, the quality of delivered outputs or fulfilment of contractual obligations. The contract should therefore include, already in its introductory provisions, a list of outputs to be provided for the individual types of services.

Several categories of outputs can be identified in DFIR services. The first group consists of **operational or interim outputs produced** while the incident is being handled. Their purpose is to keep the client continuously informed of the current status of the incident and the measures taken. They include, in particular, situation reports, progress reports on the intervention, interim analyses or alerts concerning critical findings. The contract should specify **the frequency with which these outputs are provided, the communication method and the persons authorised to receive the information**. For serious incidents, it may be appropriate to require regular updates at defined intervals or when pre-defined milestones are reached.

The second category consists of **preliminary analytical reports**. These documents are usually **prepared shortly after the investigation begins and are intended to provide the client with a basic overview of the situation**. They typically include information on the nature of the incident, the presumed method of system compromise, the scope of affected assets and a preliminary risk assessment. Because the investigation may not yet be complete at this stage, the contract should expressly state that these are preliminary findings that may be supplemented or refined during later stages of the investigation.

The key output of most DFIR services is **the final forensic report**. It is **a comprehensive professional document summarising the entire investigation**. To ensure consistent quality, the contract should specify minimum content requirements. The report should include identification of the incident, a description of methodologies and tools used, a list of systems

and data sources analysed, a chronological account of the incident, identified vulnerabilities, a description of detected attacker activity, a list of secured evidence and expert conclusions. It should also include recommendations for remedying identified deficiencies and preventing similar incidents in the future.

The provider's final forensic or technical report should be distinguished from an expert opinion prepared under specific legislation governing court-appointed experts. This does not, however, preclude its use as a professional basis or as evidence in particular proceedings where the applicable procedural rules permit. The contract should therefore emphasise the specificity, completeness and reviewability of the report, identification of data sources and procedures used, and the ability to verify its conclusions (cf. judgment of the Regional Court in Košice, case No. 6S/115/2018 of 3 June 2021).

Digital evidence as **a separate type of output also requires particular attention**. Unlike analytical reports, it does not represent an interpretation of findings, but the data itself obtained during the investigation. This may include forensic images of hard drives, copies of logs, network-communication records, contents of volatile memory, database exports or other electronic data. Because such evidence may be used in legal proceedings, the contract must regulate in detail the conditions for its acquisition, storage and transfer. It is recommended to require documentation of the entire evidence-handling process through a Chain of Custody, i.e. records of all persons who handled the evidence and all actions performed.

Where derivative materials such as transcripts, exports, screenshots, tables or analytical summaries are created from original digital data, the contract should, depending on the nature of the service, also regulate preservation of the original source data or a forensic copy so that the origin, accuracy and completeness of the derivative output can subsequently be verified. A derivative output alone may not be sufficient in subsequent proceedings if it cannot be verified against the original record (cf., in the context of the assessment of audiovisual recordings and their transcripts, order of the Regional Court in Košice, case No. 4To/106/2021 of 17 June 2022).

The contract should also address the **form of the outputs**. In practice, outputs may need to be delivered in different formats and on different media. Forensic reports are usually supplied as electronic PDF documents, whereas digital evidence may be delivered on encrypted external storage media or through secure data repositories. The contract should include requirements for encryption, recipient authentication and confirmation of receipt of the outputs.

An important issue is **the determination of deadlines for delivery of individual outputs**. Time is critical when dealing with cybersecurity incidents. In the event of a security incident, the client may require analysis results within hours or days, for example in order to comply with reporting obligations under personal data protection or cybersecurity legislation. The contract

should therefore distinguish between deadlines for interim information, preliminary reports and final outputs.

The contractual arrangements should also address **ownership and usage rights in the outputs**. In the case of forensic reports, the client is generally expected to receive the right to use the documents for the protection of its rights and interests. At the same time, it may be necessary to regulate the provider's rights in its own methodologies, procedures or analytical tools used to produce the outputs. If the provider intends to use acquired data or knowledge for research purposes, creation of datasets, testing or improvement of analytical tools, development of new detection mechanisms or creation of threat databases, this possibility must be expressly regulated by the contract. The contract should determine the scope of such further use, conditions for anonymisation or other appropriate modification of the data, protection of personal data, confidential information and trade secrets, and rules for handling data after the contractual relationship ends.

Protection of confidential information is particularly important. DFIR outputs often contain detailed information about the client's technical infrastructure, security measures, identified weaknesses and, in some cases, personal data of employees or customers. The contract should therefore contain **strict rules on confidentiality, access to outputs, retention and further dissemination**. It is also advisable to specify which persons are authorised to handle the outputs and under what conditions they may be disclosed to third parties.

When regulating outputs contractually, **their potential future evidentiary use should also be considered**. Where it is anticipated that outputs may be used in administrative, civil or criminal proceedings, the contract should require compliance with internationally recognised forensic standards, in particular the recommendations published by the National Institute of Standards and Technology in NIST SP 800-86 or the ISO/IEC 27037, ISO/IEC 27041 and ISO/IEC 27042 standards. Compliance with these standards significantly increases the credibility of the results and minimises the risk of challenge.

From the perspective of this methodology for concluding DFIR contracts, outputs should not be regarded merely as the technical result of the service. They are also legally relevant documents, carriers of digital evidence and sources of information necessary for the client's further decision-making. Their contractual regulation should therefore be detailed and unambiguous and should cover not only their content and form, but also ownership, protection, confidentiality, evidentiary usability, the manner of delivery and the conditions of any further use. A contractual framework structured in this manner makes a significant contribution to legal certainty for the parties and to effective handling of cybersecurity incidents.

Specific Requirements for Contractual Relationships in the Financial Sector (DORA Regulation)

If the client is a financial entity (for example, a bank, insurance undertaking, management company or investment firm), the conclusion of contractual relationships for DFIR services may be subject to specific requirements under Regulation (EU) 2022/2554 of the European

Parliament and of the Council on digital operational resilience for the financial sector (DORA). For other entities involved in the supply chain of a financial entity, the applicability of these requirements must be assessed according to the entity's specific position and contractual relationship.

When entering into a contract with a financial entity, the first step is to assess whether the DFIR services constitute information and communication technology services within the meaning of DORA. In most cases, digital forensic analysis and incident response will fall within the definition of ICT services under Article 3(21) DORA. This is fundamental to the content of the contract because DORA requires financial entities to have contracts with external providers that contain precisely specified mandatory elements.

If Incident Response or digital forensic analysis services support a critical or important function of a financial entity, the contractual relationship must also take into account the additional DORA requirements applicable to such services. In that case, in addition to the general elements required by Article 30(2), the contract must contain the additional contractual elements required by Article 30(3) DORA.

A contract between a financial entity and a DFIR service provider must clearly regulate the rights and obligations of both parties and should **be in writing**. It should also include agreed service levels (SLAs) defining the expected quality, availability and parameters of the services.

A basic prerequisite for compliance with DORA is **a precise definition of the subject matter of the services**. The contract should contain a detailed description of all DFIR services provided, including the scope of digital forensic analysis, incident response, collection and processing of digital evidence, malware analysis, support with incident reporting and preparation of professional reports. **If subcontractors are expected to be involved, the conditions governing their use and the scope of activities they may perform must be clearly defined.**

Particular attention should be paid to **the location of the services and the data processed**. The financial entity must have an overview of where data will be analysed, stored or backed up. The provider should be required to inform the client of any planned change in the location of data processing or transfer of services to another country or data centre. This requirement is particularly important when cloud solutions are used.

The contract must also **regulate data protection and security measures**. The DFIR provider should ensure an appropriate level of confidentiality, integrity, availability and authenticity of the data processed. Where personal data is involved, compliance with the GDPR and other relevant legislation must be ensured. The contract should include rules on encryption, management of access rights, activity logging and protection of digital evidence.

An important contractual requirement is ensuring access to data and its return to the client. The provider must be able to hand over to the financial entity all data processed, including digital evidence, logs, forensic images and analytical outputs, in a usable and commonly

available format. This obligation must also be secured in the event of termination of the contract, cessation of the provider's business activities or the provider's insolvency.

For DFIR services, the obligation to provide assistance in handling incidents is particularly important. **The provider should be contractually required to assist the client without undue delay in investigating a security incident, provide professional support, analyse the events and supply information necessary for compliance with reporting obligations to regulatory authorities.** It is recommended that the contract specify response times, incident-escalation procedures and the form of communication during the incident.

A specific DORA requirement is **cooperation with supervisory and regulatory authorities**. The DFIR provider should be prepared to provide assistance not only to the client but also to supervisory authorities where necessary for an incident investigation or regulatory inspection. This obligation should be expressly included in the contract.

If the DFIR services support critical or important functions of the financial entity, the contractual requirements are further expanded. In that case, **qualitative and quantitative service indicators, including precisely measurable performance targets, should be defined in detail.** The financial entity must be able to monitor compliance with these parameters on an ongoing basis and require remediation in the event of non-compliance.

The contract should also regulate **the provider's obligations concerning business continuity and crisis management.** The provider should maintain its own business-continuity and incident-recovery plans and regularly test their effectiveness. It should also be required to implement appropriate technical and organisational security measures corresponding to the importance of the services provided.

Audit rights of the financial entity are an important element required by DORA. The client must be able to verify the manner in which services are provided, monitor compliance with security requirements and audit the provider. Equivalent rights must also be secured for the competent supervisory authorities. The provider should be required to supply the necessary documentation, permit inspections and provide cooperation during audits or inspections.

An exit strategy must also be an integral part of the contract. It should ensure that termination of the cooperation does not adversely affect the financial entity's operations. During an agreed transition period, the provider should continue to provide the services and ensure the handover of all data, documentation and outputs necessary for transfer to another provider or for the financial entity itself to take over the activities.

When preparing DFIR contracts in the financial sector, the contract should therefore be regarded not only as a commercial instrument governing the provision of services, but also as a key element of the financial institution's digital operational resilience framework. Careful consideration of DORA requirements significantly contributes to protecting the financial

entity, increases legal certainty for the contracting parties and supports effective handling of cybersecurity incidents.⁴

4 Overview

The methodology systematises the conclusion of contractual relationships for DFIR services into two consecutive stages. The pre-contractual stage focuses primarily on identifying the client's needs and objectives, preliminary analysis of its environment, verification of the provider's competence, protection of confidential information and assessment of personal data processing. The contract-conclusion stage covers selection of an appropriate contractual model, definition of the subject matter and scope of authorisations, SLA and response-time arrangements, protection of information and personal data, handling of digital evidence, liability for damage, price, duration and termination, dispute resolution and regulation of outputs. The following diagrams summarise the recommended procedure in both stages.

⁴ Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA Regulation).

PRE-CONTRACTUAL PHASE IN THE PROVISION OF DFIR SERVICES

The pre-contractual phase is crucial for properly establishing the contractual relationship, minimizing risks and ensuring that cooperation is legally sound, effective and compliant with technical and regulatory requirements.



i Thorough completion of the pre-contractual phase reduces the risk of misunderstandings, unauthorized access and breaches of legal requirements, and ensures effective incident response.

Diagram 1: Steps in the Pre-contractual Stage

PROCEDURE FOR CONCLUDING A LEGALLY SOUND AND EFFECTIVE DFIR AGREEMENT

Goal: to ensure legal certainty, data protection, effective cooperation, and evidentiary value.



1) WHAT THE CLIENT SHOULD DO / CONSIDER BEFORE CONCLUDING THE CONTRACT

STEP	WHAT TO PREPARE/ADDRESS	WHY
NEEDS & RISK ANALYSIS	Identify incident types, critical systems and data, define desired response and forensic outputs.	Ensure the contract covers real needs and risks.
PROVIDER ASSESSMENT	- Verify DFIR experience, references, certifications (e.g., CREST, ISO 27037). - Assess technical capacity, tools, and methodologies. - Evaluate financial stability and insurance coverage.	Minimize risk of provider failure and ensure a professional approach.
LEGAL & REGULATORY ASSESSMENT	- Verify compliance with legislation (GDPR, Cybersecurity Act, other applicable law). - Consider cross-border data transfers. - Assess the need for a DPA (if the provider is a data processor).	Ensure legal data processing and prevent sanctions.
TECHNICAL PREPARATION	- Ensure logging and log retention. - Provide access and resources for the DFIR team. - Consider tool compatibility and forensic readiness.	Enable fast and effective response without unnecessary delays.
INTERNAL APPROVALS & BUDGET	- Obtain approval from management and legal department. - Secure budget (including potential extra costs). - Verify alignment with internal policies and processes.	Prevent internal risks and ensure cooperation support.
CRISIS SCENARIO PREPARATION	- Define contact persons and communication channels. - Prepare communication plan (internal and external). - Prepare escalation plan.	Ensure coordinated response and minimize chaos during an incident.

2) WHAT THE CONTRACT SHOULD REGULATE (KEY AREAS) AND WHY

CONTRACT AREA	WHAT TO PREPARE/ADDRESS	WHY
SUBJECT & SCOPE OF SERVICES	Precise scope of DFIR services (incident response, forensic analysis, reporting, consulting). What is included / what is out of scope.	Prevent ambiguities and disputes over service scope.
AVAILABILITY & SLA	- Response times, availability (24/7) - SLA metrics and measurement method.	Ensure expected service level and measurable outputs.
ACQUISITION & HANDLING OF DIGITAL EVIDENCE	- Method of acquisition (forensically sound procedure) - Hashing, chain of custody, storage, transfer, destruction - Use of evidence only for incident purpose.	Ensure evidentiary value and data integrity.
DATA PROTECTION (GDPR)	- Role of parties (controller / processor) - Processing instructions, security measures - Subcontractors, non-disclosure, rights of data subjects	Ensure GDPR compliance and minimize legal risks.
LIABILITY FOR DAMAGE	- Division of liability between parties - Caps on liability, exclusions (indirect damage, lost profit) - Exceptions (intent, gross negligence)	Protect both parties from disproportionate financial risks.
CONFIDENTIALITY & SECURITY	- Non-disclosure obligation (NDA), access rights - Physical and environmental security - Information security measures	Protect sensitive information and trust.
SUBCONTRACTORS	- Possibility of using subcontractors - Approval process, liability, identical obligations	Ensure control over third parties.
PAYMENT TERMS	- Remuneration (flat fee / hourly rate / retainer) - Invoicing, due date, extra costs	Prevent financial ambiguities.
CONTRACT TERMINATION	- Termination conditions, withdrawal - Handover / return of data and evidence - Deletion or archiving	Govern the end of cooperation and data protection.
DISPUTE RESOLUTION & APPLICABLE LAW	- Applicable law and jurisdiction - Dispute resolution mechanism (mediation / arbitration / court)	Enable effective resolution of potential disputes.

KEY PRINCIPLES OF A SUCCESSFUL CONTRACT

LEGACITY & COMPLIANCE Compliance with law and internal policies.	CLARITY Precise definitions, scope, and expectations.	BALANCE Fair distribution of rights and obligations.	SECURITY & EVIDENTIARY VALUE Protection of data and integrity of digital evidence.	FLEXIBILITY & REVIEW Ability to adjust to evolving risks and technologies.
--	---	--	--	--

Diagram 2: Procedure during the Contractual Stage

5 References

Literature and Professional Sources

BAJTOŠ, Tomáš – SOKOL, Pavol – BAČO, Ladislav. Digitálna forenzná analýza I [Digital Forensic Analysis I]. Košice: Pavol Jozef Šafárik University in Košice, 2020. Available at: <https://unibook.upjs.sk/img/cms/2020/pf/digitalna-forenzna-analyza-1.pdf>

HUDECOVÁ, Irena – CYPRICHOVÁ, Anna – MAKATURA, Ivan et al. Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov/GDPR. Veľký komentár [Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data/GDPR. Major Commentary]. Volume 2. 2nd updated edition. Žilina: EUROKÓDEX, 2020.

KENT, Karen – CHEVALIER, Suzanne – GRANCE, Tim – DANG, Hung. Guide to Integrating Forensic Techniques into Incident Response. NIST Special Publication 800-86. Gaithersburg: National Institute of Standards and Technology, 2006.

MAKATURA, Ivan. Ciele dokazovania v kybernetickej bezpečnosti [Objectives of Proving in Cyber Security]. In: Acta Facultatis Iuridicae Universitatis Comenianae, 2023, Vol. 42, No. 1, pp. 116–146.

OLEJÁR, Daniel et al. Základy kybernetickej a informačnej bezpečnosti [Fundamentals of Cybersecurity and Information Security]. 1st edition. Bratislava: Comenius University Bratislava, 2020.

SELINŠEK, Liljana. Některé právní aspekty forenzní analýzy digitálních dat [Selected Legal Aspects of Forensic Analysis of Digital Data]. In: Acta Universitatis Carolinae – Iuridica, 2008, No. 4, pp. 131–140.

Technical Standards

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements.

ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence.

ISO/IEC 27041:2015 Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method.

ISO/IEC 27042:2015 Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence.

ISO/IEC 27043:2015 Information technology – Security techniques – Incident investigation principles and processes.

ISO 21043-2:2018 Forensic sciences – Part 2: Recognition, recording, collecting, transport and storage of items.

Case Law

Judgment of the Supreme Administrative Court of the Slovak Republic, case No. 4Sfk/110/2022 of 24 April 2024, ECLI:SK:NSSSR:2024:6021200033.1.

Judgment of the Regional Court in Košice, case No. 6S/115/2018 of 3 June 2021, ECLI:SK:KSKE:2021:7018200828.2.

Judgment of the Regional Court in Bratislava, case No. 3To/55/2019 of 17 September 2019, ECLI:SK:KSBA:2019:1518010031.1.

Order of the Regional Court in Košice, case No. 4To/106/2021 of 17 June 2022, ECLI:SK:KSKE:2022:7217010310.2.

Judgment of the Regional Court in Košice, case No. 4Cob/46/2024 of 23 April 2025, ECLI:SK:KSKE:2025:6123373185.1.

Judgment of the Administrative Court in Bratislava, case No. BA-1S/83/2020 of 29 October 2025, ECLI:SK:SpSBA:2025:1020200456.1.