

D10 – ADFIR Project Communications Toolkit



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.

Content

1 Project Description	3
2 Introduction	3
2.1 Purpose of the Communications Toolkit	3
2.2 Basis and Link to KPB1.6 and D7	3
2.3 Users and Scope of the Toolkit.....	4
3 ADFIR Project Communications Toolkit.....	4
3.1 Project Identity and Mandatory Communication Elements	4
3.2 Key Messages and Standard Project Descriptions.....	6
3.3 Language, Terminology and Communication Style	8
3.4 Templates for Communication Channels	9
3.4.1 Website article / news item	9
3.4.2 Social media	10
3.4.3 Press release and media release	10
3.4.4 Invitation to a workshop, conference or event	11
3.4.5 Newsletter / information e-mail	11
3.4.6 Presentations	12
3.4.7 Brochures, posters and leaflets	12
3.4.8 Policy brief / recommendation for policymakers	12
3.5 Communication Preparation and Approval Process.....	13
3.6 Recording Communication Activities	14
4 Overview.....	14
5 Ready-to-Use Text Templates	16
5.1 Standard Project Boilerplate	16
5.2 Standard Funding Wording	16
5.3 Short Text for Social Media	16
5.4 Short Text for an Event	16
5.5 Closing Text for a Presentation	16
6 Basis and Related Project Documents	17

1 Project Description

The Automation of Digital Forensic and Incident Response (hereinafter “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. The project addresses one of the key challenges in cybersecurity and information security – how to efficiently process large volumes of digital evidence generated during cybersecurity incidents or forensic investigations. Automation using data analytics and machine learning methods can support the quality of digital forensic analysis and reduce the time required to perform it. 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.
- Reduced workload for forensic analysts. Routine and time-consuming tasks can be supported by automated methods, allowing experts to focus on more complex cases and decision-making.
- Higher quality and consistency of outputs. Common methodologies and tools are intended to support more accurate, consistent and verifiable processing of digital traces.
- Potential use in criminal and other legal proceedings. The project takes into account legal requirements for handling digital evidence and the usability of automated analysis results.

2 Introduction

2.1 Purpose of the Communications Toolkit

The ADFIR Communications Toolkit is a practical set of rules, recommendations, standard texts and templates designed to help project partners communicate about the project, its activities and results in a consistent, coordinated and understandable manner. Its purpose is not to replace the Communication, Dissemination and Exploitation Plan (D7), but to translate its strategic principles into operational tools that can be used in day-to-day communication.

The Project Description explicitly envisages the creation of a communications toolkit to support clear and consistent communication by all partners. The Toolkit is the public D10 deliverable of Work Package KPB1 and is intended for publication on the project website. Its basic principle is that the ADFIR project should be presented accurately in terms of content and consistently in visual terms across the website, social media, professional events, printed materials, presentations and media outputs.

2.2 Basis and Link to KPB1.6 and D7

The Toolkit is based on Task KPB1.6 – communication, dissemination and exploitation of results (CDE), which includes the creation and maintenance of the main project website, dissemination of information through partner websites, and preparation of a detailed

communication and dissemination plan, including media promotion. It also builds on D7 – Communication, Dissemination and Exploitation Plan, which identifies target groups, key messages, communication channels, visual identity and rules for monitoring communication activities.

D7 sets out the strategy – to whom, why, when and through which channels the project communicates. D10 provides a practical answer to the question of how partners should prepare communication so that it remains consistent. The rules in this Toolkit should therefore be used for every communication activity together with the current CDE Plan and the applicable funding acknowledgement and visual identity requirements.

2.3 Users and Scope of the Toolkit

The Toolkit is intended for all ADFIR project partners and persons who prepare or approve project communication on their behalf. It is used in particular when preparing:

- content for the project website and partner websites;
- social media posts and campaigns;
- press releases and media releases;
- presentations at conferences, workshops and professional events;
- leaflets, posters, brochures and other promotional materials;
- invitations, newsletters and e-mail communication addressed to external target groups;
- policy briefs, professional outreach materials and training materials;
- communication of results, milestones and opportunities for further use of project outputs.

The Toolkit does not apply to internal professional or administrative communication in which the project is not presented externally, unless a specific project document provides otherwise.

3 ADFIR Project Communications Toolkit

This section contains practical rules and templates that partners should use in external communication activities. The core principles are consistent use of the project name and visual identity, common key messages, an appropriate communication style and mandatory funding information.

3.1 Project Identity and Mandatory Communication Elements

Project name and acronym

When the project is first mentioned in a document or communication output, its official title “Automatizácia digitálnej forenzej analýzy a odpovede na incident” should be used together with the acronym ADFIR. The official project code is 09I05-03-V02-00079. In subsequent text,

the shortened designation “ADFIR project” or “ADFIR” may be used. The official Slovak title and acronym should not be altered arbitrarily. In English-language communication outputs, a working English translation of the title may be used, while the official project title remains Slovak.

Recommended project designation	
Full title	Automatizácia digitálnej forenznej analýzy a odpovede na incident (ADFIR)
Short designation	ADFIR project / ADFIR
Working English translation	Automation of Digital Forensic and Incident Response (ADFIR)

Project partners

When referring to the project consortium, the official names of the partners should be used. Shortened names may be used after the full name has been stated for the first time or where this follows from the graphical format of the material.

- Univerzita Pavla Jozefa Šafárika v Košiciach (UPJŠ).
- IstroSec s. r. o. (IstroSec).
- European Information Society Institute, o. z. (EISI).

Logo and visual identity

The ADFIR project logo is the primary identifying element of the project. Only its approved version should be used in communication materials and together with the other elements of the project visual identity. The logo should not be distorted, cropped, recoloured arbitrarily or combined with graphic elements in a manner that reduces its legibility. If a particular format requires resizing, the logo aspect ratio must be preserved.

Preferred fonts, the colour palette and graphic elements should be based on approved project templates. For materials created by partners, use of an existing project template is preferred over creating a new one in order to maintain visual continuity across outputs.

Funding information

Every communication material for which the format and funding rules so require must contain the applicable logos and information on project funding. The following standard wording may be used in text-based outputs:

Standard funding wording	
SK	Projekt Automatizácia digitálnej forenznej analýzy a odpovede na incident (ADFIR) je financovaný Európskou úniou – Next GenerationEU prostredníctvom Plánu obnovy a odolnosti Slovenskej republiky pod číslom projektu č. 09I05-03-V02-00079.

Standard funding wording	
EN	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.

If specific funding publicity rules prescribe exact wording, logo order or other mandatory elements, those requirements take precedence over this general template.

3.2 Key Messages and Standard Project Descriptions

Key messages should communicate the substance of the project simply and accurately, without unduly overstating the results. ADFIR is a research project at TRL 1–3; communication should therefore not create the impression that it is a fully commercialised or production-deployed system unless a specific result has actually reached that level.

One-sentence project description

One-sentence description	
EN	ADFIR is a research project focused on automating selected processes of digital forensic analysis and cybersecurity incident response using data analytics and machine learning, while taking into account legal requirements for handling digital evidence.

Short boilerplate

Short project description – suitable for the website, social media and events	
Text	The ADFIR project explores opportunities to automate the collection, processing and analysis of digital traces in cybersecurity incident response and digital forensic analysis. It brings together expertise in cybersecurity, data analytics, machine learning and law. The aim is to support faster, more consistent and more verifiable work with digital evidence and to create results that can be used for further research, security practice and the legal environment.

Extended boilerplate

Extended project description – suitable for press releases, brochures and professional materials	
Text	The ADFIR project – Automation of Digital Forensic and Incident Response – responds to the growing volume of digital data and the shortage of specialist capacity needed to investigate cybersecurity incidents. The project explores automated approaches to the collection, representation, analysis, interpretation and visualisation of digital traces using data analytics and machine learning. The project also includes legal research focused on personal data protection, anonymisation, integrity and usability of digital evidence, and the legal conditions for the provision of forensic services. The results are intended to support security teams, legal professionals, the research community and the further development of digital forensics tools.

Four core project benefits

- Faster incident response. Automated approaches are intended to support faster identification of the causes of incidents and the adoption of effective measures.
- Reduced demand on specialist capacity. Automation of routine and time-consuming tasks is intended to allow analysts to focus on more complex cases and decision-making.
- More consistent and verifiable outputs. Common methodologies and tools are intended to support the accuracy, repeatability and transparency of analytical procedures.
- Linking the technical and legal dimensions. The project takes into account requirements for lawful processing, data protection and the future usability of digital evidence in legal proceedings.

Messages by target group

Target group	Primary message	Recommended emphasis
Security teams (CSIRT/SOC, forensic analysts, incident responders)	ADFIR explores procedures that can accelerate and improve the accuracy of digital trace processing during incident response.	Practical usability, verifiability, reduction of routine tasks, interoperability.

Target group	Primary message	Recommended emphasis
Legal professionals and law-enforcement authorities	The project links the technical processing of digital evidence with questions of lawfulness, integrity, authenticity and procedural usability.	Legal safeguards, chain of custody, transparency of automation, expert verification.
Research and academic community	ADFIR creates new methodological, data and analytical foundations for further research in digital forensics, data analytics and machine learning.	Open results, publications, datasets, follow-on R&D.
Developers and the commercial sector	Project results may serve as a basis for further development and integration of new analytical approaches into security tools and services.	Opportunities for further development, implementation and commercialisation after further R&D.
Policymakers and public institutions	The project provides expert knowledge relevant to modernising approaches to digital evidence and cybersecurity.	Policy recommendations, legal and societal impacts, public interest.
Students and early-career researchers	ADFIR provides interdisciplinary knowledge at the intersection of cybersecurity, data analytics and law.	Education, case studies, training materials, research opportunities.
General public and media	ADFIR explores how automation can support faster and more reliable investigation of cybersecurity incidents.	Clarity, practical benefits, data protection, avoiding technical jargon.

3.3 Language, Terminology and Communication Style

D7 envisages a differentiated communication style depending on the target group. Professional and formal outputs should be precise and terminologically consistent; social media, blog and outreach outputs may use more accessible language, shorter messages and visual elements. Regardless of the channel, communication must be factually correct, grammatically accurate and understandable.

Basic style rules

- Use factual, professional and understandable language appropriate to the target group.
- Use established terminology in professional materials; explain abbreviations and technical terms when they are first used.
- In communication intended for the general public, limit jargon and technical details that are not necessary to understand the main message.
- Do not create the impression that automation replaces human expert assessment; the project communicates automation as a tool supporting analytical work.
- Do not present research or experimental results as production-validated solutions unless this has been demonstrated.
- Distinguish between a “digital trace”, “digital evidence”, “automated analysis” and a “model output” according to context, and do not present an automated output as an infallible conclusion.
- Use appropriately qualified wording for legal statements and avoid absolute claims regarding automatic admissibility or evidential weight of outputs.

Sensitive and non-public information

Communication outputs must not disclose non-public security information, personal data, confidential technical information, vulnerabilities, authentication data, internal partner information or results whose publication has not been approved. Before publishing case studies, screenshots, photographs or dataset samples, it must be verified that publication does not breach data protection, confidentiality, intellectual property or security obligations.

3.4 Templates for Communication Channels

The following templates are designed so that partners can use them directly or adapt them appropriately to a specific output. Content should always be adapted to the target group, while the basic project information, visual identity and factual statements must remain consistent.

3.4.1 Website article / news item

Website article structure template	
Headline	[Clear result or event – e.g. “ADFIR presents results ...”]
Lead	2–3 sentences: what happened, who was involved and why the information matters.
Context	Brief explanation of the problem or need addressed by the activity.
What the project did	Factual description of the activity, methodology, experiment, publication or event.

Website article structure template	
Significance / benefit	What the result means for the target group and how it may be developed further.
Quote	Optional quotation from a project team member or expert.
Call to action	Link to a publication, registration, contact, another output or the project website https://adfir.upjs.sk/
Closing	Short project boilerplate + funding information.

3.4.2 Social media

Social media posts should be concise, convey one main message and, where possible, link to more complete content on the project website. The official social media profile of the project is the ADFIR LinkedIn profile (<https://www.linkedin.com/company/adfir-project/>). A professional but accessible tone is appropriate for LinkedIn. Partners may also share project content through their own communication channels, while preserving the substance of project claims, the visual identity and a link to official project content.

Social media post template	
Hook	[One sentence stating the result or question.]
Core message	In the ADFIR project, we [activity/result]. The aim is [practical significance].
Context	The result forms part of research on the automation of digital forensic analysis and cybersecurity incident response.
CTA	More information: https://adfir.upjs.sk/
Recommended hashtags	#ADFIR #DigitalForensics #Cybersecurity #IncidentResponse #MachineLearning

When publishing their own posts, partners may adapt the text to their audience, but should not change the substance of project claims or make unverified claims about results or the commercial readiness of the project.

3.4.3 Press release and media release

D7 envisages a consistent structure for press and media releases: a concise headline; an opening paragraph summarising what happened, who was involved, when it happened and why the information is relevant; expanded context; quotations where appropriate; brief information about the project and partners; contact details; and a link to the project website.

Press / media release template	
Headline	[Concise headline with a clear result]

Press / media release template	
Date and place	[City], [date]
Lead	Who? What? When? Where? Why does it matter?
Context	Description of the problem, project activity and connection with ADFIR objectives.
Result	Specific, verifiable result or milestone and its practical significance.
Quote	"[Quote]," said [name, position, organisation].
About the project	[Short ADFIR boilerplate]
Partners	UPJŠ IstroSec EISI
Media contact	[name / e-mail / telephone] Website: https://adfir.upjs.sk/
Funding	[standard funding wording]

3.4.4 Invitation to a workshop, conference or event

Invitation template	
Event title	[Title]
Date / time / venue	[Date] [time] [venue / online]
Target audience	[target group]
What participants will learn	3–5 concise points with specific benefits.
Speakers	[names and organisations]
Registration	[URL / QR code / registration deadline]
About ADFIR	[one-sentence or short boilerplate]
Funding and logos	[mandatory project and funding logos according to the template]

3.4.5 Newsletter / information e-mail

Newsletter / information e-mail template	
Subject	ADFIR [main news item or call to action]
Introduction	One short sentence explaining why the recipient is receiving the information.
Main news item	[2–4 paragraphs / bullet points]
New outputs	[links to publications, methodologies, datasets, articles]
Events	[invitations / registration]
CTA	Visit https://adfir.upjs.sk/ / download the output / register / contact the project
Footer	Contact details + boilerplate + funding information.

3.4.6 Presentations

Presentations should use the approved project template and a consistent visual style. The opening slide should preferably state the presentation title, the ADFIR project name, the author and the organisation. The final slide should include contact details, the project website and funding information. When presenting results, verified results should be distinguished from working hypotheses or experimental findings.

Minimum presentation elements	
Opening slide	Presentation title ADFIR author partner event date
Content slides	Clear heading, one main message per slide, readable charts and explanation of abbreviations.
Results	State the data source/method to the extent necessary for expert understanding; do not overstate the degree of validation.
Closing slide	Key takeaway website: https://adfir.upjs.sk/ LinkedIn: https://www.linkedin.com/company/adfir-project/ contact funding.

3.4.7 Brochures, posters and leaflets

D7 envisages the use of brochures, posters and leaflets as supporting promotional materials. For short formats, it is recommended to focus on the minimum information necessary to identify the project and direct the audience to further sources.

- project name and ADFIR logo;
- one or two key messages or project objectives;
- a brief statement of the main benefits or current result;
- the project website and basic contact information;
- a QR code directing users to the relevant subpage or output;
- mandatory logos and funding information.

3.4.8 Policy brief / recommendation for policymakers

The Project Description envisages the preparation of policy briefs and communication of findings and recommendations to policymakers. A policy brief should be shorter than a scientific study and should clearly distinguish scientific findings, legal or technical limitations and the recommendation itself.

Policy brief template	
Title	[Specific issue / recommendation]

Policy brief template	
Executive summary	3–5 sentences stating the main issue and recommendation.
Problem	Why the topic is relevant to digital forensics / cybersecurity / justice.
ADFIR findings	Verified findings only; clearly state limitations.
Recommendations	3–5 specific, actionable recommendations.
Impacts	Expected benefit and possible risks / trade-offs.
Contact and sources	Project website https://adfir.upjs.sk/ , relevant outputs and contact person.
Funding	[standard funding wording]

3.5 Communication Preparation and Approval Process

Consistency of communication is ensured not only through the use of templates, but also through appropriate review before publication. The specific process may be adapted to the type of output and the organisational arrangements of the partner. At a minimum, content, expert and communication review should be distinguished.

Step	Responsibility	Review	Output
1. Draft content	Partner / activity author	Are the target group and main message clear?	First draft
2. Expert review	Relevant team member / partner	Are the statements factually correct and consistent with the current state of the project?	Expert-reviewed draft
3. Legal / security review where needed	Relevant expert	Does the text avoid unauthorised personal data, confidential information, IP or security-sensitive information?	Approved content
4. Communication review	Person responsible for CDE / communication	Are key messages, visual identity, funding information and language quality compliant?	Publishable version

Step	Responsibility	Review	Output
5. Publication and recording	Manager of the relevant channel	Has the correct file/link been published and has the activity been recorded for KPI purposes?	Published output + record

Communication before publication of results

For results that have not yet been published or approved by the project team, it is recommended to verify before external communication whether publication could affect intellectual property protection, a planned scientific publication, confidentiality or security. Where there is doubt, internal approval should take precedence over speed of publication.

3.6 Recording Communication Activities

Communication and dissemination activities should be recorded so that their reach can be evaluated and a KPI report can be prepared. For each significant activity, it is recommended to record at least the date, type of activity, channel, responsible partner, target group, URL or evidence of publication, and available reach or engagement data.

Minimum communication activity record	
Date	[DD.MM.YYYY]
Partner	[UPJŠ / IstroSec / EISI]
Type	[website / social media / conference / workshop / press release / publication / other]
Activity title	[title]
Target group	[group/groups]
URL / evidence	[link / file / screenshot / event programme]
Reach / KPI	[views, participants, interactions, media mentions – if available]
Note	[brief result / follow-up]

4 Overview

The following checklist provides a quick aid before publication of any external ADFIR project communication output.

Checklist question	Yes / No	Note
Is it clear who the output is intended for and what its main message is?	☐ Yes ☐ No	
Is the correct ADFIR name and approved visual identity used?	☐ Yes ☐ No	
Is the content factually correct and consistent with the current state of the project?	☐ Yes ☐ No	
Is it adequately explained whether the result is research, experimental or validated?	☐ Yes ☐ No	
Does the output avoid unauthorised personal data, confidential information, trade secrets or security-sensitive information?	☐ Yes ☐ No	
Are intellectual property rights in texts, images, screenshots and data respected?	☐ Yes ☐ No	
Is the communication understandable to the target group and terminologically consistent?	☐ Yes ☐ No	
Does the output contain the required logos and funding information?	☐ Yes ☐ No	
Does the website or social media output contain an appropriate call to action and, where relevant, a link to the official project website or LinkedIn profile?	☐ Yes ☐ No	
Has the output been reviewed for language and subject-matter accuracy?	☐ Yes ☐ No	
Has the activity been recorded or is it ready to be recorded for KPI purposes?	☐ Yes ☐ No	

5 Ready-to-Use Text Templates

This section brings together the most frequently used text blocks, which may be inserted directly into a communication output after checking that they remain current.

5.1 Standard Project Boilerplate

ADFIR – Automation of Digital Forensic and Incident Response – is an interdisciplinary research project focused on automating selected processes of digital forensic analysis and cybersecurity incident response. It combines research in cybersecurity, data analytics, machine learning and law. The project is implemented by Univerzita Pavla Jozefa Šafárika v Košiciach, IstroSec s. r. o. and European Information Society Institute, o. z.

5.2 Standard Funding Wording

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.

5.3 Short Text for Social Media

ADFIR explores how automation and machine learning can support digital forensic analysis and cybersecurity incident response. The project links technical research with legal requirements for handling digital evidence. More information: <https://adfir.upjs.sk/> LinkedIn: <https://www.linkedin.com/company/adfir-project/>

5.4 Short Text for an Event

ADFIR is a research project focused on the automation of digital forensic analysis and cybersecurity incident response using data analytics and machine learning. The project examines both the technical and legal conditions for effective and trustworthy work with digital evidence.

5.5 Closing Text for a Presentation

Thank you for your attention. More information about the ADFIR project, its outputs and upcoming activities is available at <https://adfir.upjs.sk/>. Follow the project on LinkedIn: <https://www.linkedin.com/company/adfir-project/>. The project is funded by the European Union – NextGenerationEU through the Recovery and Resilience Plan of the Slovak Republic.

6 Basis and Related Project Documents

The Communications Toolkit was prepared primarily on the basis of the following project documents:

- Project Description – ADFIR, in particular Section 2.2 Measures to maximise impact – dissemination and communication, exploitation of results, and Work Package KPB1.
- D7 – Communication, Dissemination and Exploitation Plan of the ADFIR project.
- Approved project templates, the ADFIR logo and visual identity used in project outputs.

If the CDE Plan, visual identity or mandatory funding publicity rules are updated during project implementation, the current approved version of the relevant document or template should always be used.